The Grothendieck Theory of Dessins d'Enfant
LMS LNM 200, Cambridge Univ. Press, 1994

The Grothendieck-Teichmüller group and automorphisms of braid groups

Pierre Lochak* and Leila Schneps**

Abstract

We show that the groups GT_ℓ and $\widehat{GT}$ defined by Drinfel'd are respectively the automorphism groups of the tower of the "pro-ℓ completions" $B_n^{(\ell)}$ of the Artin braid groups and of their profinite completions $\hat{B}_n$, equipped with certain natural inclusion and strand-doubling homomorphisms.

*

§1. Introduction

In [D], Drinfel'd introduced the groups GT_ℓ and $\widehat{GT}$ via deformations of quasi-Hopf algebras, a structure which he had defined in a previous paper. He showed, using tensor-categorical methods, that for each $n \geq 3$, $\widehat{GT}$ can be viewed as a subgroup of the automorphism group of $\hat{B}_n$, the profinite completion of the Artin braid group B_n (see §2 and the appendix for the precise definitions of braid groups). One of the main goals of this article, is to characterize this subgroup completely for $n \geq 1$ in both the pro-ℓ and the profinite cases. It is worth recalling that $\mathrm{Aut}(B_n)$, the automorphism group of the *discrete* group B_n, is easily described: by a result of Dyer and Grossman (cf. [DG]), we know that $\mathrm{Aut}(B_n)$ is generated by the inner automorphisms of B_n and a single other one given by the mirror reflection, which sends each generator of B_n to its inverse. In contrast to this, the automorphism groups of the pro-ℓ and profinite completions $B_n^{(\ell)}$ and $\hat{B}_n$ of B_n are large and complex groups; this emphasizes the fact that working with such completions is an essential part of the theory.

One of the most interesting features of the group $\widehat{GT}$ is that, using a result of Belyi (cf. [Be]), Drinfel'd showed that there exists an injection of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $\widehat{GT}$. Characterizing the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\widehat{GT}$ is still a major open problem. This connection of $\widehat{GT}$ with Galois theory is not pursued in [D]; it is a surprising fact that one can even define a group containing the absolute Galois group with no reference whatsoever to the Galois theory of number fields.

A different way of perceiving the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as elements of $\widehat{GT}$

was described by Ihara (cf. [I1]), using moduli spaces of Riemann surfaces with ordered marked points. It is known that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on certain fundamental groups of these moduli spaces. By considering the two simplest cases, those of the sphere with 4 and 5 marked points respectively, Ihara shows that this classical action corresponds exactly to that of $\widehat{GT}$ restricted to certain subgroups of $\hat{B}_3$ and $\hat{B}_4$ which are isomorphic to these fundamental groups. This construction should probably be thought of as a starting point for an impressive construction sketched by A. Grothendieck in his "Esquisse d'un programme" ([G], 1984, unpublished). He describes there an action of the absolute Galois group on what he calls the tower of Teichmüller groupoids, that is, a "tower" of algebraic fundamental groupoids (using certain geometrically significant base points) of the moduli spaces for all genera and any number of marked points (and presumably over any ground field).

Let us now extract a few points and suggestions which served as motivations for the present work, and particularly as inspiration for future directions.

i) $\widehat{GT}$ (resp. GT_ℓ) acts on the profinite (resp. "pro-ℓ", see below) completions of the braid groups B_n, and these groups can be joined by the extensions of the natural inclusion homomorphisms $i_n : B_n \hookrightarrow B_{n+1}$ to form a "tower" of groups whose structure is respected by the action of $\widehat{GT}$ (resp. GT_ℓ). We may ask the following question (inspired by a question of Drinfel'd relative, not to the profinite completions but to the k-pro-unipotent completions of the B_n for a field k): is the group of tuples $(\phi_n)_{n\geq 1}$, where each $\phi_n \in \mathrm{Aut}(\hat{B}_n)$ and the ϕ_n respect the inclusion homomorphisms i_n, equal to $\widehat{GT}$? The goal of this article is to give a partial answer to this question; we show that $\widehat{GT}$ (resp. $\widehat{GT_\ell}$) are the groups of tuples $(\phi_n)_{n\geq 1}$ where the ϕ_n respect not only the inclusion homomorphisms but certain natural "string-doubling" ones as well.

ii) The B_n's are closely related to the Teichmüller modular groups in genus 0. Indeed $M(0,n)$, the modular group corresponding to spheres with n marked points, is a quotient of B_n and contains B_{n-2} and $B_{n-1}/(\text{center})$ as subgroups (cf. §2 and the appendix, as well as [Bi]). This gives the main link between the braid groups considered in this article and the geometry of moduli spaces as reflected by the modular groups which are their fundamental groups.

iii) Grothendieck considers what he calls the full Teichmüller tower, i.e. the tower consisting of the Teichmüller groupoids mentioned earlier (rather than the Teichmüller groups) in all genera. One should consider the towers of braid groups given below as very primitive versions of this tower, in genus zero and without the geometric significance of the choice of base points.

iv) A very important suggestion of Grothendieck is that the tower of Teichmüller groupoids (fundamental groupoids of the moduli spaces) should be entirely reconstructible from its first two levels ("les deux premiers étages"), levels being numbered according to their modular dimension (the complex dimension of the moduli space). This is in some sense true for the braid towers considered below, the first and second levels being embodied in B_3 and B_4 respectively.

v) Grothendieck suggests that although the absolute Galois group acts on the whole Teichmüller tower, by virtue of the preceding remark this action should be completely reflected in the restriction of this action to the first two levels. This remark corresponds precisely to what happens in the more limited situation of the actions of GT_ℓ and $\widehat{GT}$ on the braid towers considered below (see the main theorem).

From this general and speculative viewpoint (which does not claim to do more than render the faintest shadow of Grothendieck's vision), it would seem that from the profinite situation one should be able to derive a new description of the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. So far, only the information coming from the action of this group on the fundamental group of the first level, namely the spheres with four marked points (whose moduli space is the much-studied $\mathbb{P}^1\mathbb{C} - \{0, 1, \infty\}$), has been studied in any detail, and just enough is known about the second level (the spheres with five marked points) to be able to derive the important new property of elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which it entails (the so-called pentagon equation, corresponding to (III) below). It is still an open question whether considering higher levels, in genus zero or in any genus, should or should not provide any new constraints on the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (see [I1] for further remarks on this subject). One of the tasks which lie ahead of us may well consist in an exploration of the deep interplay between the action of the absolute Galois group and the geometry of the various moduli spaces, which Grothendieck appears to have uncovered.

Precise definitions and various necessary results on the different kinds of braid groups can be found in §2 and especially in the appendix included at the end of this article. Let us now turn to the definition of the groups GT_ℓ and $\widehat{GT}$, as given in [D]. In reading this definition, it should be kept in mind that the form (λ, f) of the elements, and the relations (I), (II) and (III) are all combinatorical properties of the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ itself.

In general (i.e. with the exception of $\widehat{GT}$), we write $\hat{G}$ for the profinite completion of a group G, and G^ℓ for its pro-ℓ completion. Let $\mathbb{Z}_\ell$ denote the ℓ-adic integers, $\hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$, F_n the free group on n generators for $n \geq 1$, and F_n^ℓ and $\hat{F}_n$ its pro-ℓ and profinite completions respectively. If x, y are the generators of $\hat{F}_2$, we write an element of $\hat{F}_2$ as a "profinite word" $f(x,y)$, although it is not generally a word in x and y. This notation allows us to give a meaning to the element $f(\bar{x},\bar{y})$ where $\bar{x}$ and $\bar{y}$ are arbitrary elements of a profinite group.

For a group G, let $[G,G]$ denote its derived subgroup (in the topological sense if G is a topological group). Let $\underline{GT}_{\ell,0}$ (resp. $\underline{\widehat{GT}}_0$) be the set of couples $(\lambda,f) \in \mathbb{Z}_\ell^* \times [F_2^\ell, F_2^\ell]$ (resp. $(\lambda,f) \in \hat{\mathbb{Z}}^* \times [\hat{F}_2,\hat{F}_2]$) satisfying the two following relations:

(I) $f(x,y)f(y,x) = 1$

(II) $f(z,x)z^m f(y,z)y^m f(x,y)x^m = 1$,

where $m = \frac{1}{2}(\lambda-1)$ and $z = (xy)^{-1}$, this set being equipped with the multiplication law defined by:

$$\bigl(\lambda_1, f_1(x,y)\bigr)\bigl(\lambda_2, f_2(x,y)\bigr) = \bigl(\lambda_1\lambda_2, f_2\bigl(f_1(x,y)x^{\lambda_1}f_1(x,y)^{-1}, y^{\lambda_1}\bigr)f_1(x,y)\bigr),$$

which makes it into a semigroup. Define $\widehat{GT}_0$ (resp. $\widehat{GT}_{\ell,0}$) to be the group of invertible elements of this semigroup. Define GT_ℓ (resp. $\widehat{GT}$) to be the subgroup of $GT_{\ell,0}$ (resp. $\widehat{GT}_0$) of couples (λ,f) satisfying the following relation, which takes place in the pro-ℓ (resp. profinite) completion of the group K_4 (the precise definition of which, together with its generators x_{ij} for $1 \leq i < j \leq 4$, is given in §2):

(III) $f(x_{12},x_{23}x_{24})f(x_{13}x_{23},x_{34}) = f(x_{23},x_{34})f(x_{12}x_{13},x_{24}x_{34})f(x_{12},x_{23})$.

Acknowledgments: We would like to extend our warmest thanks to Pascal Degiovanni and Jean-Marc Couveignes for the hours of (extremely animated, occasionally hilarious) discussion on many aspects of the questions considered in this article, and the reams of e-mail to which these discussions gave rise. We are also particularly grateful to Professor Ihara for the patience and generosity with which he answered our questions and explained his work to us. It is a real pleasure to thank Professor Nakamura for his careful reading of the manuscript, for pointing out some errors and for making the preprint [N], containing some results which were especially helpful (cf. §4), available to us. It goes without saying that the results presented here were principally inspired by ideas of Grothendieck.

§2. The braid towers

We now introduce the groups we shall work with, starting with the discrete versions, and recall some useful facts about them; a general reference for this is [Bi], but the main reference is the appendix to this article in which detailed proofs of all the necessary technical results on braid groups (and somewhat more) are given.

For $n \geq 2$, let B_n be the Artin braid group on n strings, generated by elements $\sigma_1, \ldots, \sigma_{n-1}$ such that

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } 1 \leq i \leq n-2 \quad \text{and} \quad \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2. \tag{1}$$

It is useful to consider the following more symmetric presentation of B_n (which is restated and proved as proposition A1 of the appendix).

Proposition 1: *The following is a presentation for the Artin braid group B_n: as generators we take σ_{ij} for $1 \leq i, j \leq n$ with the relations*

$$\sigma_{ii} = 1, \quad \sigma_{ij} = \sigma_{ji} \;\; \textit{and} \;\; \sigma_{jk}\sigma_{ij} = \sigma_{ik}\sigma_{kj} (= \sigma_{ij}\sigma_{ki}) \quad \text{for} \quad i < j < k;$$

$$\sigma_{ij}\sigma_{kl} = \sigma_{kl}\sigma_{ij} \quad \text{for} \quad i < j < k < l \quad \text{or} \quad k < i < j < l.$$

The usual generators are given by $\sigma_i = \sigma_{i,i+1}$ for $1 \leq i \leq n-1$. An important consequence of the above relations is that σ_{ij} and σ_{kl} are conjugate for all i, j, k, l $(i \neq j, k \neq l)$. Indeed, if $k = i$, σ_{ij} and σ_{il} are conjugate because $\sigma_{jl}\sigma_{ij} = \sigma_{il}\sigma_{jl}$. If $k \neq i$, σ_{ij} is conjugate to σ_{ik}, which in turn is conjugate to σ_{kl}, so that σ_{ij} and σ_{kl} are again conjugate. In particular, every σ_{ij} $(i \neq j)$ is conjugate to $\sigma_{12} = \sigma_1$, that is

$$\sigma_{ij} = a_{ij}^{-1}\sigma_1 a_{ij} \quad \text{for} \quad 1 < i, j < n, \; i \neq j, \tag{2}$$

for some elements a_{ij} which can be easily computed. This property will be used below (see sublemma 13 in §6).

We now pass to the definition and some properties of the *pure* braid groups. There exists a canonical surjection $\rho_n : B_n \to S_n$, where S_n is the group of permutations on n letters, obtained by quotienting B_n by the relations $\sigma_i^2 = 1$. The kernel $K_n = \operatorname{Ker} \rho_n$, the pure plane braid group on n strings, can be described as follows: it is generated by the elements x_{ij} for $1 \leq i < j \leq n$ defined by

$$x_{ij} = \sigma_{j-1} \cdots \sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1} \cdots \sigma_{j-1}^{-1}.$$

It is useful to set $x_{ji} = x_{ij}$ and $x_{ii} = 1$; then $x_{ij} = \sigma_{ij}^2$ for the σ_{ij} as in proposition 1. The x_{ij} satisfy the following relations, where we write (a, b) for the commutator $aba^{-1}b^{-1}$:

- $x_{ij}x_{ik}x_{jk}$ commutes with x_{ij}, x_{ik} and x_{jk} for all $i < j < k$;

- $(x_{ij}, x_{kl}) = (x_{il}, x_{jk}) = 1$ for $i < j < k < l$; $\quad (1')$

- $(x_{ik}, x_{ij}^{-1}x_{jl}x_{ij}) = 1$ for $i < j < k < l$.

As an immediate consequence of the conjugation relations (2) above, we get:

$$x_{ij} = a_{ij}^{-1}x_{12}a_{ij} \quad \text{for} \quad 1 < i < j < n. \tag{2'}$$

Let us also define $y_i \in K_n$ and $\omega_i \in K_n$ by:

$$y_1 = 1, \quad y_i = \sigma_{i-1}\cdots\sigma_2\sigma_1^2\sigma_2\cdots\sigma_{i-1} = x_{1i}x_{2i}\cdots x_{i-1,i} \text{ for } 2 \le i \le n$$

and

$$\omega_i = y_1y_2\cdots y_i \ , \text{ for } 1 \le i \le n.$$

Then the y_i's commute, i.e. $(y_i, y_j) = 1$ for all i, j, and the center of B_n and of K_n is an infinite cyclic group generated by ω_n. From now on we use the notation $Z(G)$ for the center of a group G. However we generally write just G/Z for the quotient of G modulo its center.

The sphere braid group H_n (the Hurwitz braid group) is the quotient of B_n by the "sphere relation" $y_n = 1$ (sometimes called the Hurwitz relation), and the modular group $M(0, n)$ (0 because it is the modular group for genus 0 surfaces, i.e. spheres) is the quotient H_n/Z; in other words:

$$M(0, n) = H_n/\langle\tilde{\omega}_n = 1\rangle = B_n/\langle y_n = \omega_n = 1\rangle,$$

where $\tilde{\omega}_n$ is the image of ω_n in H_n. The pure sphere braid groups P_n and modular groups $K(0, n)$ are defined to be the kernels of the natural maps $H_n \to S_n$ and $M(0, n) \to S_n$ induced by $\rho_n : B_n \to S_n$. In particular, the subgroup U_n of K_n generated by the n elements $x_{1i}x_{2i}\cdots x_{n,i}$, for $1 \le i \le n$ is a normal subgroup and P_n is exactly K_n modulo this subgroup (cf. lemma A2 of the appendix), while $K(0, n)$ is P_n/Z. The n equations

$$x_{1i}x_{2i}\cdots x_{n,i} = 1, \quad 1 \le i \le n \tag{3}$$

are known as the "Hurwitz relations based at i".

We use the notation $\tilde{\alpha}$ for the image in P_n (resp. its completions P_n^ℓ or $\hat{P}_n$) of any element $\alpha \in K_n$ (resp. K_n^ℓ or $\hat{K}_n$) and $\bar{\alpha}$ for the image of α in $K(0, n)$ (resp. $K(0, n)^\ell$ or $\widehat{K(0, n)}$). The following proposition, giving several relations, inclusions and homomorphisms between the various types of braid groups, is proved as proposition A4 of the appendix, but we state it here for the convenience of the reader.

Proposition 2: *Let K'_n be the subgroup of K_n generated by the x_{ij} for $1 \le i < j \le n$ with $(i,j) \ne (1,2)$. Then*

(i) $K_n = K'_n \times \langle \omega_n \rangle$.

(ii) There are two natural inclusions i_1 and i_2 of K_{n-1} into K_n. Both send x_{ij} to x_{ij} for $1 \le i < j \le n$, $(i,j) \ne (1,2)$. But i_1 is then defined by setting $i_1(x_{12}) = x_{12}$, whereas i_2 is defined by setting $i_2(\omega_{n-1}) = \omega_n$.

(iii) $P_n \simeq K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ and $K(0, n+1) \simeq P_{n+1}/Z \simeq K'_n$.

(iv) $P_{n+1} \simeq K_{n+1}/U_{n+1} \simeq K_n/\langle \omega_n^2 \rangle$.

(v) The subgroup of P_{n+1} generated by the $\tilde{x}_{ij}$ with $1 \le i < j \le n-1$ and $(i,j) \ne (1,2)$ and the central element $\tilde{\omega}_{n+1}$ of P_{n+1} is isomorphic to P_n. Indeed, $P_{n+1} = F_n \rtimes P_n$ where P_n is this subgroup and F_n is the free group of rank $n-1$ generated by $\tilde{x}_{1,n+1}, \ldots, \tilde{x}_{n,n+1}$ (whose product equals 1).

(vi) We have the inclusions $K(0, n+1) \simeq K_n/Z \subset B_n/Z \subset M(0, n+1)$.

Let us consider some low-dimensional examples which will be needed later on.

- B_3 is generated by σ_1, σ_2, with the relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$; its infinite cyclic center is generated by $\omega_3 = x_{12}x_{13}x_{23} = (\sigma_1\sigma_2)^3$.

- K_3 is the direct product of a free group on two generators, generated say by $x = x_{12}$ and $y = x_{23}$, and the infinite cyclic center generated by $x_{12}x_{13}x_{23}$. These x and y (together with $z = (xy)^{-1}$) appear in the defining relations (I) and (II) of $\widehat{GT}$ given above. The group $K(0,4) \simeq K_3/Z(K_3)$ is thus a free group on two generators.

We will need the following two relations, valid in the group $M(0,5)$:

$$\bar{x}_{45} = \bar{x}_{12}\bar{x}_{13}\bar{x}_{23} \ , \quad \bar{x}_{15} = \bar{x}_{23}\bar{x}_{24}\bar{x}_{34}. \tag{4}$$

Proof: In $M(0,5)$, we have $\bar{y}_5 = \bar{\omega}_5 = 1$, so

$$\bar{y}_2\bar{y}_3\bar{y}_4 = \bar{x}_{12}\bar{x}_{13}\bar{x}_{23}\bar{x}_{14}\bar{x}_{24}\bar{x}_{34} = 1;$$

moreover, we have $\bar{x}_{14}\bar{x}_{24}\bar{x}_{34}\bar{x}_{45} = 1$ in $M(0,5)$. This last identity is the Hurwitz relation based at 4 (see equation (3)). Combining it with the center relation written as above proves the first of the relations (4); the second follows by shifting the indices (which *is* a legitimate operation in this situation, as the reader can easily convince her(him)self). $\diamond$

To finish with the preliminaries, we still have to define a – nonstandard – subgroup of $\hat{B}_n$ which will be used below. For $n > 1$, let A_n denote the abstract group isomorphic to the subgroup of B_n generated by $\sigma_1^2, \sigma_2, \cdots, \sigma_{n-1}$; a presentation of A_n is given by the following sets of relations:
- the relations (1) between the generators $\sigma_2, \cdots, \sigma_{n-1}$;
- the relations $(\sigma_1^2, \sigma_i) = 1$ for $2 < i \leq n-1$;
- the commutation relation $(\sigma_1^2, \sigma_2\sigma_1^2\sigma_2) = 1$, which is just $(y_2, y_3) = 1$.

We set by convention $B_1 = K_1 = A_1 = \{1\}$. Now, the pro-ℓ (resp. profinite) completions of the groups K_n, P_n and $K(0,n)$ are isomorphic to the free pro-ℓ (resp. profinite) groups on $n(n-1)/2$ generators quotiented by the relations $(1')$. Moreover (see for example [M] §2), the presentation of the profinite completions of the B_n and the A_n are identical to those of the discrete groups (so in particular all groups in Proposition 2 can be replaced by their profinite completions). This does not hold for the pro-ℓ completions of the B_n. We therefore set $B_n^{(\ell)}$ to be the free group on $n-1$ generators quotiented by the relations (1). This is not as arbitrary a procedure as it seems. Indeed, the group $B_n^{(\ell)}$ can be obtained as a modified pro-ℓ completion of B_n as follows: consider the elements of B_n as automorphisms of K_n (by the restriction to K_n of their action as inner automorphisms); these automorphisms extend to automorphisms of K_n^ℓ. The group $B_n^{(\ell)}$ occurs as the quotient of the semi-direct product $K_n^\ell \rtimes B_n$ defined by this action by the subgroup of elements of the form (x, x^{-1}), $x \in K_n \subset K_n^\ell$. Let us define $H_n^{(\ell)}$ and $M(0,n)^{(\ell)}$ to be the quotients of $B_n^{(\ell)}$ by the same relations as in the discrete case. Proposition 2 is valid when the groups K_n, P_n, B_n and $M(0,n)$ are replaced by K_n^ℓ, P_n^ℓ, $B_n^{(\ell)}$ and $M(0,n)^{(\ell)}$.

The map ρ_n can be extended to a map $\rho_n : B_n^{(\ell)} \to S_n$ (resp. $\rho_n : \hat{B}_n \to S_n$) and we still have $K_n^\ell = \mathrm{Ker}\,\rho_n$ (resp. $\hat{K}_n = \mathrm{Ker}\,\rho_n$). From now on we simply write ρ for the canonical epimorphisms from $B_n^{(\ell)}$ or $\hat{B}_n$ to S_n for any n. A final useful remark on $[B_n, B_n]$, the derived subgroup of the Artin braid group (and its pro-ℓ and profinite completions): the quotient of B_n (resp. $B_n^{(\ell)}$, $\hat{B}_n$) by its derived subgroup is isomorphic to the free abelian group on $n-1$ generators (resp. free pro-ℓ, free profinite).

Let us turn to the definition of the braid group tower $\mathcal{T}$.

A *tower of groups* is given by a family of groups $\{G_n\}_{n\in\mathcal{N}}$ for some index set $\mathcal{N}$, and for each pair $(i,j) \in \mathcal{N}$, of a (possibly empty) family $\mathcal{F}_{i,j}$ of homomorphisms $G_i \to G_j$. We ask that the sets $\mathcal{F}_{i,j}$ be saturated with respect to the composition of maps, i.e. we assume that $\mathcal{F}_{i,j} \supseteq \mathcal{F}_{k,j} \circ \mathcal{F}_{i,k}$ for all triples of indices i, j, k.

The *automorphism group* of a tower of groups is defined by

$$\{(\phi_n)_{n\in\mathcal{N}} \mid \phi_n \in \mathrm{Aut}(G_n) \text{ for } n \in \mathcal{N} \text{ and } f \circ \phi_i = \phi_j \circ f$$

$$\text{for all } i, j \in \mathcal{N}, \text{ and } f \in \mathcal{F}_{i,j}\}.$$

In what follows, we will frequently make use the following maps:

- $i_n : \hat{B}_n \to \hat{B}_{n+1}$, the natural inclusion map, given by $i_n(\sigma_i) = \sigma_i$ for $1 \le i \le n-1$;
- $f_n : \hat{A}_n \to \hat{B}_{n+1}$ the restriction of i_n to $\hat{A}_n$ and
- $g_n : \hat{A}_n \to \hat{B}_{n+1}$, such that $g_n(\sigma_1^2) = \sigma_2\sigma_1^2\sigma_2$ and $g_n(\sigma_i) = \sigma_{i+1}$ for $2 \le i \le n-1$.

Remark: *The maps i_n, f_n and g_n are group homomorphisms for $n \ge 1$.*

Proof: The maps i_n and f_n are clearly group homomorphisms. In order to prove that g_n is also a group homomorphism, it suffices to show that it respects the relations defining the group $\hat{A}_n$. Since these relations are the same as those defining A_n as remarked above, it suffices to show that g_n is a homomorphism from A_n into B_{n+1}, which is a straightforward calculation. Actually, using the set of defining relations for A_n given above, one sees that only the last one, namely $(y_2, y_3) = 1$ could be a problem, but g_n maps it onto the – true – relation $(y_3, y_4) = 1$. ◇

It is more enlightening to visualize the map g_n in terms of braids: the image of any braid in A_n is the same braid but with the first string doubled, in B_{n+1} (and in fact in A_{n+1}). Doubling the first string does not respect multiplication of arbitrary braids in B_n, and therefore does not induce a group homomorphism of B_n into B_{n+1}. In order for this map to be a group homomorphism, it is necessary to restrict it to those braids whose first strand, though it may wander about the braid, must return to its place at the end, i.e. the set of braids which is the pre-image under ρ_n in B_n of the subgroup of permutations in S_n which fix 1. But this is exactly the group A_n.

Let $\mathcal{T}$ be the tower of braid groups defined as follows: let the index set be the positive integers: as groups we take the $B_n^{(\ell)}$ for $n \ge 1$, and we equip this family with natural inclusions $i_n : B_n^{(\ell)} \to B_{n+1}^{(\ell)}$ given by $i_n(\sigma_i) = \sigma_i$ for $1 \le i \le n-1$. Saturation of these maps under composition means that in fact $\mathcal{T}$ is equipped with all the natural inclusions $i_{n,m} : B_n^{(\ell)} \to B_m^{(\ell)}$ for

$n < m$, so $i_n = i_{n,n+1}$. In order to avoid a cumbersome notation, we often write $B_n^{(\ell)} \subset B_m^{(\ell)}$ instead of $i_{n,m}(B_n^{(\ell)}) \subset B_m^{(\ell)}$. We also add in the map $g_3 : A_3^{(\ell)} \to B_4^{(\ell)}$ – together with its composition with the inclusion maps. For $N \geq 1$, let $\mathcal{T}_N$ denote the truncated tower given by the finite family of groups $B_n^{(\ell)}$ for $1 \leq n \leq N$, the inclusions $i_{n,m}$ for $1 \leq n < m \leq N$, and the map g_3 if $N \geq 4$.

The automorphism group of $\mathcal{T}$ is given by

$$\mathrm{Aut}(\mathcal{T}) = \{(\phi_n)_{n\geq 1} \mid \phi_n \in \mathrm{Aut}(B_n^{(\ell)}),\ i_n\phi_n = \phi_{n+1}i_n \text{ and } \phi_4 g_3 = g_3\phi_3\};$$

for $N \geq 1$, the automorphism group $\mathrm{Aut}(\mathcal{T}_N)$ of $\mathcal{T}_N$ is given in the exact same way, with n restricted by $1 \leq n \leq N-1$ and the compatibility condition for g_3 not included if $N \leq 3$. Note that the conditions $i_{n,m}\phi_n = \phi_n i_{n,m}$ are automatically satisfied for all $n < m$ if they are satisfied by the $i_n = i_{n,n+1}$. The reason for the appearance of the map g_3 will be clear from the proof of the corollary of proposition 6 (see §4 in fine). We do not know whether the result still holds true without this extra compatibility condition imposed on the ϕ_n.

Let now $\hat{\mathcal{T}}$ (resp. $\hat{\mathcal{T}}_N$) be the tower of groups defined as follows: as groups we take the $\hat{B}_n$ and the $\hat{A}_n$ for $n \geq 1$ (resp. $1 \leq n \leq N$), and we equip this family with all the maps i_n, f_n, g_n (and all maps obtained by composing them), for $n \geq 1$ (resp. $1 \leq n \leq N-1$).

We shall now prove that $\phi \in \mathrm{Aut}(\mathcal{T})$ (resp. $\mathrm{Aut}(\hat{\mathcal{T}})$) preserves the permutations of the $B_n^{(\ell)}$ (resp. $\hat{B}_n$) up to a possible twist by σ_1. From now on, for any element g of a group G, we write $\mathrm{Inn}(g)$ for the inner automorphism of G given by conjugation by g: $\mathrm{Inn}(g)(h) := g^{-1}hg$.

Lemma 3: *Suppose $\phi = (\phi_n)_{n\geq 1} \in \mathrm{Aut}(\mathcal{T})$ (resp. $\mathrm{Aut}(\hat{\mathcal{T}})$) fixes the permutations of $B_3^{(\ell)}$ (resp. $\hat{B}_3$), i.e. $\rho\circ\phi_3 = \phi_3$. Then ϕ fixes the permutations globally, i.e. $\rho \circ \phi_n = \phi_n$ for all n. If ϕ_3 does not fix the permutations of $B_3^{(\ell)}$ (resp. $\hat{B}_3$), then $\tilde{\phi}_3 = \mathrm{Inn}(\sigma_1) \circ \phi_3$ does, so $\tilde{\phi} := \big((\mathrm{Inn}(\sigma_1)\phi_n\big)_{n\geq 1}$ fixes the permutations globally.*

Proof: The proof is identical for the pro-ℓ and the profinite completions; indeed it only uses the fact that the automorphisms of the respective towers respect the inclusions i_n. We use the notation of the profinite case. Let us first suppose the following assertion true.

(*) Let ψ be an automorphism of $\hat{B}_n$ (for some $n \geq 1$); then it induces an inner automorphism of the permutation group S_n, i.e. there exists $\alpha \in S_n$ such that:

$$\rho \circ \psi(\sigma) = \alpha^{-1}\rho(\sigma)\alpha \quad \text{for all} \quad \sigma \in \hat{B}_n.$$

Write $\rho\phi_n = \mathrm{Inn}(\alpha_n)\rho$ for $n \geq 3$; since the center of S_n is trivial for $n \geq 3$, the $\alpha_n \in S_n$ are uniquely defined. Assume that ϕ_3 fixes the permutations, i.e. that $\alpha_3 = 1$. By a simple inductive argument, we show that then $\alpha_n = 1$ for all n. Assume it is true for $n-1$ ($n \geq 4$). Then α_n must lie in the centralizer of S_{n-1} in S_n, where S_{n-1} denotes the subgroup of the permutations in S_n fixing n. But as is easy to check, this centralizer is the identity when $n > 4$. So ϕ fixes the permutations globally, i.e. ϕ_n fixes the permutations of $\hat{B}_n$ for $n \geq 1$.

Note that for $n = 3$, the centralizer of S_2 in S_3 is isomorphic to $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$. This shows that if ϕ_3 does not fix the permutations of S_3, then $\mathrm{Inn}(\sigma_1) \circ \phi_3$ does, which gives the last assertion in the lemma.

We now prove assertion (*), which is the generalization to the profinite case of the following result ([DG], cor. 12): for every $\psi \in \mathrm{Aut}(B_n)$, there exists an inner automorphism β of B_n such that $\rho \circ \psi \circ \beta = \rho$. We know that K_n is characteristic in B_n (see [DG], thm. 11), and if $\psi \in \mathrm{Aut}(\hat{B}_n)$ is such that $\psi(\hat{K}_n) = \hat{H}$, then setting $H := B_n \cap \hat{H}$, we see that $\hat{H}$ is the profinite completion of H (since $\hat{H}$ is of finite index in $\hat{B}_n$), and so $B_n/H = \hat{B}_n/\hat{H} = S_n$. So by corollary 12 of [DG], $H = K_n$, so $\hat{H} = \hat{K}_n$, which means that $\hat{K}_n$ is characteristic in $\hat{B}_n$. Thus if $\psi \in \mathrm{Aut}(\hat{B}_n)$, $\rho \circ \psi$ induces an automorphism of S_n, so it is inner (the exceptional cases for $n = 4$ or 6 do not occur). $\diamond$

Corollary: *All the elements of* $\mathrm{Aut}(\hat{\mathcal{T}})$ *actually fix the permutations of* $\hat{B}_n$.

Proof: Let $(\phi_n)_{n\geq 1} \in \mathrm{Aut}(\hat{\mathcal{T}})$. By Lemma 3, either $\rho \circ \phi_n = \rho$ or $\rho \circ \phi_n = \mathrm{Inn}(12)\rho$ on $\hat{B}_n$, for all $n \geq 1$. If the second possibility were verified by ϕ then the following diagram would commute:

$$\begin{tikzcd} \hat{A}_n \arrow[r, "\rho"] \arrow[d, "\phi_n"'] & S_n \arrow[d, "\phi_n"] \\ \hat{A}_n \arrow[r, "\mathrm{Inn}(12)\rho"] & S_n. \end{tikzcd}$$

But ϕ_n preserves $\hat{A}_n$ and the image of $\hat{A}_n$ in S_n under ρ is the set of permutations fixing 1, whereas the image under $\mathrm{Inn}(12)\rho$ is the set of permutations fixing 2, so this diagram cannot commute. Thus $\rho \circ \phi_n = \rho$ for all $n \geq 1$. $\diamond$

Let $\mathrm{Inn}(\mathcal{T})$ $\big($resp. $\mathrm{Inn}(\mathcal{T}_N)\big)$ denote the subgroup of interior automorphisms of $\mathcal{T}$ (resp. $\mathcal{T}_N$) which act on each $B_n^{(\ell)}$ via conjugation by a fixed $\mathbb{Z}_\ell$-power of σ_1, so that $\mathrm{Inn}(\mathcal{T}) \simeq \mathrm{Inn}(\mathcal{T}_N) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_\ell$ for all N. Set

$\mathrm{Out}(\mathcal{T}) := \mathrm{Aut}(\mathcal{T})/\mathrm{Inn}(\mathcal{T})$ and $\mathrm{Out}(\mathcal{T}_N) := \mathrm{Aut}(\mathcal{T}_N)/\mathrm{Inn}(\mathcal{T}_N)$. Lemma 3 shows that if $\Phi \in \mathrm{Out}(\mathcal{T})$, then there is an element $\phi = (\phi_n)_{n\geq 1} \in \mathrm{Aut}(\mathcal{T})$ in the class Φ, such that each ϕ_n fixes the permutations of $B_n^{(\ell)}$. The same is obviously true when $\mathcal{T}$ is replaced by $\mathcal{T}_N$.

We can now state the main theorem of this article:

Main Theorem:
(i) $\mathrm{Out}(\mathcal{T}_3) \simeq GT_{\ell,0}$ and $\mathrm{Aut}(\hat{\mathcal{T}}_3) \simeq \widehat{GT}_0$;
(ii) $GT_\ell \simeq \mathrm{Out}(\mathcal{T}_4)$ and $\widehat{GT} \simeq \mathrm{Aut}(\hat{\mathcal{T}}_4)$;
(iii) $GT_\ell \simeq \mathrm{Out}(\mathcal{T}) \simeq \mathrm{Out}(\mathcal{T}_N)$ and $\widehat{GT} \simeq \mathrm{Aut}(\hat{\mathcal{T}}) \simeq \mathrm{Aut}(\hat{\mathcal{T}}_N)$ for $N > 4$.

Remark: In reference [I3] Ihara proves a result in the context of graded Lie algebras which, upon tensoring with $\mathbb{Q}_\ell$ (over $\mathbb{Q}$), is analogous to an "infinitesimal version" of the above theorem in the pro-ℓ case, namely a stability property of a certain Lie tower after the first two levels.

Before proving the theorem in §§3 to 6, let us give the basic underlying correspondence between elements of $\widehat{GT}$ and automorphisms of profinite completions of braid groups, due to Drinfel'd (and which also works for GT_ℓ and $B_n^{(\ell)}$). For $n \geq 1$, there is a natural map from GT_ℓ (resp. $\widehat{GT}$) into $\mathrm{Aut}(B_n^{(\ell)})$ (resp. $\mathrm{Aut}(\hat{B}_n)$) given as follows: if $(\lambda, f) \in GT_\ell$ (resp. $\widehat{GT}$) and $\phi \in \mathrm{Aut}(B_n^{(\ell)})$ (resp. $\mathrm{Aut}(\hat{B}_n)$) is its image, then

$$\phi(\sigma_1) = \sigma_1^\lambda \text{ and } \phi(\sigma_i) = f(\sigma_i^2, y_i)\sigma_i^\lambda f(y_i, \sigma_i^2) \text{ for } 2 \leq i \leq n-1. \tag{5}$$

Notice that although σ_1 has been singled out for convenience, it is in fact no exception to the rule: indeed, since f is in the *derived* group $[\hat{F}_2, \hat{F}_2]$, it satisfies $f(y_1, \sigma_1^2) = f(1, \sigma_1^2) = 1$.

The proof of the theorem consists in showing that the ϕ associated to couples (λ, f) are actually automorphisms of the $B_n^{(\ell)}$ (resp. the $\hat{B}_n$); (Drinfel'd shows this for the "k-pro-unipotent completions" of the B_n but his proof uses his tensor-categorical construction of the group GT; thus we prefer to reprove it in our cases by purely group-theoretic methods), that they respect the natural inclusion maps i_n (resp. the maps i_n, f_n and g_n), and that all outer automorphisms of $\mathcal{T}$ resp. $\hat{\mathcal{T}}$ come from such couples (λ, f).

§3. $GT_{\ell,0}$ and $\widehat{GT}_0$ as automorphism groups of $\mathcal{T}_3$ and $\hat{\mathcal{T}}_3$

In this section we prove (i) of the main theorem.

Proposition 4: $GT_{\ell,0} \simeq \mathrm{Out}(\mathcal{T}_3)$.

Proof: We begin by defining a homomorphism of $GT_{\ell,0}$ into $\mathrm{Aut}(\mathcal{T}_3)$. Let $(\lambda, f) \in GT_{\ell,0}$; we associate to it the map ϕ_3 defined by (5) on the generators of $B_3^{(\ell)}$, namely as $\phi_3(\sigma_1) = \sigma_1^\lambda$ and $\phi_3(\sigma_2) = f(\sigma_2^2, \sigma_1^2)\sigma_2^\lambda f(\sigma_1^2, \sigma_2^2)$. Let us show first that ϕ_3 can be extended multiplicatively to an automorphism of $B_3^{(\ell)}$. Set $\omega_3 = (\sigma_1\sigma_2)^3$; this element generates the center of $B_3^{(\ell)}$. Set $x = \sigma_1^2$, $y = \sigma_2^2$, $z' = \sigma_1\sigma_2^2\sigma_1^{-1}$ and $z = z'\omega_3^{-1}$: we have $xyz = 1$ in $B_3^{(\ell)}$. As mentioned above, K_3^ℓ is isomorphic to $\langle \omega_3 \rangle \times \langle x, y \rangle$, the group $\langle x, y \rangle$ being isomorphic to F_2^ℓ, so that an element $f \in F_2^\ell$ is entirely determined if we know $f(x, y) \in B_3^{(\ell)}$.

Note now that $\sigma_1 y = z'\sigma_1$ and $y\sigma_2 = \sigma_2 z'$, which gives the two following conjugation relations:

(a) $\sigma_1 f(y, x) = f(z, x)\sigma_1$, and

(b) $f(x, y)\sigma_2 = \sigma_2 f(z, y)$.

We may (and have) replaced z' by z inside f because, more generally, if α, β and $\gamma \in B_3^{(\ell)}$ and γ commute with α and β, then $f(\gamma\alpha, \beta) = f(\alpha, \gamma\beta) = f(\alpha, \beta)$. This in turn comes from f being in the derived group $[F_2^\ell, F_2^\ell]$.

Lemma 5: *ϕ_3 can be extended multiplicatively to an automorphism of $B_3^{(\ell)}$.*

Proof: It suffices to show that ϕ respects the unique relation $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ of $B_3^{(\ell)}$. We calculate:

$$\phi(\sigma_1)\phi(\sigma_2)\phi(\sigma_1) = \sigma_1^\lambda f(y,x)\sigma_2^\lambda f(x,y)\sigma_1^\lambda = \sigma_1^\lambda f(y,x)\sigma_2 y^m f(x,y) x^m \sigma_1$$

$$= \sigma_1^\lambda f(y,x)\sigma_2 f(z,y) z^{-m} f(x,z)\sigma_1 \text{ (since } \phi \text{ satisfies relation (II))}$$

$$= \sigma_1^\lambda f(y,x) f(x,y)\sigma_2 z^{-m}\sigma_1 f(x,y) \text{ (by (a) and (b) above)}$$

$$= \sigma_1^\lambda \sigma_2 z^{-m}\sigma_1 f(x,y) = \sigma_1^\lambda\sigma_2\sigma_1\sigma_2^{-2m}\omega_3^m f(x,y)$$

$$= x^m(\sigma_1\sigma_2\sigma_1)y^{-m}\omega_3^m f(x,y) = (\sigma_1\sigma_2\sigma_1)\omega_3^m f(x,y)$$

$$\text{(since } (\sigma_1\sigma_2\sigma_1)^{-1}x^k(\sigma_1\sigma_2\sigma_1) = y^k \text{ for all } k)$$

$$= (\sigma_2\sigma_1\sigma_2)\omega_3^m f(x,y) = \sigma_2\sigma_1\sigma_2^{-2m}\omega_3^m\sigma_2^\lambda f(x,y) = \sigma_2 z^{-m}\sigma_1\sigma_2^\lambda f(x,y)$$

$$= f(y,x)f(x,y)\sigma_2 z^{-m}\sigma_1\sigma_2^\lambda f(x,y) = f(y,x)\sigma_2 f(z,y) z^{-m}\sigma_1\sigma_2^\lambda f(x,y)$$

$$= f(y,x)\sigma_2 f(z,y) z^{-m} f(x,z) f(z,x)\sigma_1\sigma_2^\lambda f(x,y)$$

$$= f(y,x)\sigma_2 y^m f(x,y) x^m \sigma_1 f(y,x)\sigma_2^\lambda f(x,y) \text{ (by (a) and (II))}$$

$$= f(y,x)\sigma_2^\lambda f(x,y)\sigma_1^\lambda f(y,x)\sigma_2^\lambda f(x,y) = \phi(\sigma_2)\phi(\sigma_1)\phi(\sigma_2).$$

◇

Set $\phi_1 = \mathrm{id}$ and define ϕ_2 on $B_2^{(\ell)}$ by $\phi_2(\sigma_1) = \sigma_1^\lambda$. Clearly $i_n\phi_n = \phi_{n+1}i_n$ for $n = 1, 2$, so $(\phi_n)_{1 \le n \le 3} \in \mathrm{Aut}(\mathcal{T}_3)$.

We confirm using the multiplication law of $GT_{\ell,0}$ that the map $GT_{\ell,0}$ into $\mathrm{Aut}(\mathcal{T}_3)$ defined in this way is actually a group homomorphism which we denote by $\tilde{\eta}$. It induces a homomorphism of $GT_{\ell,0}$ into $\mathrm{Out}(\mathcal{T}_3)$ which we denote by η.

Let us show that η is injective. Let $(\lambda, f) \in GT_{\ell,0}$, be such that $\eta(\lambda, f) = 1$ and set $\phi = (\phi_n)_{1\le n\le 3} := \tilde{\eta}(\lambda, f)$. Then there exists $\delta \in \mathbb{Z}_\ell$ such that $\phi_3 = \mathrm{Inn}(\sigma_1^\delta)$. We then have $\phi_3(\sigma_1) = \sigma_1$ so $\lambda = 1$. Moreover we have

$$\phi_3(\sigma_2) = f(y,x)\sigma_2 f(x,y) = \sigma_1^{-\delta}\sigma_2^\lambda\sigma_1^\delta,$$

so we have an equality of the form

$$f(x,y) = C\sigma_1^\delta$$

where $C \in B_3^{(\ell)}$ commutes with σ_2.

Let us show that such a C has the form $\omega_3^\alpha\sigma_2^\gamma$ for α, $\gamma \in \mathbb{Z}_\ell$. We use the well-known fact that the centralizer of y in the free pro-ℓ group $\langle x, y\rangle$ is the cyclic group $\langle y\rangle$. This shows that the centralizer of the element σ_2^2 in the group K_3^ℓ is generated by ω_3 and σ_2^2 since $K_3 \simeq \langle\sigma_1^2, \sigma_2^2\rangle \times \langle\omega_3\rangle$ and $\langle\sigma_1^2, \sigma_2^2\rangle$ is a free group. Now consider an element $C \in B_3^{(\ell)}$ which centralizes σ_2. Since $\rho(C)$ must centralize $\rho(\sigma_2)$ in S_3, $\rho(C)$ must be either trivial or equal to $\rho(\sigma_2)$ (which is equal to the permutation (23)). If $\rho(C)$ is trivial then $C \in K_3^\ell$, and if C centralizes σ_2 then it centralizes σ_2^2, so it is in $\langle\sigma_2^2, \omega_3\rangle$. If $\rho(C) = \rho(\sigma_2)$, then C can be written $\sigma_2 C'$ where $C' \in K_3^\ell$, and C' must centralize σ_2 ...therefore it is again in $\langle\sigma_2^2, \omega_3\rangle$. This gives the result.

Now, $f(x,y) \in K_3^\ell$, so the expression $f(x,y) = \omega_3^\alpha\sigma_2^\gamma\sigma_1^\delta$ must be in K_3^ℓ as well, which implies that γ and δ are congruent to 0 mod 2. But then $\sigma_2^\gamma\sigma_1^\delta = y^{\gamma/2}x^{\delta/2} \in \langle x, y\rangle = F_2^\ell$, so $\alpha = 0$ since $\omega_3 \notin \langle x, y\rangle$. But then, since f is supposed to belong to $[F_2^\ell, F_2^\ell]$, we must have $\gamma = \delta = 0$ and thus $f = 1$, which gives the injectivity of η.

Let us show that η is surjective. Let $\Phi \in \mathrm{Out}(\mathcal{T}_3)$ and let $(\phi_n)_{1\le n\le 3} \in \mathrm{Aut}(\mathcal{T}_3)$ be a representative of Φ which fixes the permutations (as can always be chosen by lemma 3). Firstly, λ is determined by ϕ_2, and $\lambda \in \mathbb{Z}_\ell^*$ since ϕ_2 is invertible. Next, because ϕ_3 fixes the permutations, there exist $\alpha \in \mathbb{Z}_\ell$ and $g \in F_2^\ell$ such that $\phi_3(\sigma_1\sigma_2\sigma_1) = \sigma_1\sigma_2\sigma_1\omega_3^\alpha g(x,y)$. Applying ϕ_3 to the relation $(\sigma_1\sigma_2\sigma_1)^{-1}\sigma_1(\sigma_1\sigma_2\sigma_1) = \sigma_2$ in $B_3^{(\ell)}$, we obtain $\phi_3(\sigma_2) = g^{-1}(x,y)\sigma_2^\lambda g(x,y)$. Let γ, δ be the unique elements of $\mathbb{Z}_\ell$ such that $y^\gamma g(x,y)x^\delta \in [F_2^\ell, F_2^\ell]$ (where F_2^ℓ is identified with $\langle x, y\rangle$), and set $f(x,y) = y^\gamma g(x,y)x^\delta$. We thus associate a couple $(\lambda, f) \in \mathbb{Z}_\ell^* \times [F_2^\ell, F_2^\ell]$ to ϕ_3. (The automorphism of $B_3^{(\ell)}$ associated to this couple is actually $\mathrm{Inn}(x^\delta)\phi_3$, which is in the same class as ϕ_3 modulo $\mathrm{Inn}(\mathcal{T}_3)$). Let us show that this couple is in $GT_{\ell,0}$, i.e. that it satisfies relations (I) and (II).

Let $T := \mathrm{Inn}(\sigma_1\sigma_2\sigma_1)$ and $U := \mathrm{Inn}\big((\sigma_1\sigma_2)^2\big) \in \mathrm{Inn}(B_3^{(\ell)})$. Note that $T^2 = U^3 = 1$. Let us calculate $\mathrm{Inn}\big(f(y,x)^{-1}\big)T\phi_3T^{-1} \in \mathrm{Aut}(B_3^{(\ell)})$; under this automorphism we have

$$\sigma_1 \mapsto \sigma_1^\lambda \text{ and } \sigma_2 \mapsto f(y,x)\sigma_2^\lambda f(y,x)^{-1}.$$

As $f(y,x) \in [F_2^\ell, F_2^\ell]$, this automorphism is equal to $\tilde\eta\big(\lambda, f(y,x)^{-1}\big)$ and is thus in particular in $\mathrm{Aut}(\mathcal{T}_3)$.

Let us also calculate $\mathrm{Inn}(f(x,z))\ U\phi_3U^{-1}$ on σ_1 and σ_2; we obtain:

$$\sigma_1 \mapsto \sigma_1^\lambda \text{ and } \sigma_2 \mapsto f(x,z)^{-1}z^m f(z,y)^{-1}\sigma_2^\lambda f(z,y)z^{-m}f(x,z);$$

thus $\mathrm{Inn}(f(x,z))\ U\phi_3U^{-1}$ is equal to $\tilde\eta\big(\lambda, y^{-m}f(z,y)z^{-m}f(x,z)x^{-m}\big)$ modulo $\mathrm{Inn}(\mathcal{T}_3)$, where $z = (xy)^{-1} \in F_2^\ell$.

If we consider that $\mathrm{Aut}(\mathcal{T}_3) \subset \mathrm{Aut}(B_3^{(\ell)})$, then in fact $\mathrm{Out}(\mathcal{T}_3) \subset \mathrm{Out}(B_3^{(\ell)})$ since $\mathrm{Aut}(\mathcal{T}_3) \cap \mathrm{Inn}(B_3^{(\ell)}) = \mathrm{Inn}(\mathcal{T}_3)$. By the injectivity of $\eta : GT_{\ell,0} \to \mathrm{Out}(\mathcal{T}_3)$, we see that if (λ, f) and $(\mu, g) \in GT_{\ell,0}$ and the images of $\eta(\lambda, f)$ and of $\eta(\mu, g)$ are equal in $\mathrm{Out}(B_3^{(\ell)})$, then $\eta(\lambda, f) = \eta(\mu, g)$ in $\mathrm{Out}(\mathcal{T}_3^\ell)$. Thus we have $f(x,y) = f(y,x)^{-1}$ and $f(x,y) = y^{-m}f(z,y)z^{-m}f(x,z)x^{-m}$, so (λ, f) satisfies relations (I) and (II). By construction, $(\phi_n)_{1\le n\le 3}$ is in the class $\eta(\lambda, f)$ in $\mathrm{Out}(\mathcal{T}_3)$, so $\eta : GT_{\ell,0} \to \mathrm{Out}(\mathcal{T}_3)$ is a bijection. This concludes the proof of proposition 4. $\diamond$

Corollary: $\mathrm{Aut}(\hat{\mathcal{T}}_3) \simeq \widehat{GT}_0$.

Proof: Most of the calculations in the proof of proposition 4 work in the profinite case with no changes whatsoever. For the injectivity, we need to verify that every automorphism of $\hat B_3$ respecting the inclusions i_n as in the pro-ℓ situation also respects the other maps f_i and g_i. Thus let $\phi := (\phi_n)_{1\le n\le 3}$ be a triple of automorphisms respecting the i_n for $n = 1, 2$. Define ϕ'_1 to be the identity, ϕ'_2 by $\phi'_2(\sigma_1^2) = \sigma_1^{2\lambda}$ and ϕ'_3 to be the restriction of ϕ_3 to $\hat A_3 \subset \hat B_3$ (ϕ'_3 is easily seen to be an automorphism of $\hat A_3$). Then $\phi := (\phi_i, \phi'_i)_{1\le i\le 3}$ respects the maps i_1 and i_2 as in proposition 4, f_1 and f_2 by construction and g_1 by triviality. The relation $g_2\phi'_2 = \phi_3 g_2$ is a consequence of the fact that $\phi_3(y_3) = y_3^\lambda$ which is proved as follows. Recall that $\omega_3 = y_2y_3$; we know that $\phi_3(\omega_3) = \omega_3^\lambda$ since ϕ_3 must send ω_3 to a power of itself and this power must be exactly λ; (looking at the induced action of ϕ_3 modulo the derived subgroup of $\hat B_3$, i.e. in the free profinite abelian group on 2 generators, we see that $\sigma_1 \to \sigma_1^\lambda$ and $\sigma_2 \to \sigma_2^\lambda$), we also know that y_2 and y_3 commute and that $\phi_3(y_2) = y_2^\lambda$ since $y_2 = \sigma_1^2$, which suffices to show that $\phi_3(y_3) = y_3^\lambda$. (The same argument actually shows that if ϕ_n is any automorphism of $\hat B_n$ such that $\phi_n(\hat B_m) = \hat B_m$ for all

$m < n$, then $\phi_n(y_i) = y_i^\lambda$ for $1 \le i \le n$.) This shows that $(\phi_n, \phi'_n)_{1\le n\le 3} \in \mathrm{Aut}(\hat{\mathcal{T}}_3)$ and thus that the map given by equation (5) does determine an injective map $\widehat{GT}_0 \to \mathrm{Aut}(\hat{\mathcal{T}}_3)$. The surjectivity argument is easier than in the pro-ℓ case. There is no need to take a representative of an outer automorphism. Moreover the element δ introduced in order to ensure that $f(x,y)$ be in the derived group is necessarily 0 since as shown in the pro-ℓ case, $(\mathrm{Inn}(x^\delta)\phi_n)_{1\le n\le 3}$ defines an element of $\mathrm{Aut}(\hat{\mathcal{T}}_3)$, however no non-zero power of x can preserve the subgroup $\hat{A}_3 \subset \hat{B}_3$. The rest of the proof of surjectivity goes through as in the pro-ℓ case. $\diamondsuit$

§4. $\widehat{GT}$ and GT_ℓ as automorphism groups of the braid towers $\hat{\mathcal{T}}_4$ and $\mathcal{T}_4$

In this section we prove statement (ii) of the main theorem, working first in the profinite setting and stating the straightforward adaptation to the pro-ℓ case as a corollary. As the proof is somewhat involved and depends on an unexpected introduction of the mapping class group $M(0,5)$, we give a brief description of its logical structure here. The usefulness of $M(0,5)$ (and its profinite completion) lies in the existence of a torsion element of order 5 which gives rise to the pentagon equation in a natural way. The Artin braid group B_4 is not contained in $M(0,5)$, but the quotient by the center B_4/Z is a subgroup of $M(0,5)$.

In lemma 7 (and lemma 8) we show the following result. We take a certain generating set of elements for $\widehat{M(0,5)}$, namely $\bar\sigma_1$, $\bar\sigma_2$, $\bar\sigma_3$, $\bar\sigma_4$ and $\bar\sigma_{15}$ (see the beginning of the proof of proposition 6). We let couples $(\lambda, f) \in \widehat{GT}_0$ act on this generating set in a particular way and show that this action extends to an automorphism of $\widehat{M(0,5)}$ if and only if the couple actually lies in $\widehat{GT}$. We obtain an (injective) map $\tilde\iota : \widehat{GT} \to \mathrm{Aut}(\widehat{M(0,5)})$.

In lemma 9 it is shown that the automorphisms of $\widehat{M(0,5)}$ coming from elements of $\widehat{GT}$ restrict to automorphisms of the subgroup $\hat{B}_4/Z$ and lift uniquely to automorphisms of $\hat{B}_4$ which respect the arrows of the tower $\hat{\mathcal{T}}_4$; we thus obtain an (injective) map $\iota : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}}_4)$.

In order to show the surjectivity of this map we proceed as follows. Suppose $\Phi = (\phi_n)_{1\le n\le 4} \in \mathrm{Aut}(\hat{\mathcal{T}}_4)$; then, because Φ must respect the homomorphisms i_n, f_n and g_n for $1 \le n \le 3$, we have

$$\phi_4(\sigma_1) = \sigma_1^\lambda, \quad \phi_4(\sigma_2) = f(x_{23}, x_{12})\sigma_2^\lambda f(x_{12}, x_{23}),$$
$$\text{and } \phi_4(\sigma_3) = f(\sigma_3^2, y_3)\sigma_3^\lambda f(y_3, \sigma_3^2).$$

Now, any automorphism ϕ_4 of $\hat{B}_4$ which acts on σ_1, σ_2 and σ_3 in this way induces an automorphism of $\hat{B}_4/Z$; moreover if (λ, f) is the couple in $\widehat{GT}_0$ associated to ϕ_3 and a map ϕ corresponding to (λ, f) is defined on the generating set of $\widehat{M(0,5)}$ as in lemma 7, then ϕ restricted to the subgroup $\hat{B}_4/Z$ gives an automorphism of this subgroup since it is precisely the one induced by ϕ_4. We show that any ϕ defined on the generating set as in lemma 7 which induces an automorphism of the subgroup $\hat{B}_4/Z$ automatically extends to an automorphism of all of $\widehat{M(0,5)}$; by lemma 7 the couple (λ, f) must then lie in $\widehat{GT}$, so $\Phi = \iota(\lambda, f)$. This shows that ι is a bijection.

Proposition 6: $\widehat{GT} \simeq \mathrm{Aut}(\hat{\mathcal{T}}_4)$.

Proof: Let $M(0,5)$ be the mapping class group in genus 0 with 5 marked points; this group is generated by elements σ_1, σ_2, σ_3 and σ_4 – please note! in order to avoid immensely long lines over all the formulae we do *not* put bars over the elements of $M(0,5)$ as we should, throughout the whole of this section, *except* in lemma 9 in which it is necessary to distinguish between elements of $\hat{B}_4$ and their images in $\hat{B}_4/Z \subset \widehat{M(0,5)}$. We introduce $\sigma_{15} := \sigma_4\sigma_3\sigma_2\sigma_1\sigma_2^{-1}\sigma_3^{-1}\sigma_4^{-1}$ as in proposition 1 (so $\sigma_{15}^2 = x_{15}$).

Set $V := \mathrm{Inn}\big((\sigma_4\sigma_3\sigma_2\sigma_1)^{-3}\big) \in \mathrm{Inn}\big(\widehat{M(0,5)}\big)$, so $V^5 = 1$. The map V acts as follows on the σ_i's, σ_{15}, and the x_{ij}'s:

$$V(\sigma_1) = \sigma_3,\ V(\sigma_2) = \sigma_4,\ V(\sigma_3) = \sigma_{15},\ V(\sigma_4) = \sigma_1,\ V(\sigma_{15}) = \sigma_2, \tag{6}$$

$$V(x_{ij}) = x_{i+2,j+2}, \qquad \text{for } i, j \in \mathbb{Z}/5\mathbb{Z}.$$

These properties could be expressed more concisely as $V(\sigma_{i,i+1}) = \sigma_{i+2,i+3}$ for all $i \in \mathbb{Z}/5\mathbb{Z}$.

We shall make use of a more symmetric form of relation (III), which holds in $\widehat{M(0,5)}$. Namely, considering the x_{ij}'s as elements of $\widehat{M(0,5)}$, relation (III) implies the following:

$$(\mathrm{III}') \quad f(x_{34}, x_{45})f(x_{51}, x_{12})f(x_{23}, x_{34})f(x_{45}, x_{51})f(x_{12}, x_{23}) = 1$$

This form of relation (III) was given by Ihara in [I1]: as he points out, to transform (III) into (III'), one uses relation (I), the relations (4) of §2 and the remarks just preceding lemma 5. We shall write this relation as $f_5f_4f_3f_2f_1 = 1$. Note that

$$f_1 = f(x_{12}, x_{23}), \quad f_{i+1} = V^{-1}(f_i) \qquad \text{for } \ i \in \mathbb{Z}/5\mathbb{Z}.$$

Lemma 7: *Let* $(\lambda, f) \in \widehat{GT}_0$ *and associate to it a map* ϕ *sending* σ_1, σ_2, σ_3, σ_4 *and* σ_{15} *into* $\widehat{M(0,5)}$ *as follows:*

$$\phi(\sigma_1) = \sigma_1^{\lambda}, \quad \phi(\sigma_2) = f(x_{23}, x_{12})\sigma_2^{\lambda}f(x_{12}, x_{23}),$$

$$\phi(\sigma_3)=f(x_{34},x_{45})\sigma_3^\lambda f(x_{45},x_{34}),\ \ \phi(\sigma_4)=\sigma_4^\lambda,$$

$$\phi(\sigma_{15})=f(x_{23},x_{12})f(x_{51},x_{45})\sigma_{15}^\lambda f(x_{45},x_{51})f(x_{12},x_{23}).$$

Then ϕ can be extended multiplicatively to an automorphism of $\widehat{M(0,5)}$ if and only if (λ,f) lies in $\widehat{GT}$; this map defines an injective group homomorphism which we denote by $\tilde\imath:\widehat{GT}\to\mathrm{Aut}(\widehat{M(0,5)})$.

Remark: This action of $\widehat{GT}$ on $\widehat{M(0,5)}$ is determined by considering $\widehat{M(0,5)}$ as a quotient of $\hat B_5$ and looking at the images of the right-hand sides of equation (5) in the quotient. The idea of passing from $\hat B_5$ to $\widehat{M(0,5)}$ in this way is also employed by Nakamura in the appendix of [N].

Proof: Suppose ϕ is associated to a couple $(\lambda,f)\in\widehat{GT}_0$. We must study when ϕ respects the relations defining $\widehat{M(0,5)}$, namely those of $\hat B_5$ and the sphere and center relations $y_5=\omega_5=1$ (cf. §2). Remark first that the subgroup of $\widehat{M(0,5)}$ generated by σ_1 and σ_2 being isomorphic to $\hat B_3$, we know by proposition 4 that ϕ induces an automorphism of this group and thus that ϕ respects the relation $\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2$. For the other relations we use the following lemma:

Lemma 8: *Let ϕ act on σ_1, σ_2, σ_3, σ_4 and σ_{15} as in lemma 7. Then*

(i) the two maps ϕV and $V\,\mathrm{Inn}(f_1^{-1})\phi$ take the same values when applied to the elements σ_1, σ_2, σ_4 and σ_{15}, and

(ii) the two maps ϕV^3 and $V^3\,\mathrm{Inn}(f_1^{-1}f_2^{-1}f_3^{-1})\phi$ take the same values on σ_1 and σ_2 if (λ,f) lies in $\widehat{GT}$.

Proof: (i) It suffices to calculate $\mathrm{Inn}(f_1)V^{-1}\phi V$ on the given elements using (6). The calculations are all trivial, so we do it for σ_1 only: $\phi V(\sigma_1)=\phi(\sigma_3)=f_5\sigma_3^\lambda f_5^{-1}=V\big(f_1\sigma_1^\lambda f_1^{-1}\big)=V\,\mathrm{Inn}(f_1^{-1})\phi(\sigma_1)$.

(ii) Assume that f satisfies relation (III'), i.e. $f_5f_4f_3f_2f_1=1$, and let us do the calculation. By (III'), $f_1^{-1}f_2^{-1}f_3^{-1}=f_5f_4$. Thus we have: $\phi V^3(\sigma_1)=\phi(\sigma_2)=f_1^{-1}\sigma_2^\lambda f_1$ and $V^3\mathrm{Inn}(f_5f_4)\phi(\sigma_1)=V^3\big(f_4^{-1}f_5^{-1}\sigma_1^\lambda f_5f_4\big)$ $=f_1^{-1}f_2^{-1}\sigma_2^\lambda f_2f_1=f_1^{-1}\sigma_2^\lambda f_1$ since $f_2=f(x_{45},x_{51})$ commutes with σ_2. Moreover, we have $\phi V^3(\sigma_2)=\phi(\sigma_3)=f_5\sigma_3^\lambda f_5^{-1}$ and $V^3\mathrm{Inn}(f_5f_4)\phi(\sigma_2)=$ $V^3\big(f_4^{-1}f_5^{-1}f_1^{-1}\sigma_2^\lambda f_1f_5f_4\big)=V^3\big(f_3f_2\sigma_2^\lambda f_2^{-1}f_3^{-1}\big)=f_5f_4\sigma_3^\lambda f_4^{-1}f_5^{-1}=$ $f_5\sigma_3^\lambda f_5^{-1}$ since $f_4=f(x_{51},x_{12})$ commutes with σ_3. ◊

We use lemma 8 to determine when ϕ extends to an automorphism of $\widehat{M(0,5)}$, i.e. respects the defining relations (besides $\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2$, which is respected by the assumption that (λ,f) lies in $\widehat{GT}_0$):

(a) $\sigma_3\sigma_4\sigma_3=\sigma_4\sigma_3\sigma_4$,

(b) the sphere relation $y_5 = \sigma_4\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_4 = 1$,

(c) the center relation $\omega_5 = (\sigma_1\sigma_2\sigma_3\sigma_4)^5 = 1$,

(d) the remaining relation $\sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3$.

It turns out that (a), (b) and (c) are all respected when ϕ is associated to any couple $(\lambda, f) \in \widehat{GT}_0$, for we only need to use lemma 8 (i) (and indeed, the equality of the two given maps on the elements σ_1 and σ_2). Relation (a) is proved by the following argument using the equality of the maps ϕV and $V\,\mathrm{Inn}(f_1^{-1})\phi$ applied to σ_1 and σ_2:

$$\phi(\sigma_3)\phi(\sigma_4)\phi(\sigma_3) = (\phi V)(\sigma_1)(\phi V)(\sigma_2)(\phi V)(\sigma_1)$$

$$= (V\,\mathrm{Inn}(f_1^{-1})\phi)(\sigma_1)(V\,\mathrm{Inn}(f_1^{-1})\phi)(\sigma_2)(V\,\mathrm{Inn}(f_1^{-1})\phi)(\sigma_1)$$

$$= \big(V\,\mathrm{Inn}(f_1^{-1})\big)\big(\phi(\sigma_1)\phi(\sigma_2)\phi(\sigma_1)\big)$$

$$= \big(V\,\mathrm{Inn}(f_1^{-1})\big)\big(\phi(\sigma_2)\phi(\sigma_1)\phi(\sigma_2)\big) = \phi(\sigma_4)\phi(\sigma_3)\phi(\sigma_4).$$

Let us show that lemma 8 (i) implies that ϕ respects relation (b), $\sigma_4\sigma_3\sigma_2\sigma_1^2$ $\sigma_2\sigma_3\sigma_4 = 1$, which we rewrite as $(\sigma_2\sigma_1^2\sigma_2)^{-1} = \sigma_3\sigma_4^2\sigma_3$. Here we need to use the fact that ϕ is an automorphism when restricted to $\langle\sigma_1, \sigma_2\rangle$ (since the couple (λ, f) is assumed to lie in $\widehat{GT}_0$), and that $\phi(\sigma_2\sigma_1^2\sigma_2) = (\sigma_2\sigma_1^2\sigma_2)^\lambda$, which is proved as in the proof of the corollary to proposition 4 since $\sigma_2\sigma_1^2\sigma_2 = y_3$. We have:

$$\phi(\sigma_3)\phi(\sigma_4)^2\phi(\sigma_3) = (\phi V)(\sigma_1)(\phi V)(\sigma_2)^2(\phi V)(\sigma_1) = V\,\mathrm{Inn}(f_1^{-1})\phi(\sigma_1\sigma_2^2\sigma_1)$$

$$= V\Big(f(x_{12}, x_{23})(\sigma_1\sigma_2^2\sigma_1)^\lambda f(x_{23}, x_{12})\Big) = f(x_{34}, x_{45})(\sigma_3\sigma_4^2\sigma_3)^\lambda f(x_{45}, x_{34})$$

$$= f(x_{34}, x_{45})(\sigma_2\sigma_1^2\sigma_2)^{-\lambda} f(x_{45}, x_{34}) = (\sigma_2\sigma_1^2\sigma_2)^{-\lambda} = \phi(\sigma_2\sigma_1^2\sigma_2)^{-1}.$$

Similarly, lemma 8 (i) suffices to show that ϕ respects relation (c). We work with the equivalent relation $\sigma_1^2\sigma_2\sigma_1^2\sigma_2\sigma_4^{-2} = 1$ (the left-hand side is equal to $(\sigma_1\sigma_2\sigma_3\sigma_4)^5$ in $\widehat{M(0,5)}$). As the three elements σ_1^2, $\sigma_2\sigma_1^2\sigma_2$ and σ_4^2 commute and ϕ takes each one to itself to the power λ, it is immediate that ϕ respects this relation.

Let us now show that ϕ extends to an automorphism of $\widehat{M(0,5)}$ if and only if (λ, f) lies in $\widehat{GT}$. First suppose that $(\lambda, f) \in \widehat{GT}$. We only need to show that ϕ respects (d), which we do using lemma 8 (ii), which tells us that when (λ, f) lies in $\widehat{GT}$, the maps ϕ and $\mathrm{Inn}(f_3f_2f_1)V^{-3}\phi V^3$ take the same values on σ_1 and σ_2. Thus we calculate

$$\phi(\sigma_2)\phi(\sigma_3)\phi(\sigma_2) = (\phi V^3)(\sigma_1)(\phi V^3)(\sigma_2)(\phi V^3)(\sigma_1) =$$

$$(V^3\mathrm{Inn}(f_3f_2f_1)^{-1}\phi)(\sigma_1)(V^3\mathrm{Inn}(f_3f_2f_1)^{-1}\phi)(\sigma_2)(V^3\mathrm{Inn}(f_3f_2f_1)^{-1}\phi)(\sigma_1)$$
$$= \bigl(V^3\mathrm{Inn}(f_3f_2f_1)^{-1}\bigr)\Bigl(\phi(\sigma_1)\phi(\sigma_2)\phi(\sigma_1)\Bigr)$$
$$= \bigl(V^3\mathrm{Inn}(f_3f_2f_1)^{-1}\bigr)\Bigl(\phi(\sigma_2)\phi(\sigma_1)\phi(\sigma_2)\Bigr) = \phi(\sigma_3)\phi(\sigma_2)\phi(\sigma_3),$$

which shows that (d) is respected by ϕ, so ϕ extends to an automorphism of $\widehat{M(0,5)}$ if it is associated to a couple $(\lambda, f) \in \widehat{GT}$.

Now let us show that if a couple $(\lambda, f) \in \widehat{GT}_0$, acting as in the statement of lemma 7, extends to an automorphism of $\widehat{M(0,5)}$ then it must lie in $\widehat{GT}$. This is most simply done by adapting an argument of Nakamura (see the appendix of [N]). By lemma 8 (i), since σ_1, σ_2, σ_4 and σ_{15} generate all of $\widehat{M(0,5)}$, if we assume that ϕ is an automorphism then we must have the equality $\phi = \mathrm{Inn}(f_1)V^{-1}\phi V$ on all of $\widehat{M(0,5)}$. Replacing ϕ by $\mathrm{Inn}(f_1)V^{-1}\phi V$ in the right-hand side gives $\phi = \mathrm{Inn}(f_2f_1)V^{-2}\phi V$; reiterating three more times gives $\phi =$

$$\mathrm{Inn}(f_3f_2f_1)V^{-3}\phi V^3 = \mathrm{Inn}(f_4f_3f_2f_1)V^{-4}\phi V^4 = \mathrm{Inn}(f_5f_4f_3f_2f_1)V^{-5}\phi V^5.$$

Since $V_5 = 1$, we have $\phi = \mathrm{Inn}(f_5f_4f_3f_2f_1)\phi$, so the element $f_5f_4f_3f_2f_1$ must be in the center of $\widehat{M(0,5)}$, which is trivial. But this element is exactly the left-hand side of relation (III').

We thus associate to every $(\lambda, f) \in \widehat{GT}$ an automorphism of $\widehat{M(0,5)}$; by the multiplication law, we see that this map of $\widehat{GT}$ into $\mathrm{Aut}(\widehat{M(0,5)})$, which we denote by $\tilde{\iota}$, is a group homomorphism. Restriction to the subgroup $\langle\sigma_1, \sigma_2\rangle$ of $\widehat{M(0,5)}$, gives the injective map $\tilde{\eta} : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}}_3) \subset \mathrm{Aut}(\hat{B}_3)$ of proposition 4, which shows that $\tilde{\iota} : \widehat{GT} \to \mathrm{Aut}(\widehat{M(0,5)})$ is also injective. This concludes the proof of lemma 7. $\diamond$

As before, for any group G, we write (by a slight abuse of notation) G/Z for G modulo its center. We have already remarked that the subgroup of $\widehat{M(0,5)}$ generated by σ_1 and σ_2 is isomorphic to $\hat{B}_3$, and similarly, the subgroup generated by σ_1, σ_2 and σ_3 inside $\widehat{M(0,5)}$ is isomorphic, not to $\hat{B}_4$, but to $\hat{B}_4/Z$ (since the relation $(\sigma_1\sigma_2\sigma_3)^4 = 1$ holds in $\widehat{M(0,5)}$ and this element generates the center of $\hat{B}_4$). It is immediate that if ϕ is the automorphism of $\widehat{M(0,5)}$ associated to a couple $(\lambda, f) \in \widehat{GT}$ as in lemma 7, then ϕ induces an automorphism of $\hat{B}_4$ since ϕ preserves this subgroup of $\widehat{M(0,5)}$, thanks to the first of relations (4) in §2. The map $\tilde{\iota} : \widehat{GT} \to \mathrm{Aut}(\widehat{M(0,5)})$ of lemma 7 thus induces an injective map $\tilde{\iota} : \widehat{GT} \to \mathrm{Aut}(\hat{B}_4/Z)$.

Lemma 9: *The map $\tilde{\iota}$ induces an injective map $\iota:\widehat{GT}\rightarrow \mathrm{Aut}(\hat{\mathcal{T}}_4)$.*

Proof: Let $(\lambda,f)\in\widehat{GT}$ and let $\phi:=\tilde{\iota}(\lambda,f)\in \mathrm{Aut}(\hat{B}_4/Z)$. In the proof of this lemma, let σ_i and x_{ij} denote elements of $\hat{B}_4$, not to be confused with the elements of $\hat{B}_4/Z\subset\widehat{M(0,5)}$ (which ought to have been denoted $\bar{\sigma}_i$ and $\bar{x}_{ij}$ but were not for aesthetic reasons). The $\bar{\sigma}_i$ satisfy the relation $(\bar{\sigma}_1\bar{\sigma}_2\bar{\sigma}_3)^4=1$, and this is of course not true of the σ_i; indeed $\omega_4=(\sigma_1\sigma_2\sigma_3)^4$ generates the infinite cyclic center of $\hat{B}_4$. Let us associate to ϕ an element $\tilde{\phi}$ of $\mathrm{Aut}(\hat{\mathcal{T}}_4)$. Define $\tilde{\phi}$ on the generators σ_1, σ_2 and σ_3 of $\hat{B}_4$ by

$$\tilde{\phi}(\sigma_1)=\sigma_1^{\lambda},\ \ \tilde{\phi}(\sigma_2)=f(x_{23},x_{12})\sigma_2^{\lambda}f(x_{12},x_{23}),\ \tilde{\phi}(\sigma_3)$$
$$=f(x_{34},x_{45})\sigma_3^{\lambda}f(x_{45},x_{34});$$

here, we write $x_{45}:=x_{12}x_{13}x_{23}$ in order to consider x_{45} as an element of $\hat{B}_4$, but it is to be considered purely as a formal notation. We first show that $\tilde{\phi}$ induces an automorphism of $\hat{B}_4$. By proposition 4, it induces one on the subgroup of $\hat{B}_4$ generated by $\langle\sigma_1,\sigma_2\rangle$ since this subgroup is isomorphic to $\hat{B}_3$. Thus $\tilde{\phi}$ respects the relation $\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2$ which holds in $\hat{B}_4$. Since ϕ is an automorphism of $\hat{B}_4/Z$, we know that $\tilde{\phi}$ respects the relation $\sigma_2\sigma_3\sigma_2=\sigma_3\sigma_2\sigma_3$ modulo the center of $\hat{B}_4$, which means that there exists $\mu\in\mathbb{Z}^*$ such that

$$\tilde{\phi}(\sigma_2)\tilde{\phi}(\sigma_3)\tilde{\phi}(\sigma_2)=\tilde{\phi}(\sigma_3)\tilde{\phi}(\sigma_2)\tilde{\phi}(\sigma_3)\omega_4^{\mu}.$$

Define a map $\tilde{\phi}'$ on σ_1, σ_2 and σ_3 as follows: $\tilde{\phi}'(\sigma_1)=\tilde{\phi}(\sigma_1)$, $\tilde{\phi}'(\sigma_2)=\tilde{\phi}(\sigma_2)$, and $\tilde{\phi}'(\sigma_3)=\tilde{\phi}(\sigma_3)\omega_4^{-\mu}$. Then it is immediate that $\tilde{\phi}'$ respects the two relations defining $\hat{B}_4$, so it is an automorphism of $\hat{B}_4$. This automorphism clearly sends the derived subgroup of $\hat{B}_4$ into itself (since it induces an automorphism on the quotient, i.e. on the free profinite abelian group on three generators, namely sending each generator to itself to the power λ), and modulo this subgroup, σ_1, σ_2 and σ_3 become equal, which shows that μ must be equal to 0 (since the center of $\hat{B}_4$ does not intersect the commutator subgroup). Thus $\tilde{\phi}'=\tilde{\phi}$, and we have lifted $\phi\in\mathrm{Aut}(\hat{B}_4/Z)$ to $\tilde{\phi}\in\mathrm{Aut}(\hat{B}_4)$. This lifting map is clearly injective, and a simple calculation confirms that $\tilde{\phi}$ is in $\mathrm{Aut}(\hat{\mathcal{T}}_4)$, i.e. that it respects all the homomorphisms i_n, f_n and g_n for $1\le n\le 3$. So we have an injective map $\iota:\widehat{GT}\rightarrow\mathrm{Aut}(\hat{\mathcal{T}}_4)$. $\diamond$

In order to finish the proof of proposition 6, it remains only to prove the surjectivity of ι. Take an element $\Phi=(\phi_n)_{1\le n\le 4}$ in $\mathrm{Aut}(\hat{\mathcal{T}}_4)$. We know by proposition 4 that the couple (λ,f) determined by ϕ_3 is in $\widehat{GT}_0$. By the relation $\phi_4 i_3=i_3\phi_3$ we see that

$$\phi_4(\sigma_1)=\sigma_1^{\lambda},\ \text{and}\ \phi_4(\sigma_2)=f(x_{23},x_{12})\sigma_2^{\lambda}f(x_{12},x_{23}).$$

By the commutation $\phi_4 g_3 = g_3\phi_3$ we compute that

$$\phi_4(\sigma_3) = \phi_4 g_3(\sigma_2) = g_3\phi_3(\sigma_2) = g_3\big(f(x_{23},x_{12})\sigma_2^\lambda f(x_{12},x_{23})\big)$$
$$= f(x_{34},x_{45})\sigma_3^\lambda f(x_{45},x_{34}).$$

Let ϕ be the map associated to $(\lambda,f)\in\widehat{GT}_0$ given in the statement of lemma 7, defined on the generating set of $\widehat{M(0,5)}$ considered there. Consider ϕ restricted to the subgroup $\hat{B}_4/Z\subset\widehat{M(0,5)}$; it agrees with the automorphism of $\hat{B}_4/Z$ induced by ϕ_4, so it is an automorphism of this subgroup. We will show that this implies that ϕ actually gives an automorphism of all of $\widehat{M(0,5)}$, which in turn shows by lemma 7 that the couple (λ,f) must lie in $\widehat{GT}$. We must verify that ϕ respects the defining relations of $\widehat{M(0,5)}$. Since ϕ is an automorphism of $\hat{B}_4/Z$, it respects $\sigma_1\sigma_2\sigma_1=\sigma_2\sigma_1\sigma_2$, $\sigma_2\sigma_3\sigma_2=\sigma_3\sigma_2\sigma_3$ and $(\sigma_1\sigma_2\sigma_3)^4=1$ (this last relation is well-known to be equivalent to the center relation $(\sigma_1\sigma_2\sigma_3\sigma_4)^5=1$, cf. [Bi]). The relation $\sigma_3\sigma_4\sigma_3=\sigma_4\sigma_3\sigma_4$ and the Hurwitz relation $\sigma_4\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_4$ are respected simply because ϕ satisfies the conditions of lemma 8 (i), as in the proof of lemma 7; these two relations are respected by ϕ's associated to any couple in $\widehat{GT}_0$. Therefore ϕ is an automorphism of $\widehat{M(0,5)}$ and thus by lemma 7 (λ,f) lies in $\widehat{GT}$, so $\Phi=\iota(\lambda,f)$ and ι is a bijection. This concludes the proof of proposition 6. $\diamond$

Corollary: $\mathrm{Out}(\mathcal{T}_4)\simeq GT_\ell$.

Proof: Much as in the last section, this is really a corollary of the proof of proposition 6, which carries over to the pro-ℓ case. Specifically, note that the statement and proof of lemma 7 are entirely valid when $\widehat{M(0,5)}$ is replaced by $M(0,5)^{(\ell)}$. This shows that if $(\lambda,f)\in GT_\ell$ then it induces an automorphism of $B_4^{(\ell)}/Z$ which is easily seen to lift to one of $B_4^{(\ell)}$ as in the profinite case. Conversely, if ϕ_4 is an automorphism of $B_4^{(\ell)}$ which acts on σ_1, σ_2 and σ_3 as in equation (5), it induces one of $B_4^{(\ell)}/Z\subset M(0,5)^{(\ell)}$ which extends uniquely to one of $M(0,5)^{(\ell)}$ as in the proof of lemma 9, so the couple (λ,f) must belong to GT_ℓ. If ϕ_4 is associated to $(\lambda,f)\in GT_\ell$, it is immediate that defining ϕ_n for $1\le n\le 3$ as the restrictions of ϕ_4 to $B_n^{(\ell)}\subset B_4^{(\ell)}$ we obtain a map $GT_\ell\to\mathrm{Aut}(\mathcal{T}_4)$ which is injective because its kernel must be contained in the kernel of the injective map $\tilde{\eta}$ defined in §3. To prove the surjectivity of this map, we again simply copy the proof of the surjectivity of the map ι given above. This is where we use the fact that the strand-doubling map g_3 is part of the tower $\mathcal{T}_4$. Needless to say, one would prefer to dispense with this extra compatibility condition. $\diamond$

§5. $\widehat{GT}$ is the full automorphism group of $\mathrm{Aut}(\hat{\mathcal{T}})$

We now prove the profinite part of (iii) of the main theorem. In proposition 10 we define an injective homomorphism of $\widehat{GT}$ into $\mathrm{Aut}(\hat{\mathcal{T}})$, which is shown to be a bijection in proposition 11.

Proposition 10: *Let $(\lambda, f) \in \widehat{GT}$ and associate to it for all $n \geq 1$ a map $\phi_n = \phi_{n,(\lambda,f)}$ which sends the generators of $\hat{B}_n$ into $\hat{B}_n$ as in equation* (5), *namely:*

$$\phi_n(\sigma_1) = \sigma_1^\lambda \text{ and } \phi_n(\sigma_i) = f(\sigma_i^2, y_i)\sigma_i^\lambda f(y_i, \sigma_i^2) \text{ for } 2 \leq i \leq n-1.$$

Then ϕ_n can be extended by multiplicativity to an automorphism of $\hat{B}_n$ for all n which preserves the subgroup $\hat{A}_n \subset \hat{B}_n$. Set $\phi'_n = \phi_n|_{\hat{A}_n}$; then $(\lambda, f) \mapsto (\phi_n, \phi'_n)_{n\geq 1}$ defines an injective map $\theta : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}})$.

Proof: Fix $(\lambda, f) \in \widehat{GT}$. Let us show that for all $n \geq 1$, ϕ_n determines an element of $\mathrm{Aut}(\hat{B}_n)$. We know by proposition 6 that ϕ_4 is an automorphism of $\hat{B}_4$. To see that ϕ_n can be extended multiplicatively to an automorphism of all of $\hat{B}_n$, we must show that ϕ_n respects relations (1) of the definition of B_n given in §2. For the commutation relations $(\sigma_i, \sigma_j) = 1$ when $|i-j| \geq 2$, it suffices to recall that the elements $y_i \in \hat{B}_n$ commute, which shows that $\phi_n(\sigma_i)\phi_n(\sigma_j) = \phi_n(\sigma_j)\phi_n(\sigma_i)$ since the factors of $\phi_n(\sigma_j)$ only contain y_j and σ_j and thus commute with those of $\phi_n(\sigma_i)$ which themselves only contain y_i and σ_i.

For the braid relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$, we first note that since ϕ_n restricted to $\hat{B}_4 \subset \hat{B}_n$ is an automorphism, it respects these relations for $i = 1$ and $i = 2$. For $2 < i \leq n-2$, let C_i be the subgroup of $\hat{B}_n$ generated by σ_i, σ_{i+1}, y_i and y_{i+1}. Then there is a canonical isomorphism $\psi_i : C_i \to C_2$ taking σ_i to σ_2, σ_{i+1} to σ_3, y_i to y_2 and y_{i+1} to y_3. This isomorphism can be visualized in terms of braids by noting that the braids in C_i are exactly those in C_2 where the first strand is replaced by $i-1$ parallel strands – the situation is similar to the proof that the maps g_n are homomorphisms, cf. §2. Now, consider the map $h_i := \psi_i^{-1}\phi_n\psi_i$ on the subgroup C_i for $2 < i \leq n-2$. Since ϕ_n is an automorphism of $C_2 = \psi_i(C_i)$ because $C_2 \subset \hat{B}_4$, the map h_i is an automorphism of C_i. But

$$h_i(\sigma_i) = \psi_i^{-1}\phi_n\psi_i(\sigma_i) = \psi_i^{-1}\phi_n(\sigma_2) = \psi_i^{-1}\big(f(\sigma_2^2, y_2)\sigma_2^\lambda f(y_2, \sigma_2^2)\big) =$$

$$f(\sigma_i^2, y_i)\sigma_i^\lambda f(y_i, \sigma_i^2)$$

and

$$h_i(\sigma_{i+1}) = \psi_i^{-1}\phi_n(\sigma_3) = f(\sigma_{i+1}^2, y_{i+1})\sigma_{i+1}^\lambda f(y_{i+1}, \sigma_{i+1}^2),$$

so h_i agrees with ϕ_n on σ_i and σ_{i+1}, so ϕ_n respects the braid relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $2 < i < n-1$ since h_i does. This shows that the ϕ_n are in $\mathrm{Aut}(\hat{B}_n)$ for $n \geq 1$. The automorphisms ϕ_n defined in this way preserve the subgroups $\hat{A}_n \subset \hat{B}_n$, so we define $\phi'_n = \phi_n|_{\hat{A}_n}$. Then it is easily checked by a simple calculation that $(\phi_n, \phi'_n)_{n\geq 1} \in \mathrm{Aut}(\hat{\mathcal{T}})$ since the ϕ_n and the ϕ'_n respect all the arrows i_n, f_n and g_n. Thus we have a map $\theta : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}})$. Moreover, this map is injective because its kernel is contained in the kernel of the injective homomorphism $\tilde{\eta} : \widehat{GT}_0 \to \mathrm{Aut}(\mathcal{T}_3)$ (restricted to $\widehat{GT}$) defined in §3. $\diamondsuit$

Proposition 11: *The map* $\theta : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}})$ *is bijective.*

Proof: We prove surjectivity of θ. Let $(\phi_n, \phi'_n)_{n\geq 1} \in \mathrm{Aut}(\hat{\mathcal{T}})$. Let $(\lambda, f) \in \widehat{GT}$ be the couple associated to $(\phi_n, \phi'_n)_{1\leq n\leq 4} \in \mathrm{Aut}(\hat{\mathcal{T}}_4)$ by proposition 6. Let $(\psi_n, \psi'_n)_{n\geq 1} := \theta(\lambda, f)$, so $\phi_4 = \psi_4$. We must show that $\phi_n = \psi_n$ for $n > 4$, or equivalently, that ϕ_n must be as defined on $\hat{B}_n$ as in equation (5). We proceed by induction; it is true for $1 \leq n \leq 4$; suppose it true for a given n. We must determine how ϕ_{n+1} acts on σ_n. We thus calculate using the compatibility of the ϕ_n with the maps g_n that:

$$\phi_{n+1}(\sigma_n) = \phi_{n+1}g_n(\sigma_{n-1}) = g_n\phi'_n(\sigma_{n-1}),$$

$$= g_n\Big(f(y_{n-1}, \sigma_{n-1}^2)^{-1}\sigma_{n-1}^{\lambda}f(y_{n-1}, \sigma_{n-1}^2)\Big) = f(y_n, \sigma_n^2)^{-1}\sigma_n^{\lambda}f(y_n, \sigma_n^2),$$

since for $2 \leq i \leq n-1$, we have $g_n(y_i) = y_{i+1}$. This shows that for all $n \geq 1$, ϕ_n acts on $\hat{B}_n$ as in (5), so $\phi_n = \psi_n$ for all n, so $(\phi_n, \phi'_n)_{n\geq 1} = \theta(\lambda, f)$. Thus the map $\theta : \widehat{GT} \to \mathrm{Aut}(\hat{\mathcal{T}})$ is bijective, which concludes the proof of the profinite part of the Main Theorem (it is obvious that we also have $\widehat{GT} \simeq \mathrm{Aut}(\hat{\mathcal{T}}_N)$ for all $N > 4$). $\diamondsuit$

§6. GT_ℓ is the full automorphism group of $\mathcal{T}$

In this paragraph we finish the proof of the pro-ℓ statement (iii) of the Main Theorem. This involves proving analogues of propositions 10 and 11 in the pro-ℓ case. The statement and proof of proposition 10 are very easily adapted to the pro-ℓ case. This is not the case for proposition 11, since the strand-doubling maps g_n are not included in the tower $\mathcal{T}$. One could of course include them, however we found that thanks to an injectivity theorem proved by Ihara in the pro-ℓ case (see the proof of lemma 16) which is not known to hold in the profinite case, they are actually not needed to obtain the result. Before establishing the Main Theorem in the pro-ℓ case, we prove a necessary auxiliary result on the general behavior of the automorphism groups of the $B_n^{(\ell)}$ in Proposition 12.

For all $N \geq 1$, let us denote by $\mathrm{Aut}_1(\mathcal{T}_N)$ (resp. $\mathrm{Out}_1(\mathcal{T}_N)$) the subgroup of elements (resp. classes of elements mod $\mathrm{Inn}(\mathcal{T}_N)$) $(\phi_n)_{1\leq n\leq N}$ such that $\phi_n(\sigma_1) = \sigma_1$. Note that this condition implies that $\phi_n(\omega_n) = \omega_n$ for $1 \leq n \leq N$; indeed, ϕ_n must map ω_n to a $\mathbb{Z}_\ell^*$-power μ of itself since the center of $B_n^{(\ell)}$ is cyclic, and this power is easily seen to be equal to 1 by considering the identity $\phi_n(\omega_n) = \omega_n^\mu$ modulo the derived subgroup of $B_n^{(\ell)}$.

Proposition 12: *The map* $\mathrm{Out}_1(\mathcal{T}_N) \to \mathrm{Out}_1(\mathcal{T}_{N-1})$ *induced by restricting automorphisms of* $B_N^{(\ell)}$ *to the subgroup* $B_{N-1}^{(\ell)} \subset B_N^{(\ell)}$ *is injective for* $N \geq 4$.

Proof: The proof uses sublemmas 13, 14 and 15 to reduce the statement to the similar statement for the pure braid groups given in lemma 16, which is an adaptation of an analogous result for the pure Hurwitz braid groups proven by Ihara in [I2].

Sublemma 13: *Let* $\phi \in \mathrm{Aut}(\mathcal{T}_N)$. *Then for* $1 \leq i < j \leq N$ *there exists* $\alpha_{ij} \in K_N^\ell$ *such that* $\phi(x_{ij}) = \alpha_{ij}^{-1} x_{ij}^\lambda \alpha_{ij}$, *and for* $1 \leq i \leq N-1$, *there exists* $\alpha_i \in K_N^\ell$ *such that* $\phi(\sigma_i) = \alpha_i^{-1}\sigma_i^\lambda\alpha_i$.

Proof: If $\phi \in \mathrm{Aut}(\mathcal{T}_N)$, then $\phi(\sigma_1) = \sigma_1^\lambda$ and $\phi(x_{12}) = x_{12}^\lambda$ for some $\lambda \in \hat{\mathbb{Z}}_\ell^*$ since ϕ must preserve $B_2^{(\ell)}$. Using equation (2') in §2 we find that

$$\phi(x_{ij}) = \phi(a_{ij})^{-1}x_{12}^\lambda\phi(a_{ij}) = \phi(a_{ij})^{-1}a_{ij}x_{ij}^\lambda a_{ij}^{-1}\phi(a_{ij}) = \alpha_{ij}^{-1}x_{ij}^\lambda\alpha_{ij}$$

which is the statement of the lemma, with $\alpha_{ij} = a_{ij}^{-1}\phi(a_{ij})$. For the σ_i we proceed more explicitly. Set $\pi = \sigma_1\cdots\sigma_{n-1}$ (this is denoted π_2 in the appendix); it is easy to check that $\sigma_i = \pi^{i-1}\sigma_1\pi^{-(i-1)}$ for $1 \leq i \leq n-1$. Thus:

$$\phi(\sigma_i) = \phi(\pi)^{i-1}\sigma_1^\lambda\phi(\pi)^{-(i-1)} = \phi(\pi)^{i-1}\pi^{-(i-1)}\sigma_i^\lambda\pi^{i-1}\phi(\pi)^{-(i-1)},$$

i.e. $\phi(\sigma_i) = \alpha_i^{-1}\sigma_i^\lambda\alpha_i$ where $\alpha_i := \pi^{i-1}\phi(\pi)^{-(i-1)}$. ◇

Sublemma 14: *The map* $\mathrm{Aut}(B_N^{(\ell)}/Z) \to \mathrm{Aut}(K_N^\ell/Z)$ *induced by restricting automorphisms to the subgroup* $K_N^\ell/Z \subset B_N^{(\ell)}/Z$ *is injective.*

Proof: Let $K \lhd B$ be groups and suppose that the centralizer $\mathrm{Centr}_B(K)$ of K in B is trivial. Consider B as a normal subgroup of $\mathrm{Aut}(B)$ via inner automorphisms. Let us show that the restriction map $\mathrm{Aut}(B) \to \mathrm{Aut}(K)$ is injective. It suffices to show that that $\mathrm{Centr}_{\mathrm{Aut}(B)}(K)$ is trivial since any $\phi \in \mathrm{Aut}(B)$ whose restriction to K is the identity is in $\mathrm{Centr}_{\mathrm{Aut}(B)}(K)$. So let $x \in \mathrm{Centr}_{\mathrm{Aut}(B)}(K)$ and $b \in B$ be considered as an inner automorphism .

Consider the automorphism $b^{-1}xbx^{-1}$ of B. It is inner since B is normal in $\mathrm{Aut}(B)$. But it is in $\mathrm{Centr}_B(K)$ since it acts trivially on K. So it is trivial and x commutes with b. Since this is true for all $b \in B$, $x \in \mathrm{Centr}_{\mathrm{Aut}(B)}(B)$. But this centralizer is also trivial since if $\phi \in \mathrm{Aut}(B)$, then $\phi \mathrm{Inn}(b)\phi^{-1} = \mathrm{Inn}(\phi(b))$, so if this expression is equal to $\mathrm{Inn}(b)$ for all $b \in B$, then ϕ is the identity (the center of B being trivial). So $x = 1$, which shows that $\mathrm{Aut}(B) \to \mathrm{Aut}(K)$ is injective.

The sublemma is proved by applying this result to $K_N^\ell/Z \lhd B_N^{(\ell)}/Z \lhd \mathrm{Aut}(B_N^{(\ell)}/Z)$ since the centralizer of K_N^ℓ/Z in $B_N^{(\ell)}/Z$ is trivial. ◊

Let $\mathcal{K}_N$ be the tower consisting of the pure braid groups K_n^ℓ for $1 \le n \le N$, with the restrictions to these groups of the inclusions $i_{n,m}$ for $1 \le n < m \le N$. For each N, let $\mathrm{Aut}_1^r(\mathcal{K}_N)$ denote the image of $\mathrm{Aut}_1(\mathcal{T}_N)$ under the natural restriction map $\mathrm{Aut}(\mathcal{T}_N) \to \mathrm{Aut}(\mathcal{K}_N)$. Denote by $\mathrm{Inn}(\mathcal{K}_N)$ the image of $\mathrm{Inn}(\mathcal{T}_N)$ under this map (although its elements are not really inner automorphisms of $\mathcal{K}_N$). Let $\mathrm{Out}(\mathcal{K}_N) = \mathrm{Aut}(\mathcal{K}_N)/\mathrm{Inn}(\mathcal{K}_N)$.

Sublemma 15: *The restriction map* $\mathrm{Out}_1(\mathcal{T}_N) \to \mathrm{Out}_1^r(\mathcal{K}_N)$ *is an isomorphism for* $N \ge 1$.

Proof: By definition, this map is surjective. We must show it is injective. Consider the diagram

$$\begin{array}{ccc} \mathrm{Aut}_1(\mathcal{T}_N) & \to & \mathrm{Aut}_1^r(\mathcal{K}_N) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(B_N^{(\ell)}/Z) & \to & \mathrm{Aut}(K_N^\ell/Z). \end{array}$$

The lower map is injective by sublemma 14. The vertical maps are given by the fact that any automorphism of $B_N^{(\ell)}$ which fixes the center naturally induces an automorphism of $B_N^{(\ell)}/Z$. These maps are easily seen to be injective (see [DG], thm. 20); as usual, one considers what happens modulo the derived subgroup. So the upper map is an isomorphism. By definition, it remains an isomorphism when Aut is replaced by Out. ◊

Lemma 16: *The natural restriction map* $\mathrm{Out}_1^r(\mathcal{K}_N) \to \mathrm{Out}_1^r(\mathcal{K}_{N-1})$ *is injective for* $N \ge 4$.

Proof: Let P_n denote the pure Hurwitz braid group contained in H_n. By proposition 2 (iv) (pro-ℓ), P_{n+1}^ℓ is a semi-direct product $F_n^\ell \rtimes P_n^\ell$ for $n \ge 3$, where F_n^ℓ is the pro-free group of rank $n-1$ generated by $\tilde{x}_{1,n+1}, \ldots, \tilde{x}_{n,n+1}$ with the Hurwitz relation $\tilde{x}_{1,n+1} \cdots \tilde{x}_{n,n+1} = 1$. For $n \ge 1$, let $(K_n')^\ell \subset K_n^\ell$

be as in proposition 2. Let the groups $\mathrm{Out}^*(P_n^\ell)$ be as defined in [I2], i.e. $\mathrm{Out}^*(P_n^\ell) =$

$$\{\phi \in \mathrm{Out}(P_n^\ell) \mid \exists \alpha_{ij} \in P_n^\ell \text{ such that } \phi(\tilde{x}_{ij}) = \alpha_{ij}^{-1}\tilde{x}_{ij}\alpha_{ij} \ \forall\ 1 \le i < j \le n\}.$$

For $n \ge 1$, let

$$h_n : \mathrm{Out}_1^r(\mathcal{K}_n) \to \mathrm{Out}((K_n')^\ell, *)$$

be the maps obtained by restricting the elements of $\mathrm{Out}_1^r(\mathcal{K}_n)$, considered as outer automorphisms of $K_n^\ell = (K_n')^\ell \times Z(K_n^\ell)$, to the subgroup $(K_n')^\ell$ (they are actually automorphisms of K_n', as can easily be seen by recalling that they conjugate each x_{ij}) Let $\mathrm{Out}_1^r((K_n')^\ell) = \mathrm{Im}(h_n)$. The h_n are injective since elements of $\mathrm{Out}_1^r(\mathcal{K}_n)$, considered as automorphisms of K_n^ℓ, fix the center, so they are isomorphisms

$$h_n : \mathrm{Out}_1^r(\mathcal{K}_n) \xrightarrow{\sim} \mathrm{Out}_1^r((K_n')^\ell).$$

Fix $N \ge 1$. The following diagram commutes:

$$\begin{array}{ccc} \mathrm{Out}^*(P_{N+1}^\ell) & \to & \mathrm{Out}^*(P_N^\ell) \\ \downarrow & & \downarrow \\ \mathrm{Out}_1^r((K_N')^\ell) & \xrightarrow{h} & \mathrm{Out}_1^r((K_{N-1}')^\ell), \end{array}$$

where the upper map corresponds to the quotient by F_N^ℓ, which induces an automorphism of P_N^ℓ since F_N^ℓ is normal and so preserved by all $\phi \in \mathrm{Out}^*(P_{N+1}^\ell)$. The lower map h is simply the restriction map ($(K_{N-1}')^\ell$ is considered to be included in $(K_N')^\ell$ via $i_{N-1,N}$). The vertical maps come from the fact that elements of $\mathrm{Out}^*(P_N^\ell)$ fix the center of P_N^ℓ, so these maps induce automorphisms on P_N^ℓ/Z, which is isomorphic to $(K_{N-1}')^\ell$ by proposition 2 (iii).

Ihara showed that the upper map is injective; this theorem is the main result of [I2]. The right-hand vertical map is also injective. For if ϕ is in the kernel, then ϕ fixes $(K_{N-1}')^\ell$, but ϕ fixes the center of P_N^ℓ, so since $P_N^\ell = (K_{N-1}')^\ell \times Z(P_N^\ell)$ by proposition 2 (iii), ϕ is the identity. This shows that the lower map is injective. So the map

$$g_{N-1}^{-1} \circ h \circ g_N : \mathrm{Out}_1^r(\mathcal{K}_N) \to \mathrm{Out}_1^r(\mathcal{K}_{N-1})$$

is injective; it is the map in the statement of the lemma. $\diamond$

To conclude, we consider the commutative diagram

$$\begin{tikzcd}
\mathrm{Out}_1(\mathcal{T}_N) \arrow[r] \arrow[d] & \mathrm{Out}_1(\mathcal{T}_{N-1}) \arrow[d] \\
\mathrm{Out}_1^r(\mathcal{K}_N) \arrow[r] & \mathrm{Out}_1^r(\mathcal{K}_{N-1}).
\end{tikzcd}$$

By sublemma 14, the vertical arrows are isomorphisms and the lower arrow is injective by lemma 16, so the upper arrow is injective. This finally concludes the proof of proposition 12. $\diamond$

We can now easily establish pro-ℓ analogues of propositions 6, 10 and 11.

Proposition 17: *(i) There is an injective map* $\theta : GT_\ell \to \mathrm{Out}(\mathcal{T})$ *given by associating to a couple* (λ, f) *an automorphism* ϕ_n *of* $B_n^{(\ell)}$ *defined as in equation (5);*

(ii) the map θ *is a bijection.*

Proof: (i) Fix $(\lambda, f) \in GT_\ell$ and define ϕ_n on the generators of $B_n^{(\ell)}$ as in equation (5). The proof of proposition 10 can be copied directly to prove this result once the use of proposition 6 is replaced by its corollary.

(ii) We finally prove the surjectivity of the map $\theta : GT_\ell \to \mathrm{Out}(\mathcal{T})$. Let $\Phi \in \mathrm{Out}(\mathcal{T})$ and let $\phi = (\phi_n)_{n\geq 1} \in \mathrm{Aut}(\mathcal{T})$ be a representative of Φ which fixes the permutations of the $B_n^{(\ell)}$ (it exists by lemma 3). Then by proposition 4, there exists a unique couple $(\lambda, f) \in GT_{\ell,0}$ such that $\phi_3 = \tilde{\eta}(\lambda, f)$. Let $\psi = (\psi_n)_{n\geq 1} = \tilde{\theta}(\lambda, f)$. Then $\psi \in \mathrm{Aut}(\mathcal{T})$ and $\psi_3 = \phi_3$. Set $\chi = \phi\psi^{-1}$. Then writing $\chi = (\chi_n)_{n\geq 1}$, we see that χ_3 is the identity on $B_3^{(\ell)}$, so by proposition 12, χ_n is the identity on $B_n^{(\ell)}$ for $n \geq 1$, which means that $\phi = \psi = \tilde{\theta}(\lambda, f)$, so θ is surjective. Thus we obtain $\mathrm{Out}(\mathcal{T}) \simeq GT_\ell \simeq \mathrm{Out}(\mathcal{T}_N)$ for all $N \geq 4$, which concludes the proof of proposition 17, and of the Main Theorem. $\diamond$

Appendix

The goal of this appendix is to assemble a number of results on Artin and sphere braid groups and modular groups, which although quite elementary to prove, do not seem to be anywhere in the usual literature on braid groups ([A1], [A2], [Bi], [DG], [Ma], etc.). The basic result is proposition A3, which gives rise to a number of different isomorphisms, homomorphisms, inclusions and relations between the different braid groups described in proposition A4 (which occurs as proposition 2 of §2). We have chosen to make this appendix entirely self-contained at the price of repeating several of the definitions and restating some results already given in §§2 and 4 of the main article.

Let us begin again with notation and definitions. For $n > 2$, we write B_n for the Artin braid group on n strings, K_n for the pure Artin braid group on n strings, H_n for the Hurwitz (or sphere) braid group on n strings, P_n for the pure Hurwitz braid group, $M(0,n)$ for the modular group of the sphere with n marked points and $K(0,n)$ for the pure modular group. We will recall a presentation by generators and relations for each of these groups as well as a good many other extremely well-known facts, but we do not recall their proofs and/or geometric interpretations since these are to be found everywhere in the literature ([Bi] for example).

– B_n is generated by elements $\sigma_1,\ldots,\sigma_{n-1}$ satisfying the following relations:

$$\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for } 1\le i\le n-2 \text{ and } \sigma_i\sigma_j=\sigma_j\sigma_i \text{ for } |i-j|\ge 2. \qquad (A1)$$

It is well-known that the center of B_n is an infinite cyclic group generated by $\omega_n:=(\sigma_1\cdots\sigma_{n-1})^n$.

– H_n is the quotient of B_n by normal closure of the element

$$\alpha_n:=\sigma_{n-1}\sigma_{n-2}\cdots\sigma_2\sigma_1^2\sigma_2\cdots\sigma_{n-2}\sigma_{n-1}.$$

It is well-known that the center of H_n is of order 2, generated by the image $\tilde{\omega}_n$ of $(\sigma_1\cdots\sigma_{n-1})^n$ in H_n.

– $M(0,n)$ is the quotient of H_n by its center.

There is a natural surjective homomorphism $\rho: B_n\to S_n$, where S_n is the permutation group on n letters, giving by quotienting by the relations $\sigma_i^2=1$. This ρ induces homomorphisms $H_n\to S_n$ and $M(0,n)\to S_n$. The groups K_n, P_n and $K(0,n)$ are defined to be the kernels of these maps in B_n, H_n and $M(0,n)$ respectively.

Let us give a more symmetric presentation of the group B_n which we have frequently found useful.

Proposition A1: *The following is a presentation for the Artin braid group B_n: as generators we take σ_{ij} for $i,j \in \mathbb{Z}/n\mathbb{Z}$, with the relations*

$$\sigma_{ii} = 1, \ \ \sigma_{ij} = \sigma_{ji}, \ \ \sigma_{jk}\sigma_{ij} = \sigma_{ik}\sigma_{kj} (= \sigma_{ij}\sigma_{ki}) \ \ \textit{and} \ \ \sigma_{ij}\sigma_{kl} = \sigma_{kl}\sigma_{ij} \quad (A2)$$

for i,j,k,l distinct in cyclic order in $\mathbb{Z}/n\mathbb{Z}$.

Proof: Let us imagine the strings of a braid to be hanging from a ring and attached at equally spaced points. The elements σ_{ij} should then be thought of as intertwining the i-th and j-th strings once. We use $1,\ldots,n$ as representatives of the elements of $\mathbb{Z}/n\mathbb{Z}$. Set $\sigma_{ij} = \sigma_{j-1}\cdots\sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\cdots\sigma_{j-1}^{-1}$ for $i,j \in \mathbb{Z}/n\mathbb{Z}$ (so $\sigma_{i,i+1} = \sigma_i$ for $1 \le i \le n-1$). The symbol σ_n which appears in this expression when $i > j$ is not defined in B_n, so we define it by setting $\sigma_n := \sigma_{n1} = \sigma_{1n}$, the last quantity being well-defined. Thus, $\sigma_{ii} = 1$ holds by convention and $\sigma_{1n} = \sigma_{n1}$ is true by definition. The defining relations (A1) for B_n appear as particular cases of the relations (A2): the braid relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ correspond to the "triangular" relations for $i, j = i+1, k = i+2$ and the commutation relations to the "four-points" relations with $i, j = k+1, k, l = k+1$. To prove that all the relations of the proposition hold in B_n, we first prove the relation

$$\sigma_{1,n}\sigma_{n-1,n}\sigma_{1,n}^{-1} = \sigma_{1,n-1} \qquad (A3)$$

(which is just the case $i = 1$, $j = n-1$, $k = n$ of the triangular relation) in B_n. For this we use the following principle of "index shifting". Set $\pi_1 = \sigma_{n-1}\cdots\sigma_1$ and $\pi_2 = \sigma_1\cdots\sigma_{n-1}$. Then we have the relations

(i) $\pi_1^{-1}\sigma_{i,i+1}\pi_1 = \sigma_{i+1,i+2}$ for $i \in \mathbb{Z}/n\mathbb{Z}$ and

(ii) $\pi_2\sigma_{i,i+1}\pi_2^{-1} = \sigma_{i+1,i+2}$ for $1 \le i \le n-2$.

We can now prove relation (A3) from the known relation $\sigma_{23}\sigma_{12}\sigma_{23}^{-1} = \sigma_{13}$ in B_n by conjugating both sides by π_1 to obtain π_1^2 (with the positive power on the left). The other relations are proved by induction on n, starting from the fact that the relations (A2) are valid for $n = 3$ (by inspection) and in the classical cases enumerated above which correspond to Artin's relations (A1), and checking that they remain valid if one adds a further $n+1$-th string. This is rather obvious if one keeps in mind the geometric meaning of σ_{ij} but the computations are admittedly a bit messy and we shall not reproduce them here.

$\diamond$

The σ_{ij} arise naturally, in particular because their squares $x_{ij} := \sigma_{ij}^2$ generate the pure braid group K_n. Since $x_{ii} = 1$ and $x_{ij} = x_{ji}$, K_n is actually generated by the x_{ij} for $1 \le i < j \le n$, with the following classical defining relations ([A1], [Bi]), where we write (a,b) for the commutator $aba^{-1}b^{-1}$:

- $x_{ij}x_{ik}x_{jk}$ commutes with x_{ij}, x_{ik} and x_{jk} for all $i < j < k$;

- $(x_{ij}, x_{kl}) = (x_{il}, x_{jk}) = 1$ for $i < j < k < l$;

- $(x_{ik}, x_{ij}^{-1}x_{jl}x_{ij}) = 1$ for $i < j < k < l$.

P_n is the image of K_n under the map $B_n \to H_n$. More precisely, we have

Lemma A2: *P_n is the quotient of K_n by the normal subgroup U_n generated by the elements α_i for $1 \le i \le n$ given by*

$$\alpha_i = x_{1i}x_{2i}\cdots x_{n-1,i}x_{n,i}. \tag{A4}$$

Proof: We use the presentation given in proposition A1 and the remark that any $n-1$ of the elements $\sigma_{12}, \sigma_{23}, \ldots, \sigma_{n-1,n}, \sigma_{n1}$ give a generating system for B_n. The lemma is then a consequence of the following identities: $(\alpha_i, \sigma_{j,j+1}) = 1$ for $j \not\equiv i$ or $i-1$ in $\mathbb{Z}/n\mathbb{Z}$, and $\sigma_{i-1,i}^{-1}\alpha_i\sigma_{i-1,i} = \alpha_{i-1}$; in particular these identities show that U_n is normal in B_n (and thus in K_n), and indeed is exactly the normal closure of the group generated by the element α_n. It suffices to prove these identities for a single value of $i \in \mathbb{Z}/n\mathbb{Z}$ since they are then all obtained by shifting indices as in the proof of proposition A1. Let us take $i = n$, $\alpha_n = x_{1n}\cdots x_{n-1,n} = \sigma_{n-1}\cdots\sigma_1^2\cdots\sigma_{n-1}$. The fact that α_n commutes with σ_i for $1 \le i \le n-2$ is immediate to anyone having the courage to draw the the braids. We prove it explicitly by noting that $\alpha_n = \pi_2\pi_1$,

$$\alpha_n\sigma_{j,j+1}\alpha_n^{-1} = \pi_2\pi_1\sigma_{j,j+1}\pi_1^{-1}\pi_2^{-1} = \pi_2\sigma_{j+1,j+2}\pi_2^{-1} = \sigma_{j,j+1}$$

for $1 \le j \le n-2$.

For the final identity, note that $\sigma_{n-1}^{-1}\alpha_n\sigma_{n-1} = \sigma_{n-2}\cdots\sigma_1^2\cdots\sigma_{n-2}\sigma_{n-1}^2$, which is exactly equal to $\alpha_{n-1} = x_{1,n-2}\cdots x_{n-3,n-2}x_{n-1,n-2}$. ◇

From now on, let us write $\tilde{\alpha}$ for the image in H_n of any element $\alpha \in B_n$, and $\bar{\alpha}$ for the image of α in $M(0,n)$. Thus P_n is generated by the $\tilde{x}_{ij}$. For $1 \le j \le n$, we have the sphere relations "based at i" in P_n, namely:

$$\tilde{x}_{1i}\cdots\tilde{x}_{n,i} = 1, \tag{A5}$$

which, for $1 \le i \le n-1$, can also be written

$$\tilde{x}_{i,n} = (\tilde{x}_{1i}\tilde{x}_{2i}\cdots\tilde{x}_{i,n-1})^{-1}. \tag{A5'}$$

These relations show that in fact, $\{\tilde{x}_{ij} \mid 1 \le i < j \le n-1\}$ is a generating set for P_n.

The center of P_n is given by the element of order 2

$$\tilde{\omega}_n := (\tilde{x}_{12})(\tilde{x}_{13}\tilde{x}_{23}) \cdots (\tilde{x}_{1n}\tilde{x}_{2n} \cdots \tilde{x}_{n-1,n}),$$

or equivalently,

$$\tilde{\omega}_n = (\tilde{x}_{12})(\tilde{x}_{13}\tilde{x}_{23}) \cdots (\tilde{x}_{1,n-1}\tilde{x}_{2,n-1} \cdots \tilde{x}_{n-2,n-1}) \qquad (A6)$$

since $\tilde{x}_{1,n}\tilde{x}_{2,n} \cdots \tilde{x}_{n-1,n} = 1$ by the sphere relation based at n. In particular, we have

$$\tilde{x}_{12} = \tilde{\omega}_n \big(\tilde{x}_{13} \cdots \tilde{x}_{n-2,n-1}\big)^{-1}. \qquad (A7)$$

Let us introduce the following important sets:

$$\begin{aligned} E_n &:= \{x_{ij} \mid 1 \le i < j \le n,\ (i,j) \ne (1,2)\}, \\ \tilde{E}_n &:= \{\tilde{x}_{ij} \mid 1 \le i < j \le n,\ (i,j) \ne (1,2)\}, \qquad (A8) \\ \bar{E}_n &:= \{\bar{x}_{ij} \mid 1 \le i < j \le n,\ (i,j) \ne (1,2)\}, \end{aligned}$$

where these sets are considered as subsets of K_m, P_m and $K(0,m)$ respectively, for any $m \ge n$.

By equations (A5') and (A7), $\tilde{E}_{n-1} \cup \{\tilde{\omega}_n\}$ is a generating set for P_n, and thus $\bar{E}_{n-1}$ is a generating set for $K(0,n)$. If we denote by $\langle \tilde{E}_n \rangle$ the subgroup of P_n generated by $\tilde{E}_n$, then $P_n \simeq \langle \tilde{E}_n \rangle \times \mathbb{Z}/2\mathbb{Z}$, and this implies that

$$K(0,n+1) \simeq \langle \tilde{E}_n \rangle \simeq \langle \bar{E}_n \rangle. \qquad (A9)$$

In fact we have the stronger result

Proposition A3: *Let K'_{n-1} denote the subgroup of K_{n-1} generated by E_{n-1}. Then*

$$P_n \simeq K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}.$$

Proof: The main idea of the rather topological proof given here is that on the sphere, any pure braid on n-strings can be deformed into a unique braid with the following property: if the third to $n-1$-st strings are removed, the first two strings intertwine either exactly once (via $\tilde{x}_{12}$) or not at all. This implies that $P_3 = \mathbb{Z}/2\mathbb{Z}$ and in general reflects the fact that P_n is generated by a certain subgroup of braids in which the first and second strings do not intertwine at all, namely $\langle \tilde{E}_{n-1} \rangle$, and the central element $\tilde{\omega}_n$ of P_n, which intertwines them once and which is of order 2. Thus there is a bijection between the braids in P_n whose first two strings do not intertwine and the plane braids in K_n whose first two strings do not intertwine, which precisely means that $\langle E_{n-1}\rangle \simeq \langle \tilde{E}_{n-1}\rangle$.

In order to prove the result, it is best to use an other well-known interpretation of P_n, namely as the fundamental group of the following "configuration space"

$$F_{0,n} = \{Z = (z_1, \cdots, z_n), z_i \in \mathbb{P}^1\mathbb{C}, z_i \neq z_j \text{ for all } (i,j) \in \{1, \cdots, n\},\ i \neq j\}.$$

A braid is then represented as a path $Z(t), t \in (0,1)$, or rather as the class $[Z(t)] \in \pi_1(F_{0,n}) \simeq P_n$. To any path $Z(t)$ we associate a path ζ_t in $\mathrm{PGL}_2(\mathbb{C})$ as follows: ζ_t is the unique element of $\mathrm{PGL}_2(\mathbb{C})$ which maps the points $\{0,1,\infty\}$ to $\{z_1(t), z_2(t), z_3(t)\}$. We assume below that $n \geq 3$ ($n=1$ or 2 are trivial cases) and $\mathrm{PGL}_2(\mathbb{C})$ acts on $\mathbb{P}^1\mathbb{C}$ via Möbius transformations as usual. To a path α_t in $\mathrm{PGL}_2(\mathbb{C})$ and a path $Z(t)$ in $F_{0,n}$ we associate the path $\alpha_t \cdot Z(t)$ in $F_{0,n}$ defined by the componentwise action of α_t, i.e. by $(\alpha_t \cdot Z(t))_i = \alpha_t z_i(t)$. It is easy to check that the corresponding braid $[\alpha_t \cdot Z(t)]$ actually depends only on the class $[\alpha_t] \in \pi_1(\mathrm{PGL}_2(\mathbb{C}))$; indeed if α_t can be homotoped to the trivial path by a homotopy $\alpha_t(s)$, $\alpha_t(s) \cdot Z(t)$ provides a homotopy between $\alpha_t \cdot Z(t)$ and $Z(t)$.

Recall now that $\pi_1(\mathrm{PGL}_2(\mathbb{C})) = \mathbb{Z}/2\mathbb{Z}$ and that a representative of the only non-trivial element can be taken to be

$$\gamma_t = \begin{pmatrix} e^{i\pi t} & 0 \\ 0 & e^{-i\pi t} \end{pmatrix}, \quad t \in (0,1).$$

Let now $[Z(t)]$ be an arbitrary braid represented by $Z(t)$ and consider $\zeta_t^{-1} \cdot Z(t)$; by the very definition of ζ_t, this path fixes $\{0,1,\infty\}$ so in particular it can be considered as a path on the plane, representing a braid with $n-1$ strings, out of which two are kept fixed. Two cases may arise according to whether $[\zeta_t] = 1 \in \pi_1(\mathrm{PGL}_2(\mathbb{C}))$ or not. In the first case, $[\zeta_t^{-1} \cdot Z(t)] = [Z(t)] \in P_n$ and we have an explicit correspondence of this class of braids with K'_{n-1}. If on the other hand $[\zeta_t] \neq 1 \in \pi_1(\mathrm{PGL}_2(\mathbb{C}))$, we have that $[\zeta_t] = [\zeta_t^{-1}] = [\gamma_t]$.

Let $\Omega(t)$ be a path corresponding to the center $\tilde{\omega}_n$ of P_n, and ω_t the corresponding path in $\mathrm{PGL}_2(\mathbb{C})$. A possible choice of $\Omega(t)$ can be described as follows (see [Bi]; of course all choices are equivalent). We set $\Omega(0) = (0, 1, 2, \cdots, n-2, \infty)$ (these are points on $\mathbb{P}^1\mathbb{C}$) and $\Omega_i(t) = \exp(2i\pi t)\Omega_i(0)$ (so that 0 and ∞ are actually fixed). From this, we obviously get $\omega_t = \gamma_t$ and a fortiori $[\omega_t] = [\gamma_t] \neq 1 \in \pi_1(\mathrm{PGL}_2(\mathbb{C}))$. Thus returning to the case when $[\zeta_t]$ associated to $Z(t)$ is non-trivial, we see that the path $\Omega_t \circ Z(t)$, obtained by composing $Z(t)$ with Ω_t is associated with the trivial element of $\pi_1(\mathrm{PGL}_2(\mathbb{C}))$ and we are back to the first case. But now $[\Omega_t \circ Z(t)] = \tilde{\omega}_n[Z(t)] \in P_n$, which finishes the proof and in fact provides an explicit description of the stated isomorphism.

$\diamond$

Corollary: $\langle E_n \rangle \simeq \langle \tilde{E}_n \rangle \simeq \langle \bar{E}_n \rangle$ for $n > 2$.

Proposition A3 gives rise to a number of natural relations between the braid groups which we summarize as follows.

Proposition A4: *We have:*

(i) $K_n = K'_n \times \langle \omega_n \rangle$.

(ii) There are two natural inclusions i_1 *and* i_2 *of* K_{n-1} *into* K_n. *Both send* x_{ij} *to* x_{ij} *for* $1 \leq i < j \leq n$, $(i,j) \neq (1,2)$. *But* i_1 *is then defined by setting* $i_1(x_{12}) = x_{12}$, *whereas* i_2 *is defined by setting* $i_2(\omega_{n-1}) = \omega_n$.

(iii) $P_n \simeq K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ *and* $K(0, n+1) \simeq P_{n+1}/Z \simeq K'_n$.

(iv) $P_{n+1} \simeq K_{n+1}/U_{n+1} \simeq K_n/\langle \omega_n^2 \rangle$.

(v) The subgroup $\tilde{P}_n$ *of* P_{n+1} *generated by* $\tilde{E}_{n-1} \cup \{\tilde{\omega}_{n+1}\}$ *is isomorphic to* P_n.

(vi) $P_{n+1} = F_n \rtimes \tilde{P}_n$, *where* F_n *is the free group of rank* $n-1$ *generated by* $x_{1,n+1}, \ldots, x_{n,n+1}$ *(whose product equals* 1*).*

(vii) We have the inclusions $K(0, n+1) \simeq K_n/\langle \omega_n \rangle \subset B_n/\langle \omega_n \rangle \subset M(0, n+1)$.

Proof: (i) Since $x_{12} = \omega_n (x_{13} x_{23} \cdots x_{n-1,n})^{-1}$, we see that K'_n and ω_n generate K_n. To see that their intersection is trivial, it suffices to consider their images modulo the derived subgroup of K_n, and notice that the quotient is just the free abelian group on the images of the x_{ij}. Finally, it is obvious that K'_n is normal in K_n since it is normalized by ω_n. This shows that $K_n = K'_n \rtimes \langle \omega_n \rangle$, so $K_n = K'_n \times \langle \omega_n \rangle$ since ω_n is central.

(ii) That $i_1(K_{n-1}) \hookrightarrow K_n$ is injective is obvious. As for $i_2(K_{n-1})$, it sends K'_{n-1} injectively into K'_n and the cyclic group $\langle \omega_{n-1} \rangle$ isomorphically onto $\langle \omega_n \rangle$, so it sends $K_{n-1} = K'_{n-1} \times \langle \omega_{n-1} \rangle$ injectively into $K_n = K'_n \times \langle \omega_n \rangle$.

(iii) The first isomorphism is just proposition A3 and the others immediate consequences of it and the definitions.

(iv) The first isomorphism is by definition. For the second, we have $K_n/\langle \omega_n^2 \rangle \simeq K'_n \times \mathbb{Z}/2\mathbb{Z} \simeq P_{n+1}$ by (i) and (iii).

(v) Consider the map $K_{n+1} \to K_{n+1}/U_{n+1} \simeq P_{n+1}$. This map induces an injection on K'_{n-1} because by proposition A3, the image of K'_{n-1} in P_{n+1} is $\langle \tilde{E}_{n-1}\rangle$ which is isomorphic to $\langle E_{n-1}\rangle$ which is isomorphic to K'_{n-1}, where we consider K'_{n-1} to be included in K_n as in (ii). The subgroup $\langle \tilde{E}_{n-1}\rangle \times \langle \tilde{\omega}_{n+1}\rangle$ of P_{n+1} is thus isomorphic to $K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$, so to P_n by proposition A3.

(vi) Let V_n denote the image of U_n under the map $K_n \to K_n/\langle \omega_n^2\rangle \simeq P_{n+1}$ (by (iv)). This image is generated in P_{n+1} by the images $\tilde{\alpha}_i$ in P_{n+1} of the $\alpha_i = x_{1i}\cdots x_{ni} \in K_n$, so they are the products $\tilde{x}_{1i}\cdots \tilde{x}_{ni}$. But in P_{n+1}, we have the relations $x_{1i}\cdots x_{ni}x_{n+1,i} = 1$, so $x_{n+1,i}^{-1} = \tilde{\alpha}_i$, so in P_{n+1}, it is generated by the $x_{n+1,i}$ for $1 \le i \le n$; it is precisely $F_n \subset P_{n+1}$. Since U_n is normal in K_n, F_n is normal in P_{n+1}.

Under the isomorphism $P_{n+1} \simeq K'_n \times \mathbb{Z}/2\mathbb{Z}$ of proposition A3, F_n thus corresponds to V_n. We saw in (v) that moreover $\tilde{P}_n \subset P_{n+1}$ corresponds to the subgroup $K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ included in $K'_n \times \mathbb{Z}/2\mathbb{Z}$ in the obvious way. The intersection $K'_{n-1} \cap V_n$ is trivial in $K'_n \times \mathbb{Z}/2\mathbb{Z}$ for the following reason: we know that $(K'_n \times \mathbb{Z}/2\mathbb{Z})/V_n \simeq P_n$ and that the image of $K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ is $\tilde{P}_{n-1} \subset P_n$ which is isomorphic to P_{n-1} and therefore to $K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ (by (iii) and (v)). So this quotient map is injective on $K'_{n-1} \times \mathbb{Z}/2\mathbb{Z}$ and V_n is its kernel, so these groups cannot intersect. This shows that $F_n \cap \tilde{P}_n = \{1\}$ in P_{n+1}. Since F_n and $\tilde{P}_n$ generate all of P_{n+1}, this means that $P_{n+1} \simeq F_n \rtimes \tilde{P}_n$ as stated.

(vii) The isomorphism comes from $K(0, n+1) \simeq K'_n = K_n/\langle \omega_n\rangle$ (by (i) and (iii)). The first inclusion is obvious and the second is because the relation $(\bar{\sigma}_1 \cdots \bar{\sigma}_n)^{n+1} = 1$ and the Hurwitz relation $\bar{\alpha}_n = 1$ in $M(0, n+1)$ imply that the relation $(\bar{\sigma}_1 \cdots \bar{\sigma}_{n-1})^n$ is also valid in $M(0, n+1)$ (cf. [Bi]) which means that the subgroup generated by $\bar{\sigma}_1, \ldots, \bar{\sigma}_{n-1}$ in $M(0, n+1)$ is isomorphic to $B_n/\langle \omega_n\rangle$. $\diamond$

References

[A1] E. Artin, Theory of braids, Annals of Math. **48** (1947), 101-126.

[A2] E. Artin, Braids and permutations, Annals of Math. **48** (1947), 643-649.

[Be] G.V.Belyi, On Galois extensions of a maximal cyclotomic field, Math. USSR Izv. **14** (1980), 247-256.

[Bi] J.Birman, Braids, links, and mapping class groups, Ann. of Math. Studies, vol. 82, Princeton Univ. Press, 1975.

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

[DG] J.L.Dyer and E.K.Grossman, The automorphism groups of the braid groups, American Journal of Mathematics **103** (1981), 1151-1169.

[G] A. Grothendieck, *Esquisse d'un Programme*, 1984, unpublished.

[I1] Y.Ihara, Braids, Galois groups, and some arithmetic functions, Proceedings of the International Congress of Mathematicians, Kyoto (1990), 99-120.

[I2] ———, Automorphisms of pure sphere braid groups and Galois representations, The Grothendieck Festschrift, Vol. 2, Progress in Mathematics **87** (1990), Birkhäuser, 353-373.

[I3] ———, On the stable derivation algebra associated with some braid groups, Israel J. of Math. **80** (1992), 135-153.

[M] B.H. Matzat, Zöpfe und Galoissche Gruppen, J. Crelle **420** (1991), 99-159.

[N] H.Nakamura, Galois rigidity of pure sphere braid groups and profinite calculus, to appear in J. Fac. Sc. Univ. of Tokyo.

[S] L.Schneps, Groupe de Grothendieck-Teichmüller et automorphismes de groupes de tresses, Note aux *Comptes Rendus de l'Académie de Sciences*, Paris.

*URA 762 du CNRS, Département de Mathématiques et Informatique
Ecole Normale Supérieure, 45 rue d'Ulm, 75230 Paris Cedex

**UA 741 du CNRS, Laboratoire de Mathématiques
Faculté des Sciences de Besançon, 16 route de Gray, 25030 Besançon Cedex