A cohomological interpretation of the Grothendieck-Teichmüller group

Pierre Lochak and Leila Schneps

Abstract

In this article we interpret the relations defining the Grothendieck-Teichmüller group $\widehat{GT}$ as cocycle relations for certain non-commutative cohomology sets, which we compute using a result due to Brown, Serre and Scheiderer. This interpretation allows us to give a new description of the elements of $\widehat{GT}$, as well as a new proof of the Drinfel'd-Ihara theorem stating that $\widehat{GT}$ contains the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. From the same methods we deduce other properties of $\widehat{GT}$ analogous to known properties of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, such as the self-centralizing of the complex conjugation element.

§1. Introduction

Let $\hat{F}_2$ denote the profinite completion of the free group on two generators, topologically generated by x and y. Set $z = (xy)^{-1}$. Let θ, ω and ι denote the three automorphisms of $\hat{F}_2$ defined as follows on x and y: $\theta(x) = y$ and $\theta(y) = x$; $\omega(x) = y$ and $\omega(y) = z$; $\iota(x) = x^{-1}$ and $\iota(y) = y^{-1}$.

For $n \geq 2$, let B_n be the Artin braid group generated by $\sigma_1, \ldots, \sigma_{n-1}$ with the relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ and $\sigma_i\sigma_j = \sigma_j\sigma_i$ whenever $\mid i - j \mid \geq 2$. There is a surjection $B_n \to S_n$ onto the group of permutations on n letters, obtained by quotienting B_n by the σ_i^2. Let K_n be the kernel of this surjection; then K_n is generated by the elements

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

for $1 \leq i < j \leq n$. We define $x_{ii} = 1$ and $x_{ji} = x_{ij}$ for $1 \leq j < i \leq n$. Let $M(0,n)$, the *mapping class group*, be the quotient of B_n by the two relations $\sigma_{n-1} \cdots \sigma_1^2 \cdots \sigma_{n-1} = 1$ and $(\sigma_{n-1} \cdots \sigma_1)^n = 1$, and let $K(0,n)$ be the image of K_n in this quotient. Conjugation by the elements $(\sigma_{n-1} \cdots \sigma_1)^i \in M(0,n)$ for $1 \leq i \leq n-1$ induces automorphisms of $K(0,n)$ which extend to the profinite completion $\hat{K}(0,n)$ (throughout this article, "conjugation of x by α" means $\alpha\, x\, \alpha^{-1}$). Let ρ denote the automorphism of $\hat{K}(0,5)$ given by conjugation by the element $(\sigma_4\sigma_3\sigma_2\sigma_1)^2$. $K(0,5)$ is generated by the five elements x_{12}, x_{23}, x_{34}, x_{45} and x_{51}, satisfying the five conditions stating that the $x_{i,i+1}$ with disjoint indices mod 5 commute, as well as the important *pentagon relation*

$$x_{51}x_{23}^{-1}x_{12}x_{34}^{-1}x_{23}x_{45}^{-1}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1} = 1 \qquad (1)$$

(see §2 for more on presentations of $K(0,5)$). The action of ρ on these generators is given by $\rho(x_{i,i+1}) = x_{i+3,i+4}$ (with indices mod 5).

Let us now recall the definition of the Grothendieck-Teichmüller group $\widehat{GT}$ defined by Drinfel'd (cf. [D]). Let $\hat{\mathbb{Z}}$ denote the profinite completion of $\mathbb{Z}$. There is an injection of $\hat{F}_2 \hookrightarrow \hat{K}(0,5)$ given by $x \mapsto x_{12}$ and $y \mapsto x_{23}$; for every $f \in \hat{F}_2$, we write $\tilde{f}$ for its image in $\hat{K}(0,5)$ under this injection. Let $\hat{F}_2'$ denote the derived subgroup of $\hat{F}_2$, in the topological sense.

Definition: Let $\underline{\widehat{GT}}$ be the monoid of pairs $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \hat{F}_2'$, satisfying the three following relations, the first two of which take place in $\hat{F}_2$ and the third in $\hat{K}(0,5)$:

(I) $\theta(f)f = 1$;

(II) $\omega^2(fx^m)\omega(fx^m)fx^m = 1$, where $m = \frac{1}{2}(\lambda - 1)$.

(III) $\rho^4(\tilde{f})\rho^3(\tilde{f})\rho^2(\tilde{f})\rho(\tilde{f})\tilde{f} = 1$.

Remark. This definition is the same as the one given by Drinfel'd [D]. Let us briefly recall his notation. For every $f \in \hat{F}_2$ and a, b in a finite or profinite group G, write $f(a,b)$ for the image of f by the homomorphism $\hat{F}_2 \to G$ sending x to a and y to b. In particular, under the identity we have $f = f(x,y)$; this notation is not to be interpreted as a substitution of variables in f, but as the images of f under various homomorphisms. The three relations (with (III) in its modified form due to Ihara, see [I1]) are generally written as (I) $f(y,x)f(x,y) = 1$; (II) $f(z,x)z^m f(y,z)y^m f(x,y)x^m = 1$ (with $z = (xy)^{-1}$) and (III) $f(x_{34},x_{45})f(x_{51},x_{12})f(x_{23},x_{34})f(x_{45},x_{51})f(x_{12},x_{23}) = 1$, which are equivalent to the forms given in our definition.

The set $\widehat{GT}$ forms a monoid under the multiplication given by:

$$\Big(\lambda, f(x,y)\Big)\Big(\mu, g(x,y)\Big) = \Big(\lambda\mu, f(x,y)g\Big(x^\lambda, f(x,y)^{-1}y^\lambda f(x,y)\Big)\Big). \tag{2}$$

This peculiar multiplication law becomes easier to understand when the elements of $\underline{\widehat{GT}}$ are interpreted as endomorphisms of $\hat{F}_2$ via $x \mapsto x^\lambda$, $y \mapsto f^{-1}y^\lambda f$; it simply expresses the composition. In other words, if F is the endomorphism associated to the pair (λ, f), then the multiplication law can be written $(\lambda, f)(\mu, g) = (\lambda\mu, fF(g))$. As for the fact that this law really defines a monoid, i.e. that the product of two pairs still satisfies relations (I), (II) and (III), it is not at all obvious, but can be deduced from the interpretation of $\underline{GT}$ as endomorphisms of higher braid groups (cf. appendix of [IM], or [LS]). Define $\widehat{GT}$ to be the group of invertible elements of $\underline{\widehat{GT}}$.

The first theorem we state is a well-known result, proved by Drinfel'd and Ihara (cf. [D],[I1], [I2]).

Theorem 1. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *injects into* $\widehat{GT}$, *with the element* $(-1,1)$ *as the image of complex conjugation.*

Ihara's proof of this theorem involves associating to each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ a pair $(\lambda_\sigma, f_\sigma) \in \hat{\mathbb{Z}}^* \times \hat{F}_2'$, showing that this pair actually lies in $\widehat{GT}$, i.e. satisfies relations (I), (II) and (III), obtaining a group homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{GT}$, and finally, showing that this homomorphism is injective. In §4, we give a new proof of the fact that the pairs $(\lambda_\sigma, f_\sigma)$ satisfy the relations (I), (II) and (III). Our method consists in proving that the f_σ take the forms (I'), (II') and (III') given in theorem 2 below; indeed this observation was the starting point for the statement and proof of theorem 2, which is the main theorem of this article. At the end of the introduction we briefly sketch our approach to theorem 1 and explain how it led to theorem 2.

The surjectivity of the inclusion $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \widehat{GT}$, i.e. the possibility that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is actually isomorphic to $\widehat{GT}$, is still an open question. Theorem 2, giving a new description of the set of elements of $\widehat{GT}$, provides some new evidence towards a favorable answer.

Theorem 2. *Let $(\lambda, f) \in \widehat{GT}$, and let $m = (\lambda - 1)/2$. Then there exist elements g and $h \in \hat{F}_2$ and $k \in \hat{K}(0,5)$ such that we have the following equalities, of which the first two take place in $\hat{F}_2$ and the third in $\hat{K}(0,5)$:*

$$(I') \qquad f = \theta(g)^{-1} g$$

$$(II') \qquad f x^m = \begin{cases} \omega(h)^{-1} h & \text{if } \lambda \equiv 1 \text{ mod } 3 \\ \omega(h)^{-1}\, xy\, h & \text{if } \lambda \equiv -1 \text{ mod } 3 \end{cases}$$

$$(III') \qquad f(x_{12}, x_{23}) = \begin{cases} \rho(k)^{-1} k & \text{if } \lambda \equiv \pm 1 \text{mod } 5 \\ \rho(k)^{-1}\, x_{34} x_{51}^{-1} x_{45} x_{12}^{-1}\, k & \text{if } \lambda \equiv \pm 2 \text{ mod } 5. \end{cases}$$

Corollary. *There is a natural $\widehat{GT}$-action on certain pro-paths of the algebraic fundamental groupoids of the moduli spaces $\mathcal{M}_{0,4}$ and $\mathcal{M}_{0,5}$ of Riemann spheres with 4 and 5 marked points respectively, based at the tangential base points near infinity and at the points with special automorphism groups.*

The description of the elements of $\widehat{GT}$ given in theorem 2, which could serve as a definition of $\widehat{GT}$, has some advantages over the usual definition given above, since rather than describing $\widehat{GT}$ as the set of all pairs satisfying three conditions, it gives a way to construct all the pairs satisfying each of the conditions, so that $\widehat{GT}$ is the intersection of these three sets. One application is the study of the action of $\widehat{GT}$ on finite covers of $\mathbb{P}^1 - \{0, 1, \infty\}$ (i.e. algebraic curves defined over $\overline{\mathbb{Q}}$), and its comparison with the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on them. Indeed, let N be a normal subgroup of finite index in $\hat{F}_2$ and let X be the finite cover of $\mathbb{P}^1 - \{0, 1, \infty\}$ corresponding to N. Then it is an important question to determine

the image in $\hat{F}_2/N$ of the set of elements $f \in \hat{F}_2$ such that for some λ the pair (λ, f) lies in $\widehat{GT}$. Using the analog of theorem 2 for the finite group $\hat{F}_2/N$, a candidate for this image can be found algorithmically: although it may be larger than the real image, it can still be used to give a bound on the order of the $\widehat{GT}$ and thus of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit of X, and thus on the degree of the field of definition of X (cf. [HS]). Indeed, if $N \supset N_1 \supset N_2 \cdots$ is a cofinal sequence of subgroups for $\hat{F}_2$, then computing this candidate image in each successive $\hat{F}_2/N_i$ and projecting the result down to $\hat{F}_2/N$ does give the exact image of the set of f's corresponding to $\widehat{GT}$ after a finite number of steps (though unfortunately this procedure is not algorithmic, because the number of steps is not known).

The proof of theorem 2 is given in §3, and its corollary is proved at the end of §4. The main point is that the relations (I), (II) and (III) of $\widehat{GT}$ are cocycle relations for the non-commutative cohomology sets given in (i), (ii) and (iii) of proposition 3 below. These cohomology sets can be explicitly determined using a result of Brown, Serre and Scheiderer, the essential part of which were written up for us by Claus Scheiderer as an appendix to this article. The results are stated in proposition 3, which is proved in §2. The forms given in theorem 2 are cocycle forms for f, so any f taking these forms satisfies relations (I), (II) and (III). But this reasoning is not necessary to check directly from the formulae in theorem 2 that the three relations are satisfied, just using the relation $xyz = 1$ in $\hat{F}_2$ and the pentagon relation (1) in $\hat{K}(0,5)$.

Proposition 3. *(i) The non-commutative cohomology set $H^1(\langle\theta\rangle, \hat{F}_2)$ is trivial;*
(ii) The set $H^1(\langle\omega\rangle, \hat{F}_2)$ consists of two elements, represented by the trivial cocycle and the cocycle given by $c_\omega = xy$;
(iii) The set $H^1(\langle\rho\rangle, \hat{K}(0,5))$ consists of two elements represented by the trivial cocycle and the cocycle given by $c_\rho = x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$.

A computation of a similar nature gives part (i) of the following proposition, and the striking statements of parts (ii) and (iii) are easy consequences of it. Proposition 3 is proved in §2, and proposition 4 at the end of §2.

Proposition 4. *(i) The group $H^0(\langle\iota\rangle, \hat{F}_2)$ of elements of $\hat{F}_2$ fixed by ι is trivial.*

(ii) The complex conjugation element $(-1, 1)$ is self-centralizing in $\widehat{GT}$, as in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(iii) $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is self-normalizing in $\widehat{GT}$. In particular, this means that if $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a normal subgroup of $\widehat{GT}$, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \widehat{GT}$.

Let us briefly sketch here the method of the proof of theorem 1 given in §4, since it was the starting point for theorem 2. Recall that Ihara associates a pair $(\lambda_\sigma, f_\sigma)$ to all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as follows. Let $\mathcal{M}_{0,4} \simeq \mathbb{P}^1 - \{0, 1, \infty\}$ denote the moduli space of Riemann spheres with 4 marked points. The set of *tangential base points* on $\mathcal{M}_{0,4}$ is the set of six

small regions of $\mathbb{P}^1 - \{0, 1, \infty\}$ neighboring the missing points 0, 1 and ∞, and lying on the real axis; they are denoted by $\{\vec{01}, \vec{10}, 0\vec{\infty}, \vec{\infty}0, 1\vec{\infty}, \vec{\infty}1\}$ (these definitions are recalled more completely in §4). Let p be the path along the real axis from $\vec{01}$ to $\vec{10}$. Then any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sends the path p to pf_σ where f_σ is a "pro-loop", i.e. an element of the profinite completion of $\pi_1(\mathcal{M}_{0,4}; \vec{01})$. Identifying $\hat{F}_2$ with $\hat{\pi}_1(\mathcal{M}_{0,4}; \vec{01})$ by taking x to be a small counterclockwise loop around 0 and y a counterclockwise loop around 1, we obtain an element $f_\sigma \in \hat{F}_2$. Let χ denote the cyclotomic character. Then Ihara associates the pair $\big(\lambda_\sigma = \chi(\sigma), f_\sigma\big)$ to σ.

Ihara then proves that the pairs $(\chi(\sigma), f_\sigma)$ satisfy relations (I), (II) and (III). We show that according to the congruence of $\chi(\sigma)$ mod 3 and 5, f_σ takes the forms given in (I'), (II') and (III') of theorem 2. We actually did this before proving theorem 2; we started from the question of whether the natural action of σ on the path r along the real axis from $\vec{01}$ to $1/2$ could not give some information on the form of f_σ. We soon found that if σ acts on r by sending it to rg_σ, then since $p = \theta(r)^{-1}r$, we must have $f_\sigma = \theta(g_\sigma)^{-1}g_\sigma$. We proceeded similarly for the path t on $\mathcal{M}_{0,4}$ running directly from $\vec{01}$ to $-\exp(4\pi\, i/3)$ together with the automorphism ω, and for analogous paths on $\mathcal{M}_{0,5}$ together with the automorphism ρ, to find that elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ took all the forms given in theorem 2. Then, attempting as usual to extend to $\widehat{GT}$ any visible combinatorial property of the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we asked ourselves whether all elements of $\widehat{GT}$ took these forms, and this led to the formulation and proof of theorem 2, and to its corollary stating that in return, the elements of $\widehat{GT}$ act naturally on the same paths on the moduli spaces. Indeed, it is more than probable that $\widehat{GT}$ is an automorphism group of the algebraic fundamental groupoids of all the $\mathcal{M}_{0,n}$ for $n \geq 4$ based at suitably defined sets of tangential base points and at the points having special automorphism group on these spaces; the difficulty even for $n = 5$ is to give a complete construction and presentation of these groupoids. In §4 we do however prove this fact for $n = 4$, which gives a stronger statement than that of the corollary to theorem 2.

§2. Proof of propositions 3 and 4.

The basic defining principles for non-commutative cohomology sets are the following. Suppose C is a group acting on a (non-commutative) group G. Then

(S0) $H^0(C, G)$ is the subgroup of C-invariant elements of G.

(S1) The elements of $H^1(C, G)$ are in bijection with the set of G-conjugacy classes of splittings of the exact sequence $1 \to G \to C \ltimes G \to C \to 1$.

Part of the following proposition was communicated to us by J-P. Serre; the proofs of the different parts are due to him, to Brown and to Scheiderer. Since the full proof was not actually written up anywhere, Claus Scheiderer was willing to write up a complete proof

which is included as an appendix to this article. Proposition 5 is valid for both discrete and profinite groups (see the last remark in the appendix). In our proof of proposition 8 below, we use the "discrete converse" implication of proposition 5, and in the proof of proposition 3 which follows it, we use the "profinite direct" implication; the appendix of course contains a complete proof of all the implications.

Proposition 5. *Let G be a discrete or a profinite group. Let $G_1, \ldots, G_r$ be finite subgroups of G, and suppose that for every prime p and every p-primary discrete G-module M the restriction map*

$$H^n(G, M) \longrightarrow \prod_{i=1}^{r} H^n(G_i, M) \qquad (*)$$

is bijective for $n > n_0 = n_0(M)$. Then:

(a) $\mathrm{vcd}_p(G) < \infty$ *for every prime p;*

(b) every nontrivial finite subgroup of G is conjugate to a subgroup of precisely one of $G_1, \ldots, G_r$;

(c) $G_i \cap xG_ix^{-1} = \{1\}$ *for $x \in G$, $x \notin G_i$, $i = 1, \ldots, r$.*

Conversely, if $G_1, \ldots, G_r$ are finite subgroups of G and (a), (b) and (c) hold, then there exists an integer $n_0(p)$ such that (*) is bijective for every p-primary discrete G-module M and every $n > n_0(p)$.

Now, following Serre (cf. [S1]), we say that a discrete group G is *good* if it has the same (ordinary, not non-commutative) cohomology as its profinite completion, i.e. if for every finite G-module M the canonical maps $H^n(\hat{G}, M) \to H^n(G, M)$ are bijective for all $n \geq 0$. Free groups and semi-direct products of free groups are good (cf. [S1, p.14]), so in particular F_2 and $K(0,5)$ are both good ($K(0,5)$ is a semi-direct product $F_2 \ltimes F_3$, described explicitly below). Let us say that if a group (discrete or profinite) satisfies the hypotheses of proposition 5, it satisfies *hypothesis (H)*. We want to verify hypothesis (H) on discrete rather than profinite groups, and use it to compute the non-commutative cohomology sets in the statement of proposition 3, for which purpose we need the following lemma.

Lemma 6. *Let G be a good discrete group which injects into its profinite completion $\hat{G}$, and suppose that G satisfies hypothesis (H) for a family $G_1, \ldots, G_r$ of finite cyclic subgroups of G. Then $\hat{G}$ also satisfies (H) for the (images of the) same family.*

Proof. For all sufficiently large n, the restriction map $H^n(G, M) \to \prod_{i=1}^{r} H^n(G_i, M)$ is an isomorphism (for all M as in proposition 5). Since G is good, the left-hand side is the same as $H^n(\hat{G}, M)$, so since the G_i are subgroups of $\hat{G}$ and the restriction map is the same, $\hat{G}$ also satisfies hypothesis (H) for the family $G_1, \ldots, G_r$. ♣

Lemma 7. *Let G be a good discrete group which injects into its profinite completion,*

and let ϕ be an automorphism of prime order p of G (and $\hat{G}$). Let H denote the semi-direct product $\langle\phi\rangle \ltimes G$. Then H is good and injects into its profinite completion (which is isomorphic to $\langle\phi\rangle \ltimes \hat{G}$). Suppose H satisfies hypothesis (H) for a family $G_1, \ldots, G_r$ of finite cyclic subgroups of prime order of H. Then the non-commutative cohomology set $H^1(\langle\phi\rangle, G)$ is in bijection with the subset of the groups $G_1, \ldots, G_r$ which are splittings of the exact sequence

$$1 \to G \to H = \langle\phi\rangle \ltimes G \to \langle\phi\rangle \to 1.$$

Moreover, the sets $H^1(\langle\phi\rangle, G)$ and $H^1(\langle\phi\rangle, \hat{G})$ are equal.

Proof. The first assertions, that H is good and injects into its profinite completion, and that $\hat{H} = \langle\phi\rangle \ltimes \hat{G}$ are all standard (cf. [N, Prop. 1.2.4] for example). By the defining property (S1), we know that the set $H^1(\langle\phi\rangle, G)$ is in bijection with the set of G-conjugacy classes of splittings of the exact sequence in the statement.

Short digression. Let us show how to make the correspondence between splittings G_i and elements of $H^1(\langle\phi\rangle, G)$ explicit. Any G_i which is a splitting of the exact sequence contains p elements of the form $(\phi^{-1}, \alpha)^i \in \langle\phi\rangle \ltimes G$ for $0 \leq i \leq n-1$, where α is in G; these powers have the form $(\phi^{-i}, \phi^{i-1}(\alpha) \cdots \phi(\alpha)\alpha)$. The relation $(\phi^{-1}, \alpha)^n = 1$ (which we sometimes simply write $(\phi^{-1}\alpha)^n = 1$) implies that $\phi^{n-1}(\alpha) \cdots \phi(\alpha)\alpha = 1$, so a cocycle for ϕ is obtained by defining $c_{\phi^i} = \phi^{i-1}(\alpha) \cdots \phi(\alpha)\alpha$.

Back to the proof of the lemma, any splitting of the exact sequence is conjugate to a unique G_i since hypothesis (H) implies (b) of proposition 5 (by assumption, the G_i have no non-trivial subgroups). Since all members of a G-conjugacy class of splittings are a fortiori H-conjugate, they are all conjugate to the same G_i, so we obtain a map from $H^1(\langle\phi\rangle, G) \to \{G_1, \ldots, G_r\}$. Now, an H-conjugate of a splitting is actually always equal to a G-conjugate of it, and therefore lies in the same G-conjugacy class of splittings. To see this, we simply note that if a splitting is generated by (ϕ^{-1}, α) as in the digression above, then its conjugate by $\phi = (\phi, 1)$ is equal to its conjugate by $\alpha = (1, \alpha)$, since

$$(\phi, 1)(\phi^{-1}, \alpha)(\phi^{-1}, 1) = \big(\phi^{-1}, \phi(a)\big) = (1, \alpha)(\phi^{-1}, \alpha)(1, \alpha^{-1}).$$

Thus our map from $H^1(\langle\phi\rangle, G) \to \{G_1, \ldots, G_r\}$ is injective, and it is obviously surjective onto the subset of the G_i which are actually splittings of the exact sequence.

Finally, the equality of the cohomology sets for G and $\hat{G}$ is a consequence of the fact that $\hat{H}$ satisfies hypothesis (H) for the same family of G_i as H by lemma 6. ♣

In particular the trivial cocycle is associated to the trivial splitting given by the G-conjugate of the subgroup $\langle\phi\rangle$ which appears in the list $G_1, \ldots, G_r$ (by (b) of proposition 5, such a subgroup must appear in the list).

Now we can apply these results to proving proposition 3. We said above that $K(0,5)$ is good because it is a semi-direct product of free groups; let us recall that presentation and another one here. Set $x_1 = x_{12}$, $x_2 = x_{23}$, $x_3 = x_{24}$, $x_4 = x_{13}$ and $x_5 = x_{34}$, where the x_{ij} are the generators defined in §1. Then $K(0,5) = \langle x_4, x_5\rangle \ltimes \langle x_1, x_2, x_3\rangle \simeq F_2 \ltimes F_3$, with the following relations:

$$\begin{cases} x_4^{-1}x_1x_4 = x_2x_1x_2^{-1} \\ x_4^{-1}x_2x_4 = x_2x_1x_2x_1^{-1}x_2^{-1} \\ x_4^{-1}x_3x_4 = x_2x_1x_2^{-1}x_1^{-1}x_3x_1x_2x_1^{-1}x_2^{-1} \\ x_5^{-1}x_1x_5 = x_1 \\ x_5^{-1}x_2x_5 = x_2x_3x_2x_3^{-1}x_2^{-1} \\ x_5^{-1}x_3x_5 = x_2x_3x_2^{-1}. \end{cases}$$

For two elements a and b of a group, let $(a,b) = aba^{-1}b^{-1}$ denote their commutator. Rewriting the above presentation in the generators x_{12}, x_{23}, x_{34}, $x_{45} = x_{12}x_{13}x_{23} = x_1x_4x_2$ and $x_{51} = x_{23}x_{24}x_{34} = x_2x_3x_5$ gives:

$$\begin{cases} (x_{12}, x_{34}) = 1 \\ (x_{23}, x_{45}) = 1 \\ (x_{34}, x_{51}) = 1 \\ (x_{45}, x_{12}) = 1 \\ (x_{51}, x_{23}) = 1 \\ x_{51}x_{23}^{-1}x_{12}x_{34}^{-1}x_{23}x_{45}^{-1}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1} = 1. \end{cases}$$

Let θ, ω and ι be the automorphisms of $\hat{F}_2$ given by: $\theta(x) = y$ and $\theta(y) = x$, $\omega(x) = (xy)^{-1}$ and $\omega(y) = x$, and $\iota(x) = x^{-1}$ and $\iota(y) = y^{-1}$. Let ρ be the automorphism of $K(0,5)$ given by $\rho(x_{i,i+1}) = \rho(x_{i+3,i+4})$ (indices considered mod 5). This is easily seen to be an automorphism by considering the second presentation of $K(0,5)$; it is the same automorphism as the one defined in §1, given by conjugation by $(\sigma_4\sigma_3\sigma_2\sigma_1)^2$ inside $M(0,5)$.

Let F_θ, F_ω, F_ι and K_ρ denote the semi-direct products $\langle\theta\rangle \ltimes F_2$, $\langle\omega\rangle \ltimes F_2$, $\langle\iota\rangle \ltimes F_2$ and $\langle\rho\rangle \ltimes K(0,5)$ respectively. Let $\hat{F}_\theta$, $\hat{F}_\omega$, $\hat{F}_\iota$ and $\hat{K}_\rho$ denote the profinite completions of these groups (which are all given by the same semi-direct products with the discrete infinite group replaced by its profinite completion).

Proposition 8. *The following groups satisfy hypothesis (H) for the given families of finite subgroups:*

(i) $\hat{F}_\iota$ *for* $G_1 = \langle\iota\rangle$, $G_2 = \langle\iota x\rangle$ *and* $G_3 = \langle\iota y\rangle$;

(ii) $\hat{F}_\theta$ *for* $G_1 = \langle\theta\rangle$;

(iii) $\hat{F}_\omega$ *for* $G_1 = \langle\omega\rangle$, $G_2 = \langle\omega^{-1}xy\rangle$;

(iv) $\hat{K}_\rho$ *for* $G_1 = \langle \rho \rangle$ *and* $G_2 = \langle \rho^{-1} x_{34} x_{51}^{-1} x_{45} x_{12}^{-1} \rangle$.

Proof. By lemma 6 (and the fact that F_2 and $K(0,5)$ both inject into their profinite completions), it suffices to show hypothesis (H) for the discrete groups. The first three groups are all freely generated; F_θ by an element of order 2 and an element of infinite order, namely x and θ, F_ω by two elements of order 3, namely ω and $x\omega$, and F_ι by three elements of order 2, namely ι, $x\iota$ and $y\iota$. We check that these discrete groups satisfy conditions (a), (b) and (c) of proposition 5; (a) is well-known, and both (b) and (c) are consequences of the fact that the given subgroups freely generate the groups (cf. [Br, p. 54] or [S3,I.4.3]). By the converse implication of the discrete version of proposition 5, these then imply hypothesis (H) for the discrete groups, and thus for their profinite completions since they are good, by lemma 6. This proof, the essence of proposition 5 and the idea of using it also in the case of $\hat{K}(0,5)$ was suggested to us by Serre (cf. [S2]). For a briefer argument valid for these three groups but not for $\hat{K}(0,5)$, see the commentary following the proof of proposition 3 below.

Let us show that K_ρ satisfies hypothesis (H) for the family $G_1 = \langle \rho \rangle$ and $G_2 = \langle \rho^{-1} x_{34} x_{51}^{-1} x_{45} x_{12}^{-1} \rangle$. Consider the element $c_5 = \sigma_4 \sigma_3 \sigma_2 \sigma_1$ in the full mapping class group $M(0,5)$, whose associated permutation is the 5-cycle (15432). Conjugation by c_5^2 acts on the pure subgroup $K(0,5)$ of $M(0,5)$ like the automorphism ρ, and the semi-direct product $\langle \rho \rangle \ltimes K(0,5)$ can be identified with the subgroup $\langle c_5 \rangle \ltimes K(0,5)$ of $M(0,5)$. Now, all cyclic subgroups of order 5 of $M(0,5)$ are conjugate to $\langle c_5 \rangle$ (cf. [HM, Corollary, p. 508]). We need to determine the number of $K(0,5)$-conjugacy classes of the set of all $M(0,5)$-conjugates of $\langle c_5 \rangle$ which lie inside the subgroup $\langle c_5 \rangle \ltimes K(0,5)$. These subgroups can be distinguished amongst all the $M(0,5)$-conjugates of $\langle c_5 \rangle$ simply by considering the permutations associated to their elements; they must lie in the preimage of the subgroup $\langle (15432) \rangle$ under the surjection $M(0,5) \to S_5$. This means that for a subgroup $\langle \gamma c_5 \gamma^{-1} \rangle$ with $\gamma \in M(0,5)$ to lie inside $\langle c_5 \rangle \ltimes K(0,5)$, the permutation of the element $\gamma c_5 \gamma^{-1}$ must be a non-trivial power of (15432). There are only four such powers, so there are at most four $K(0,5)$-conjugacy classes of subgroups of order 5 in $\langle c_5 \rangle \ltimes K(0,5)$, given by any of the many possible choices of a $\gamma_i \in M(0,5)$ for each $i = 1,2,3,4$ such that the element $\gamma_i c_5 \gamma_i^{-1}$ has permutation $(15432)^i$. It follows from a theorem in [HM] that the number of $K(0,5)$-conjugacy classes is in fact exactly two, and we can determine representatives of them explicitly. Let us work this out in detail.

Choose four such elements γ_i giving at most four $K(0,5)$-conjugacy classes of order 5 in $\langle c_5 \rangle \ltimes K(0,5)$. We need to determine if they are not actually $K(0,5)$-conjugate amongst themselves. Suppose that there exists $\alpha \in K(0,5)$ such that

$$\alpha \langle \gamma_i c_5 \gamma_i^{-1} \rangle \alpha^{-1} = \langle \gamma_j c_5 \gamma_j^{-1} \rangle,$$

for $1 \leq i \neq j \leq 4$. This means that

$$\alpha\gamma_i c_5 \gamma_i^{-1}\alpha^{-1} = \gamma_j c_5^{ij^{-1}} \gamma_j^{-1},$$

where the power ij^{-1} on the right (considered in $(\mathbb{Z}/5\mathbb{Z})^*$) is necessary for both sides of the equation to have the same permutation. This in turn implies that

$$(\gamma_j^{-1}\alpha\gamma_i)c_5(\gamma_i^{-1}\alpha^{-1}\gamma_j) = c_5^{ij^{-1}},$$

so the element $\gamma_j^{-1}\alpha\gamma_i$ normalizes the subgroup $\langle c_5\rangle$ of $M(0,5)$. Now, it is known that the centralizer of c_5 in $M(0,5)$ is reduced to $\langle c_5\rangle$ and the quotient of the normalizer by the centralizer contains two elements (cf. [HM, Theorem 10, p. 509]). A non-trivial element of the normalizer is given by $\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_2$: we have

$$(\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_2)^{-1}c_5(\sigma_3\sigma_2\sigma_1\sigma_2\sigma_3\sigma_2) = \sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_4\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3 = c_5^{-1}.$$

Thus the subgroups $\langle\gamma_1 c_5\gamma_1^{-1}\rangle$ and $\langle\gamma_4 c_5\gamma_4^{-1}\rangle$ are $K(0,5)$-conjugate, as are the subgroups $\langle\gamma_2 c_5\gamma_2^{-1}\rangle$ and $\langle\gamma_3 c_5\gamma_3^{-1}\rangle$. On the other hand, since the normalizer consists of two elements only, the subgroups $\langle\gamma_1 c_5\gamma_1^{-1}\rangle$ and $\langle\gamma_2 c_5\gamma_2^{-1}\rangle$ cannot be $K(0,5)$-conjugate. This shows that there are exactly two $K(0,5)$-conjugacy classes of subgroups of order 5 in $\langle c_5\rangle \ltimes K(0,5)$, so also in the isomorphic abstract group $\langle\rho\rangle \ltimes K(0,5)$. The final step is to determine them. One is of course represented simply by $\langle c_5\rangle$. The other is represented by any choice of $\langle\gamma_2 c_5\gamma_2^{-1}\rangle$, the element $\gamma_2 c_5\gamma_2^{-1}$ having the permutation $(15432)^2$. Let us choose $\gamma_2 = \sigma_3\sigma_2\sigma_1\sigma_2\sigma_1$, which has the permutation (4312), so that the permutation of $\gamma_2 c_5\gamma_2^{-1}$ is indeed $(4312)(15432)(4213) = (14253) = (15432)^2$. After generous simplification, we find that

$$\begin{aligned}\gamma_2 c_5^{-1}\gamma_2^{-1} &= c_5^{-1}x_{13}x_{51}c_5^{-1} = c_5^{-1}x_{12}^{-1}x_{45}x_{23}^{-1}x_{51}c_5^{-1}\\ &= c_5^{-2}x_{51}^{-1}x_{34}x_{12}^{-1}x_{45} = c_5^{-2}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1},\end{aligned}$$

the last equality following from the the commutation relations of $K(0,5)$. As in lemma 7 and the remark following it, since this element has order 5 and $\rho = c_5^2$, setting $s_\rho := x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$ defines a cocycle for ρ. This concludes the proof of proposition 8. ♣

Now we can finish the proof of proposition 3. All the groups G_i in the families given in proposition 8 are splittings of the associated exact sequences (as in lemma 7), so by the profinite direct implication of proposition 5, we see that $H^1(\langle\theta\rangle, \hat{F}_2)$ contains only one element, corresponding to G_1, the trivial splitting. $H^1(\langle\omega\rangle, \hat{F}_2)$ contains two elements, represented by the trivial cocycle, i.e. the group G_1, and the cocycle given by $b_\omega = xy$, corresponding to G_2. Finally, $H^1(\langle\rho\rangle, \hat{K}(0,5))$ also contains two elements, represented by the trivial cocycle corresponding to G_1 and the cocycle given by $s_\rho = x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$ corresponding to G_2. This concludes the proof of proposition 3. ♣

Commentary. Proposition 8 was stated and proved in order to prove proposition 3, and to underline the analogous treatment of the three cohomology sets corresponding to θ, ω and ρ. However, Claus Scheiderer (and the referee) pointed out to us that it is not necessary to make a detour through proposition 5 to compute the cohomology sets $H^1(\langle\theta\rangle, \hat{F}_2)$, $H^1(\langle\omega\rangle, \hat{F}_2)$ and $H^0(\langle\iota\rangle, \hat{F}_2)$. Indeed, since the three profinite groups $\hat{F}_\iota$, $\hat{F}_\theta$ and $\hat{F}_\omega$ are free *profinite* products, in order to check that the subgroups G_i exactly describe the cohomology sets as in lemma 7, it suffices to use the profinite "Kurosh subgroup theorem" given as the corollary to the proposition in Scheiderer's appendix to this paper. Since $\hat{K}_\rho$ is not a free profinite product, this argument unfortunately does not apply.

Let us prove proposition 4. By proposition 8 (i), we know that the profinite semi-direct product $\hat{F}_\iota = \langle\iota\rangle \ltimes \hat{F}_2$ satisfies (H) for the family of finite subgroups G_1, G_2 and G_3. Therefore by the profinite direct implication of proposition 5, the G_i satisfy (c) of proposition 5, so in particular the only elements of $\hat{F}_\iota$ which commute with ι are 1 and ι. By the principle (S0), the group $H^0(\langle\iota\rangle, \hat{F}_2)$ is in bijection with the elements of $\hat{F}_2$ centralizing ι inside $\hat{F}_\iota$, so it consists of only the trivial element. This proves proposition 4 (i).

To prove proposition 4 (ii), let (λ, f) be an element of $\widehat{GT}$ which commutes with $(-1, 1)$. Multiplying on the left and on the right by $(-1, 1)$ via the multiplication formula (2), we obtain the equality:

$$\big(-\lambda, f(x, y)\big) = \big(-\lambda, f(x^{-1}, y^{-1})\big),$$

which implies $f(x, y) = f(x^{-1}, y^{-1})$, i.e. $f(x, y)$ is fixed under the automorphism ι of $\hat{F}_2$. But by (i), the only element of $\hat{F}_2$ centralizing ι in the semi-direct product $\langle\iota\rangle \ltimes \hat{F}_2$ is 1, so $f(x, y) = 1$, and $\lambda = \pm 1$ by relation (II).

Finally, to prove proposition 4 (iii), we consider $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as a subgroup of $\widehat{GT}$ by theorem 1, and suppose it is normal. Let $(\lambda, f) \in \widehat{GT}$; we will show that $(\lambda, f) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Indeed, $(-1, 1) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \subset \widehat{GT}$ since this element corresponds to complex conjugation, so $(\lambda, f)^{-1}(-1, 1)(\lambda, f) \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is assumed normal, and it is an element of order 2 in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (pairs are multiplied according to (2)). But all such elements are conjugates of complex conjugation by elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so there exists $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that writing $(\lambda_\sigma, f_\sigma)$ for the image of σ under the injection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \widehat{GT}$, we have

$$(\lambda, f)^{-1}(-1, 1)(\lambda, f) = (\lambda_\sigma, f_\sigma)^{-1}(-1, 1)(\lambda_\sigma, f_\sigma).$$

Thus $(\lambda_\sigma, f_\sigma)(\lambda, f)^{-1}$ commutes with $(-1, 1)$, so by proposition 4 (ii), this product is equal to 1 or $(-1, 1)$, so (λ, f) is equal to $(\pm\lambda_\sigma, f_\sigma)$, which lie in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The same argument shows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is self-normalizing in $\widehat{GT}$, which concludes the proof of proposition 4. ♣

§3. Proof of theorem 2.

Let $(\lambda, f) \in \widehat{GT}$. Let us prove (I'). Since every element $(\lambda, f) \in \widehat{GT}$ satisfies the equation $f(y,x)f(x,y) = \theta(f)f = 1$ in $\hat{F}_2$, $a_\theta := f$ defines a cocycle for θ. But by (i) of proposition 3, the non-commutative cohomology set $H^1(\langle\theta\rangle, \hat{F}_2)$ is trivial, so a_θ is a coboundary, which means that there exists $g = g(x,y) \in \hat{F}_2$ such that $f = \theta(g)^{-1}g$.

For (II'), relation (II) of $\widehat{GT}$ says that $f(z,x)z^m f(y,z)y^m f(x,y)x^m = 1$, i.e. $\omega^2(fx^m)$ $\omega(fx^m)fx^m = 1$, so $b_\omega := fx^m$ defines a cocycle for ω. Thus by (ii) of proposition 3, fx^m is equivalent up to coboundaries to either 1 or xy, which means that there exists $h = h(x,y) \in \hat{F}_2$ such that either $fx^m = \omega(h)^{-1}h$ or $fx^m = \omega(h)^{-1}\,xy\,h$.

Recall that $f \in \hat{F}_2'$. Suppose $fx^m = \omega(h)^{-1}h$, i.e.

$$f(x,y)x^m = \omega(h)^{-1}h = h(z,x)^{-1}h(x,y) = h\big((xy)^{-1},x\big)^{-1}h(x,y),$$

and write $h(x,y) \equiv x^a y^b \bmod \hat{F}_2'$, with $a, b \in \hat{\mathbb{Z}}$. Then mod $\hat{F}_2'$ we have $x^m = (xy)^a x^{-b} x^a y^b$ $= x^{2a-b}y^{a+b}$, so $b = -a$ and $m = 3a$. Thus $m \equiv 0 \bmod 3$. On the other hand, if $fx^m = \omega(h)^{-1}xyh$, then mod $\hat{F}_2'$, we have $x^m = (xy)^a x^{-b}xyx^a y^b = x^{2a-b+1}y^{a+b+1}$, so $b = -a-1$ and $m = 3a+2$, so $m \equiv 2 \bmod 3$.

Finally, for (III'), relation (III) of $\widehat{GT}$ says that $c_\rho := f(x_{12}, x_{23})$ defines a cocycle for ρ. Recall that the automorphism ρ of $\hat{M}(0,5)$ is given, via an abuse of notation, by $\rho(g) = \rho g \rho^{-1}$ where $\rho = (\sigma_4\sigma_3\sigma_2\sigma_1)^2$. By (iii) of proposition 3, this cocycle is equivalent up to coboundaries to the trivial cocycle or the non-trivial one defined by $s_\rho := x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$ introduced in §2. It remains to show that this equivalence depends only on the congruence of $\pm\lambda \bmod 5$. We do this by comparing relation (II), in which the quantity $m = (\lambda-1)/2$ occurs, with the coboundary/cocycle forms of $f(x_{12}, x_{23})$, in the group $\hat{K}(0,5)$ modulo the second commutator group $\hat{K}(0,5)^{(2)} = (\hat{K}(0,5), \hat{K}'(0,5))$. Before doing so, we calculate the image of $f(x,y)$ in the quotient $\hat{F}_2/\hat{F}_2^{(2)}$, where $\hat{F}_2^{(2)}$ denotes the second commutator group $(\hat{F}_2, \hat{F}_2')$.

Denote by G either $\hat{F}_2/\hat{F}_2^{(2)}$ or $\hat{K}(0,5)/\hat{K}(0,5)^{(2)}$. Then G is a torsion free nilpotent group and for any prime ℓ, it injects into its $\mathbb{Q}_\ell$-envelope $G(\mathbb{Q}_\ell)$ (cf. Appendix A of [Q] for details). Like G, the group $G(\mathbb{Q}_\ell)$ is nilpotent and torsion free, but it is also divisible. It has a Lie algebra $LG(\mathbb{Q}_\ell)$, and the exponential map defines an isomorphism between $G(\mathbb{Q}_\ell)$ and $LG(\mathbb{Q}_\ell)$ for all ℓ, via the Campbell-Hausdorff formula. Because in our case G has length two, this construction is actually defined not only over $\mathbb{Q}_\ell$, but in fact over $\mathbb{Z}_\ell[\frac{1}{2}]$ $(= \mathbb{Z}_\ell$ for $\ell \neq 2)$. With (or without) this in mind, we now turn to the computation, where for simplicity we drop the index ℓ from the groups and Lie algebras.

For any prime ℓ, let $G_F = \big(\hat{F}_2/\hat{F}_2^{(2)}\big)(\mathbb{Q}_\ell)$ and $G_K = \big(\hat{K}(0,5)/\hat{K}(0,5)^{(2)}\big)(\mathbb{Q}_\ell)$. Then the map $\tilde{w} \mapsto \exp(\tilde{w}) = w$ gives the isomorphism from LG_F (resp. LG_K) to G_F (resp.

G_K). The multiplication law in LG_F (resp. LG_K) corresponding to the multiplication law in G_F (resp. G_K) is given by the Campbell-Hausdorff formula: $ww' = \exp(\tilde{w} * \tilde{w}')$ with

$$\tilde{w} * \tilde{w}' = \tilde{w} + \tilde{w}' + \frac{1}{2}[\tilde{w}, \tilde{w}'],$$

where $[\tilde{w}, \tilde{w}'] = \tilde{w}\tilde{w}' - \tilde{w}\tilde{w}'$. The Lie algebra LG_F is generated as a $\mathbb{Q}_\ell$-vector space by x, y and $[x, y]$ (for all $g \in \hat{F}_2$, we continue to write g for the corresponding element of G_F).

Considering $f(x, y)$ in G_F, write $\widetilde{f(x, y)}$ for the corresponding element in LG_F. Then we have

$$f(x, y) = \exp(\widetilde{f(x, y)}) = \exp(\alpha_\ell[\tilde{x}, \tilde{y}]),$$

i.e. since $f(x, y)$ is in the derived subgroup, there exists $\alpha_\ell \in \mathbb{Z}_\ell[\frac{1}{2}]$ such that $\widetilde{f(x, y)} = \alpha_\ell[\tilde{x}, \tilde{y}]$. Let us calculate α_ℓ. Let m_ℓ denote the $\mathbb{Z}_\ell$-component of $m = (\lambda - 1)/2 \in \hat{\mathbb{Z}}$. Rewriting relation (II) in LG_F, with $z = (xy)^{-1}$, gives

$$\widetilde{f(z, x)} * m_\ell\tilde{z} * \widetilde{f(y, z)} * m_\ell\tilde{y} * \widetilde{f(x, y)} * m_\ell\tilde{x} = 0.$$

Expanding this expression using the Campbell-Hausdorff formula, we find

$$(\alpha_\ell[\tilde{z}, \tilde{x}] + m_\ell\tilde{z}) * (\alpha_\ell[\tilde{y}, \tilde{z}] + m_\ell\tilde{y}) * (\alpha_\ell[\tilde{x}, \tilde{y}] + m_\ell\tilde{x}) = 3\alpha_\ell[\tilde{x}, \tilde{y}] - \frac{1}{2}m_\ell[\tilde{x}, \tilde{y}] - \frac{1}{2}m_\ell^2[\tilde{x}, \tilde{y}] = 0$$

so $\alpha_\ell = m_\ell(m_\ell + 1)/6$. Note that since $\lambda \in \hat{\mathbb{Z}}^*$, m cannot be congruent to 1 mod 3, so $m(m + 1) \equiv 0 \bmod 6$, and $\alpha = (\alpha_\ell)_\ell \in \hat{\mathbb{Z}}$.

Before finishing the proof of theorem 2, we take a moment to draw attention to the fact just proved, by stating it as follows.

Lemma 9. *Let $f \in \hat{F}_2$ and suppose there exists $\lambda \in \hat{\mathbb{Z}}^*$ such that $(\lambda, f) \in \widehat{GT}$. Then the set of $\mu \in \hat{\mathbb{Z}}^*$ such that $(\mu, f) \in \widehat{GT}$ is given by $\{\pm\lambda\}$. These two values of λ can be determined by considering the image of f in $\hat{F}_2/\hat{F}_2^{(2)}$, which takes the form $(x, y)^r$ for some $r \in \hat{\mathbb{Z}}$; we have $\lambda^2 = 24r + 1$.*

Proof. This lemma was actually proved just before its statement, but we give another simple argument for the first part. Suppose $f \in \hat{F}_2$ and (λ, f) and (μ, f) lie in $\widehat{GT}$. Let F_λ and F_μ denote the two automorphisms of $\hat{F}_2$ associated to these two elements. Consider the automorphism $F_\lambda^{-1}F_\mu$; by the multiplication formula (2), it is associated to the pair $(\lambda^{-1}\mu, 1)$. Set $n = (\lambda^{-1}\mu - 1)/2$; if this pair is in $\widehat{GT}$ it must satisfy relation (II), i.e. $x^n z^n y^n = 1$. But this is possible if and only if $n = 0$ or -1. ♣

The following lemma concludes the proof of theorem 2.

Lemma 10. *Let $(\lambda, f) \in \widehat{GT}$. If $f(x_{12}, x_{23})$ has the coboundary form $\rho(k)^{-1}k$ for some $k \in \hat{K}(0, 5)$, then $m \equiv 0$ or 4 mod 5, whereas if $f(x_{12}, x_{23})$ has the cocycle form $\rho(k)^{-1}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}k$, then $m \equiv 1$ or 3 mod 5.*

Proof. We use the Campbell-Hausdorff formula to calculate in the group G_K, or rather in LG_K. As before, for all $g \in \hat{K}(0,5)$, we continue to write g for the corresponding element of G_K. Suppose $f(x_{12}, x_{23}) = \rho(k)^{-1}k$. The Lie algebra LG_K is generated as a $\mathbb{Q}_\ell$-vector space by the $x_{i,i+1}$ and by the non-zero brackets of them, namely $[\tilde{x}_{12}, \tilde{x}_{23}]$, $[\tilde{x}_{23}, \tilde{x}_{34}]$, $[\tilde{x}_{34}, \tilde{x}_{45}]$, $[\tilde{x}_{45}, \tilde{x}_{51}]$, $[\tilde{x}_{51}, \tilde{x}_{12}]$. However, rewriting the pentagon relation (1) of $\hat{K}(0,5)$ in LG_K gives the relation

$$[\tilde{x}_{12}, \tilde{x}_{23}] + [\tilde{x}_{23}, \tilde{x}_{34}] + [\tilde{x}_{34}, \tilde{x}_{45}] + [\tilde{x}_{45}, \tilde{x}_{51}] + [\tilde{x}_{51}, \tilde{x}_{12}] = 0,$$

so we do not need $[\tilde{x}_{51}, \tilde{x}_{12}]$ in a basis of LG_K. Thus the first order part of any element of LG_K is a linear combination of the five variables $\tilde{x}_{i,i+1}$ with coefficients in $\mathbb{Z}_\ell$ and its second order part is a linear combination of the four brackets $\tilde{y}_1 := [\tilde{x}_{12}, \tilde{x}_{23}]$, $\tilde{y}_2 := [\tilde{x}_{23}, \tilde{x}_{34}]$, $\tilde{y}_3 := [\tilde{x}_{34}, \tilde{x}_{45}]$, $\tilde{y}_4 := [\tilde{x}_{45}, \tilde{x}_{51}]$ with coefficients in $\mathbb{Z}_\ell[\frac{1}{2}]$. In particular $k = \exp(\tilde{k})$ with

$$\tilde{k} = a_1\tilde{x}_{12} + a_2\tilde{x}_{23} + a_3\tilde{x}_{34} + a_4\tilde{x}_{45} + a_5\tilde{x}_{51} + b_1\tilde{y}_1 + b_2\tilde{y}_2 + b_3\tilde{y}_3 + b_4\tilde{y}_4,$$

so $\rho(k)^{-1} = \exp(-\rho(\tilde{k}))$ with

$$\rho(\tilde{k}) = a_1\tilde{x}_{45} + a_2\tilde{x}_{51} + a_3\tilde{x}_{12} + a_4\tilde{x}_{23} + a_5\tilde{x}_{34} + b_1\tilde{y}_4 - b_2(\tilde{y}_1 + \tilde{y}_2 + \tilde{y}_3 + \tilde{y}_4) + b_3\tilde{y}_1 + b_4\tilde{y}_2.$$

Expanding the identity $\exp(-\rho(\tilde{k}) * \tilde{k}) = f(x,y)$ to the first order, we see that the first order part of $-\rho(\tilde{k}) * k$ is 0, which shows that all the a_i are equal. The equality

$$-\rho(\tilde{k}) * k = \frac{m_\ell(m_\ell+1)}{6}[\tilde{x}_{12}, \tilde{x}_{23}]$$

becomes

$$(b_1 + b_2 - b_3)\tilde{y}_1 + (2b_2 - b_4)\tilde{y}_2 + (b_2 + b_3)\tilde{y}_3 + (-b_1 + b_2 + b_4)\tilde{y}_4 = \frac{m_\ell(m_\ell+1)}{6}\tilde{y}_1.$$

Solving the system obtained in the b_i, we see that $b_2 = -2b_3$, $b_1 = 2b_3$, $b_4 = -2b_3$ and $5b_3 = m_\ell(m_\ell+1)/6$. Now, the denominator of b_3 is at worst 2, and thus we see that for $\ell = 5$, $m_5(m_5+1)$ must be congruent to 0 mod 5, i.e. $m_5 \equiv 0$ or 4 mod 5, so $m \equiv 0$ or 4 mod 5. The computation for the cocycle form of $f(x_{12}, x_{23})$ is analogous up to the following small differences. We now need to make sure the equation

$$-\rho(\tilde{k}) * \tilde{x}_{34} * (-\tilde{x}_{51}) * \tilde{x}_{45} * (-\tilde{x}_{12}) * \tilde{k} = \frac{m_\ell(m_\ell+1)}{6}[\tilde{x}_{12}, \tilde{x}_{23}]$$

is satisfied. Elimination of the first order terms gives the following expression for $\tilde{k}$:

$$\tilde{k} = ax_{12} + (a-1)x_{23} + (a-1)x_{34} + (a-1)x_{45} + ax_{51} + b_1y_1 + b_2y_2 + b_3y_3 + b_4y_4.$$

Calculation of the second order term of $-\rho(\tilde{k}) * \tilde{x}_{34} * (-\tilde{x}_{51}) * \tilde{x}_{45} * (-\tilde{x}_{12}) * \tilde{k}$ gives a system to solve in the b_i similar to the one in the coboundary case, except that we find $5b_3 = 1/2 + m_\ell(m_\ell+1)/6 = (m_\ell^2 + m_\ell + 3)/6$, so by the same reasoning as before, $m_5^2 + m_5 + 3 \equiv 0 \bmod 5$, so $m \equiv 1$ or $3 \bmod 5$. ♣

§4. Proof of theorem 1 and of the corollary to theorem 2.

We first need to recall some well-known facts about pro-paths on algebraic varieties defined over $\mathbb{Q}$ and the Galois action on them.

Definitions. (1) Let X be an algebraic variety. A *pro-point* $\tilde{a}$ on X is a collection of points a_Y, one on each finite cover Y of X, such that for any two such covers Y and Y' with Y a cover of Y', the image of a_Y under the covering map $Y \to Y'$ is $a_{Y'}$.

If X is defined over $\mathbb{Q}$ and $\tilde{a} = \{a_Y\}_Y$ is a pro-point of X, then $\tilde{a}$ is said to be defined over $\overline{\mathbb{Q}}$ if a_X lies in $X(\overline{\mathbb{Q}})$. If this is the case then a_Y lies in $Y(\overline{\mathbb{Q}})$ for all finite covers Y of X, so there is a Galois action on these pro-points. The points on the universal cover $\tilde{X}$ of $X(\mathbb{C})$ gives rise to a natural subset of the set of pro-points

(2) Suppose $X(\mathbb{Q})$ is not empty. Let us fix a base point $\tilde{a} \in \tilde{X}$ lying over a point a_X in $X(\mathbb{Q})$. A *pro-loop* on X based at $\tilde{a}$ is defined to be a pro-point lying over a_X. This terminology is the generalisation of the situation where the chosen pro-point is again a point $\tilde{b}$ on $\tilde{X}$, lying over a_X, in which case the two points $\tilde{a}$ and $\tilde{b}$ uniquely determine a loop (up to homotopy) on $X(\mathbb{C})$. These pro-loops, like loops, can be composed and form a group denoted by $\hat{\pi}_1(X;\tilde{a})$, which is isomorphic to the profinite completion of the fundamental group $\pi_1(X(\mathbb{C}); a_X)$.

(3) For any finite set of points A of X, let $\pi_1(X;A)$ denote the fundamental groupoid of X based A, i.e. the set of homotopy classes of paths from a to b for all pairs $a, b \in A$.

(4) If $\tilde{a}$ and $\tilde{b}$ are pro-points of X, lying over a and $b \in X$ respectively, then we define the set of *pro-paths* on X from $\tilde{a}$ to $\tilde{b}$ to be the set of homotopy classes of paths from a to b on X, precomposed with the group of pro-loops $\hat{\pi}_1(X;\tilde{a})$. If $\tilde{A}$ is a finite set of pro-points of X, we can define the *profinite completion of* $\pi_1(X;\tilde{A})$ to be the set of pro-paths from $\tilde{a}$ to $\tilde{b}$ for all pairs $\tilde{a}, \tilde{b}$ of pro-points of A.

Well-known facts: (cf. [SGA 1], or [EL] for a short account) (1) Suppose X is an algebraic variety defined over $\mathbb{Q}$. There is a Galois action on the set of pro-paths of X whose endpoints are pro-points defined over $\overline{\mathbb{Q}}$. In particular, if $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and γ is a pro-path with endpoints $\tilde{a}$ and $\tilde{b}$ defined over $\overline{\mathbb{Q}}$, then for any pro-path γ' from $\sigma(\tilde{a})$ to $\sigma(\tilde{b})$, there exists a pro-loop $f \in \hat{\pi}_1(X;\tilde{a})$ such that $\sigma(\gamma) = \gamma' f$. (By convention, $\gamma_1 \gamma_2$

means the path γ_2 followed by the path γ_1.) In particular, even if we fix γ' to be an actual (homotopy class of) paths such an f exists.

(2) (cf. [I1, I2]) The tangential base points on $\mathcal{M}_{0,4}$ and $\mathcal{M}_{0,5}$ can be canonically lifted to pro-points which can be considered as being "defined over $\mathbb{Q}$". Thus, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the pro-points of the moduli spaces defined over $\overline{\mathbb{Q}}$ can be extended to these tangential base points by fixing them. The Galois action on pro-paths of these spaces with endpoints defined over $\overline{\mathbb{Q}}$ can also be extended to an action on pro-paths whose endpoints are tangential base points.

Now let us briefly recall the structure of the moduli spaces $\mathcal{M}_{0,4}$ (resp. $\mathcal{M}_{0,5}$) of Riemann spheres with 4 (resp. 5) ordered marked points, and particularly the nature of the tangential base points at infinity and of certain paths belonging to the fundamental groupoids based at these tangential base points and at some points with special automorphism group. Points of these moduli spaces are isomorphism classes of Riemann spheres with 4 (resp. 5) marked points, which means for instance that for each point of the moduli space there is a unique sphere whose ordered marked points are given by $(0, \epsilon, 1, \infty)$ (resp. $(0, \epsilon, 1, \infty, \mu)$) for $\epsilon \in \mathbb{C}$ different from 0 and 1 (resp. $\epsilon, \mu \in \mathbb{C}$ with $\epsilon \neq \mu$ and ϵ and μ different from 0 and 1). Namely

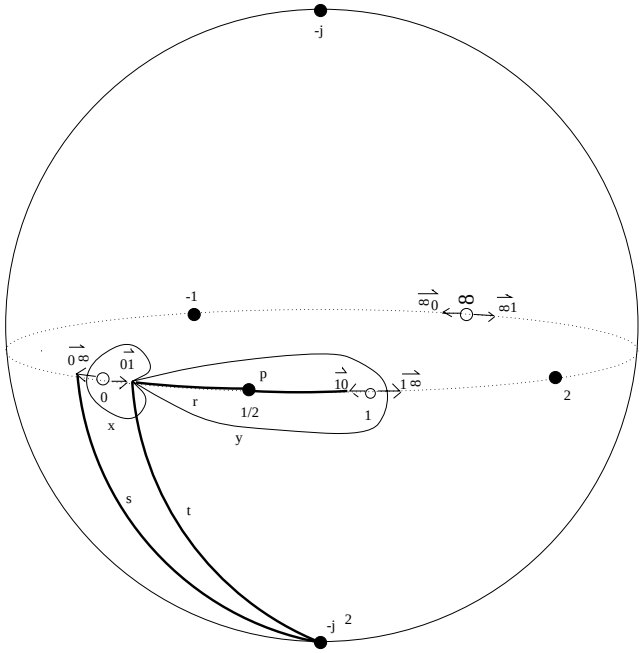
$$\mathcal{M}_{0,4} \simeq \mathbb{P}^1 - \{0, 1, \infty\} \quad \text{and} \quad \mathcal{M}_{0,5} \simeq (\mathbb{P}^1 - \{0, 1, \infty\})^2 - \Delta,$$

where Δ is the diagonal.

A complete description of the *region of maximal degeneration* of these moduli spaces is given in [PS, chapters II and III]. In particular, one can describe a set of simply connected (real) neighborhoods near infinity on the moduli spaces, the so-called *tangential base points*. The case of $\mathcal{M}_{0,4}$ is well-known and the tangential base points were first described by Deligne (cf. [De], [I]). $\mathcal{M}_{0,4} \simeq \mathbb{P}^1 - \{0, 1, \infty\}$ and its stable compactification is just $\mathbb{P}^1$; the points of maximal degeneration are the missing points 0, 1 and ∞, and their neighborhoods in $\mathcal{M}_{0,4}$ thus form three punctured disks. The real part of these three punctured disks is formed by 6 simply connected real segments which are usually denoted by $\{\vec{01}, \vec{0\infty}, \vec{10}, \vec{1\infty}, \vec{\infty 0}, \vec{\infty 1}\}$; they form the set of six tangential base points on $\mathcal{M}_{0,4}$. We denote this set by $\mathcal{B}_4$.

Let $j = \exp(4\pi i/3)$. Let p be the path on $\mathcal{M}_{0,4}$ along the real axis from $\vec{01}$ to $\vec{10}$; r the path along the real axis from $\vec{01}$ to $1/2$, s the path from $\vec{0\infty}$ to $-j^2$ (the south pole) and t the path on $\mathcal{M}_{0,4}$ from $\vec{01}$ to $-j^2$ shown in the figure above. Let t' be the image of t under complex conjugation, so t' runs directly from $\vec{01}$ to the north pole $-j$. We identify $\hat{F}_2$ with the algebraic fundamental group of $\mathcal{M}_{0,4}$, where x and y are anticlockwise loops around 0 and 1 based at the tangential base point $\vec{01}$. In order to discuss the profinite completion of the fundamental groupoid of $\mathcal{M}_{0,4}$, we need to pick liftings of the six tangential base

points and the five "special" points $1/2$, -1, 2, $-j$ and $-j^2$ to pro-points once and for all. We lift the tangential base points as Ihara does (cf. well-known fact (2) above). We choose the unique pro-point over $1/2$ such that the pro-path from the pro-point over $\vec{01}$ to the pro-point over $1/2$ is just the path on $\mathbb{P}^1 - \{0, 1, \infty\}$ from $\vec{01}$ to $1/2$; we pick the pro-points over the other "special" points analogously. Fixing these choices from now on, we allow ourselves to speak of the profinite fundamental groupoid based at $\vec{01}$, $1/2$, etc.



The neighborhood of the set of points of maximal degeneration in $\mathcal{M}_{0,5}$ is more complicated and the real neighborhood of the set of 15 points of maximal degeneration forms 60 simply connected regions; this set, which we denote by $\mathcal{B}_5$, is well-described in [PS] and we restrict ourselves to the careful description of two of these regions which will concern us here. The first is given by the set of all points on $\mathcal{M}_{0,5}$ corresponding to spheres whose five ordered marked points are of the form $(0, \epsilon, 1, \infty, \mu)$ where ϵ is a small positive real number and μ is a negative real number with very large absolute value, and the second is given by the set of points on $\mathcal{M}_{0,5}$ corresponding to the spheres whose ordered marked points have the form $(0, 1-\epsilon, 1, \infty, \mu)$, ϵ and μ as above (we say that a sphere with 5 marked points is in "standard form" if 0, 1 and ∞ are in the first, third and fourth places respectively). We denote these small simply connected real regions of $\mathcal{M}_{0,5}$ by Q and Q' respectively. Let $\bar{p}$ be the path from from Q to Q', analogous to the path p on $\mathcal{M}_{0,4}$, given by the set of points corresponding to the spheres in standard form with marked points $(0, \delta, 1, \infty, \mu)$ where δ takes all real values in the interval $[\epsilon, 1-\epsilon]$.

Let $\zeta = \exp(2\pi i/5)$, and let Z denote the point of $\mathcal{M}_{0,5}$ corresponding to the sphere with five marked points $(1, \zeta, \zeta^2, \zeta^3, \zeta^4)$. The sphere in standard form corresponding to

this point with 0, 1 and ∞ in the first, third and fourth places, is given by the points

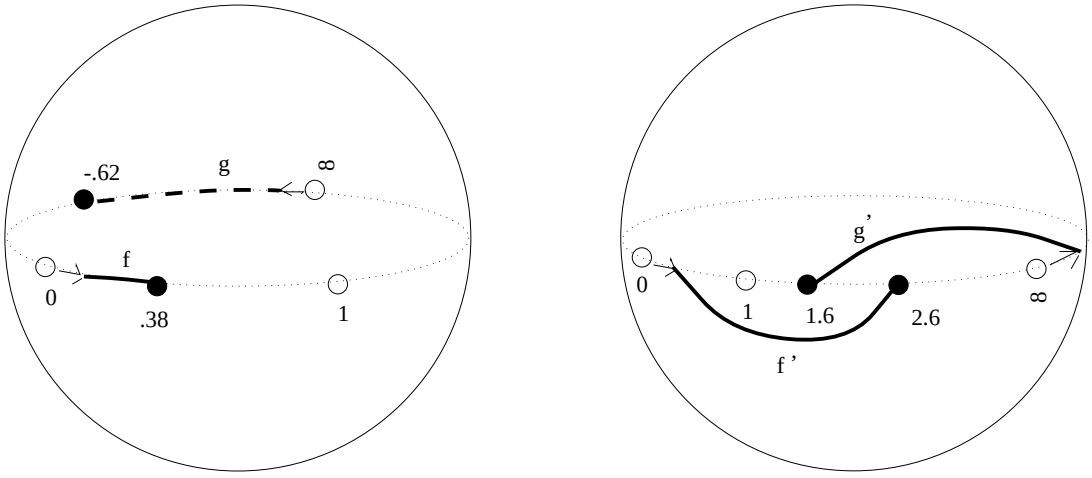
$$\big(0, \frac{\zeta}{(1+\zeta)^2}, 1, \infty, -(\zeta+\zeta^4)\big) \sim (0, .38, 1, \infty, -.62)$$

(it is easy to confirm that $\zeta/((1+\zeta)^2)$ and $-(\zeta+\zeta^4)$ are real). For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\chi(\sigma)$ is invertible mod 5. If $\chi(\sigma) \equiv 1$ or 4 mod 5, then $\chi(\sigma)(Z) = Z$. If $\chi(\sigma) \equiv 2$ or 3 mod 5, then $\chi(\sigma)(Z) = Z'$, where Z' is obtained from Z by substituting ζ^2 or ζ^3 for ζ, the two substitutions giving the same result. The standard form of Z' is given by:

$$\big(0, \frac{\zeta^2}{(1+\zeta^2)^2}, 1, \infty, -(\zeta^2+\zeta^3))\big) \sim (0, 2.6, 1, \infty, 1.6).$$

Again, we fix once and for all pro-points lying over the tangential base points Q and Q' and the points Z and Z' such that the pro-paths between these pro-points are exactly the paths on $\mathcal{M}_{0,5}$ described below.

Let v and v' denote the paths on $\mathcal{M}_{0,5}$ from Q to Z and from Q to Z' parametrized respectively by $(0, f, 1, \infty, g)$ and $(0, f', 1, \infty, g')$ where f, g, f', g' are the paths shown in the following figure (the dashed line represents a path on the back of the sphere).



Recall that the mapping class group $M(0,5)$ is the group of orientation-preserving diffeomorphisms of a sphere with 5 marked points modulo those which are isotopic to the identity. Let S_Q be a sphere in standard form corresponding to Q, with marked points $(0, \epsilon, 1, \infty, \mu)$, and let γ_i represent the loop passing through the i-th and $(i+1)$-st marked points of S_Q for $i = 1, 2, 3, 4$, running along the real axis. Each generator σ_i of $M(0,5)$ corresponds to a *Dehn twist* along the loop γ_i, and following the effect of this twist as it deforms the sphere S_Q gives a path on the moduli space $\mathcal{M}_{0,5}$ starting at Q. These paths can be composed via the automorphisms of $M_{0,5}$, so that the group $M(0,5)$ can be identified with a star of paths starting at Q. In particular, this gives an identification of the pure subgroup $K(0,5)$ with the fundamental group $\pi_1(\mathcal{M}_{0,5}; Q)$.

Proof of theorem 1. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \hookrightarrow \widehat{GT}$.

Let p, r, s, t and t' on $\mathcal{M}_{0,4}$ and $\bar{p}$, v and v' on $\mathcal{M}_{0,5}$ denote the paths defined above, and let $\hat{F}_2$ be identified with $\hat{\pi}_1(\mathcal{M}_{0,4};\vec{01})$ and $\hat{K}(0,5)$ with $\hat{\pi}_1(\mathcal{M}_{0,5};Q)$ also as above. Fix $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By the well-known fact (2), there exist pro-loops $f = f(x,y)$, $g = g(x,y)$ and $\tilde{h} = \tilde{h}(x,y) \in \hat{F}_2$ such that $\sigma(p) = pf$, $\sigma(r) = rg$, $\sigma(t) = t\tilde{h}$ if $\chi(\sigma) \equiv 1 \bmod 3$, or $\sigma(t) = t'\tilde{h}$ if $\chi(\sigma) \equiv 2 \bmod 3$. Similarly, there exists a pro-loop $k = k(x_{12}, x_{23}, x_{34}, x_{45}, x_{51})$ in $\hat{K}(0,5)$ such that $\sigma(v) = vk$ if $\chi(\sigma) \equiv 1$ or $4 \bmod 5$, $\sigma(v) = v'k$ if $\chi(\sigma) \equiv 2$ or $3 \bmod 5$. Note that Ihara proves that $f = f(x,y)$ actually lies in $\hat{F}_2'$ (cf. [I2], Prop. 1.5).

The inclusion of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $\widehat{GT}$ discovered by Ihara is given by associating to σ the pair $(\chi(\sigma), f) \in \hat{\mathbb{Z}}^* \times \hat{F}_2'$. In [I1] and [I2] Ihara proves that these pairs satisfy relations (I), (II) and (III) of the definition of $\widehat{GT}$. We associate the same pair to σ, and we show directly that such pairs satisfy properties (I'), (II') and (III') of the elements of $\widehat{GT}$ given in theorem 2. It is enough to show these properties, since they give the precise cocycle form of f and thus immediately imply the cocycle relations (I), (II) and (III).

Let us begin with (I'). Let $\Theta(z) = 1 - z$ and $\Omega(z) = 1/(1-z)$ denote two automorphisms of $\mathcal{M}_{0,4}$ of order 2 and 3 respectively; they generate $\mathrm{Aut}(\mathcal{M}_{0,4}) \simeq S_3$. These automorphisms are related to the automorphisms θ and ω of $\hat{F}_2 = \hat{\pi}_1(\mathcal{M}_{0,4};\vec{01})$ by the following formulae:

$$\theta(w) = p^{-1}\Theta(w)p \quad \text{and} \quad \omega(w) = t^{-1}\Omega(t)\Omega(w)\Omega(t^{-1})t \quad \text{for all} \quad w \in \hat{F}_2, \tag{3}$$

as can be easily confirmed by checking on the two generators x and y of $\hat{F}_2$. Let us show that $(\chi(\sigma), f)$ has property (I'). We have $\Theta(r)^{-1}r = p$; applying σ to both sides, we obtain

$$\Theta(rg)^{-1}rg = \Theta(g)^{-1}\Theta(r)^{-1}rg = \Theta(g)^{-1}pg = p\theta(g)^{-1}g = pf$$

using equation (3). This shows that $f = \theta(g)^{-1}g$, so f has the form (I') of theorem 2.

Let us show (II'). The path $s^{-1}t$ is homotopic to a small clockwise half-circle in the lower hemisphere around 0 starting at $\vec{01}$ and ending at $0\vec{\infty}$. The path $\Omega\Theta(s^{-1}t)$ is homotopic to a small half-circle around 0 starting at $0\vec{\infty}$ and ending at $\vec{01}$, lying in the upper hemisphere, so that $\Omega\Theta(s^{-1}t)s^{-1}t = x^{-1}$ is just a clockwise loop around 0 based at $\vec{01}$. We need the two following facts. First (cf. [I2, Prop. 2.5]), the action of σ commutes with that of the automorphisms of $\mathcal{M}_{0,4}$ and $\mathcal{M}_{0,5}$, and second (cf. [EL, formula 18]), if $m = (\chi(\sigma) - 1)/2$, then $\sigma(s^{-1}t) = s^{-1}tx^{-m}$. In particular, this determines the action of σ on s from its action on t: we obtain $\sigma(s) = \sigma(t)x^m t^{-1}s$ where $\sigma(t) = t\tilde{h}$ or $t'\tilde{h}$ according to the congruence of $\chi(\sigma)$ mod 3.

Moreover, $\Omega(s)$ is the path running straight from the base point $\vec{10}$ to $-j^2$, so we have $p = \Omega(s)^{-1}t$. Consider first the case $\chi(\sigma) \equiv 1 \bmod 3$, so $\sigma(t) = t\tilde{h}$. Applying σ to both

sides of the equation $p = \Omega(s)^{-1}t$, we obtain on the left-hand side $\sigma(p) = pf$ and on the right-hand side, using equation (3):

$$\begin{aligned}\sigma(p) = \sigma(\Omega(s)^{-1}t) &= \Omega(\sigma(s))^{-1}\sigma(t) = \Omega(s^{-1})\Omega\big(tx^{-m}\tilde{h}^{-1}t^{-1}\big)t\tilde{h} \\ &= \Omega(s^{-1})t\cdot t^{-1}\Omega(t)\Omega(x)^{-m}\Omega(t^{-1})t\cdot t^{-1}\Omega(t)\Omega(\tilde{h}^{-1})\Omega(t^{-1})t\tilde{h} \\ &= p\omega(x)^{-m}\omega(\tilde{h})^{-1}\tilde{h} = py^{-m}\omega(\tilde{h})^{-1}h.\end{aligned}$$

Set $h = \tilde{h}x^m$; then we obtain from this expression:

$$pf = p\omega(h)^{-1}hx^{-m},$$

i.e. $fx^m = \omega(h)^{-1}h$, which is the form given in theorem 2.

In the case $\chi(\sigma) \equiv 2 \bmod 3$, i.e. $\sigma(t) = t'\tilde{h}$, we apply σ to the same equation $p = \Omega(s)^{-1}t$ and the left-hand side is again pf. Again using equation (3), the right-hand side becomes

$$\begin{aligned}\sigma(p) = \sigma(\Omega(s)^{-1}t) &= \Omega(\sigma(s))^{-1}\sigma(t) = \Omega(s^{-1})\Omega\big(tx^{-m}\tilde{h}^{-1}t'^{-1}\big)t'\tilde{h} \\ &= \Omega(s^{-1})t\cdot t^{-1}\Omega(t)\Omega(x)^{-m}\Omega(t^{-1})t\cdot t^{-1}\Omega(t)\Omega(\tilde{h}^{-1})\Omega(t^{-1})t\cdot t^{-1}\Omega(t)\Omega(t')^{-1}t'\tilde{h} \\ &= p\omega(x)^{-m}\omega(\tilde{h})^{-1}y^{-1}\tilde{h} = py^{-m}\omega(\tilde{h})^{-1}y^{-1}\tilde{h},\end{aligned}$$

since $t^{-1}\Omega(t)\Omega(t')^{-1}t' = y^{-1}$. Now set $h = y^{-1}\tilde{h}x^m$. Then since $\omega(y) = z = (xy)^{-1}$, we obtain the equality

$$pf = py^{-m}\omega(\tilde{h})^{-1}y^{-1}\tilde{h} = p\omega(h)^{-1}xyhx^{-m},$$

so fx^m has the form given in theorem 2.

Let us prove (III'). Recall that the mapping class group $M(0,5)$ can be identified with a star of paths starting from Q via the Dehn twists described above. Let $\rho = (\sigma_4\sigma_3\sigma_2\sigma_1)^2 \in M(0,5)$ as in the previous sections. A priori, ρ corresponds to a rotation of the sphere through an angle of $6\pi\, i/5$, but this symmetry is lost using standard form. A point $(0, a, 1, \infty, b)$ goes to $(1, \infty, b, 0, a)$ under ρ, which is given in standard form by

$$\big(0, \frac{b}{b-1}, 1, \infty, \frac{b(a-1)}{a(b-1)}\big). \tag{4}$$

The permutation corresponding to ρ is given by $(14253) \in S_5$; it also gives an automorphism of $\mathcal{M}_{0,5}$, expressed on the spheres in standard form by (4). We denote this automorphism by $P \in \mathrm{Aut}(\mathcal{M}_{0,5})$, appealing to the reader to identify this letter with a capital ρ, accompanied by the suitable pronunciation, in analogy with the notation θ and Θ, ω and Ω introduced above. Considering $\rho \in M(0,5)$ as a word in the Dehn twists

σ_i, ρ induces a path in the moduli space from any point $q \in Q$ to the point $P(q)$ which by (4) lies in Q', so it induces a well-defined homotopy class of paths from the simply connected region Q to $P(Q) = Q'$. We denote this path by $\bar{p}$. The automorphisms ρ of $\hat{K}(0,5) = \hat{\pi}_1(\mathcal{M}_{0,5}; Q)$ (i.e. conjugation by ρ in $\hat{M}(0,5)$) and P of $\mathcal{M}_{0,5}$ are related by the following formula, analogous to equation (3) above:

$$\bar{p}^{-1} P(k) \bar{p} = \rho(k) \quad \text{for all} \quad k \in \hat{K}(0,5). \tag{5}$$

To study the images of the paths v and v' under the automorphism P of $\mathcal{M}_{0,5}$, we need to choose parametrizations of them. Before doing so, we note that using (4), it is easy to check that P fixes the points Z and Z' on $\mathcal{M}_{0,5}$.

Let us parametrize v by

$$(0, (\frac{\zeta}{(1+\zeta)^2} - \epsilon)z + \epsilon, 1, \infty, (-(\zeta + \zeta^4) - \mu)z + \mu),$$

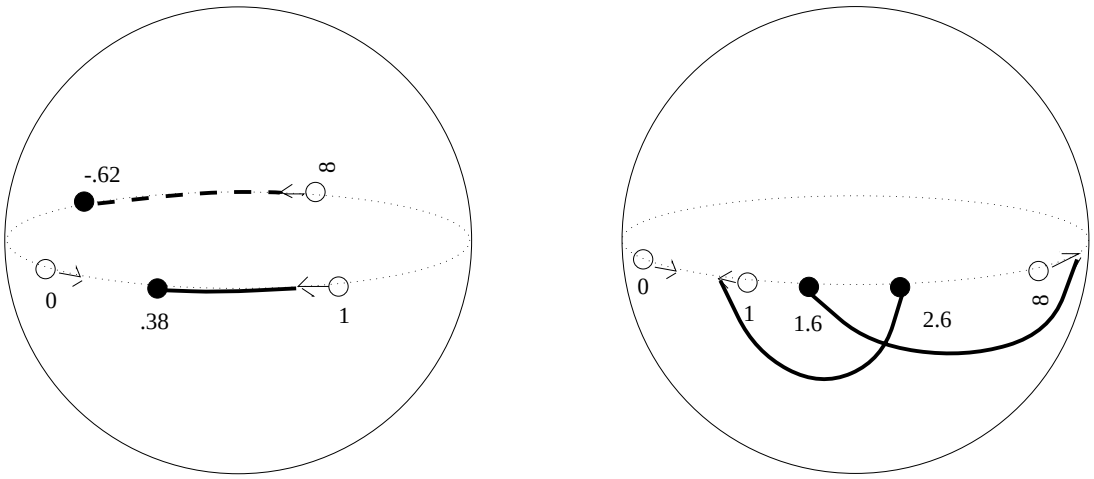
for $z \in [0,1]$ (where the first, third and fourth paths are constant paths at the given points). The path v' is only slightly more complicated; we do it with two pairs of line segments. Let $\alpha = \zeta^2/((1+\zeta^2)^2) \sim 2.6$ and $\beta = -(\zeta^2 + \zeta^3) \sim 1.6$ so that $(0, \alpha, 1, \infty, \beta)$ gives the endpoint of v'. Then we can parametrize v' via

$$(0, (2 - 2\epsilon - 2i)z + \epsilon, 1, \infty, (2i - 2\mu)z + \mu)$$

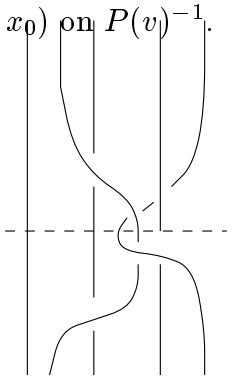
for $z \in [0, 1/2]$ and

$$(0, (2\alpha - 2 + 2i)z + (2 - \alpha - 2i), 1, \infty, (2\beta - 2i)z + (2i - \beta))$$

for $z \in [1/2, 1]$. These parametrizations allow us to compute the images of the paths v and v' under the automorphism P. Using (4) to calculate them directly, we find that $P(v)$ and $P(v')$ are as in the following figure. In particular, this calculation (left to the unconvinced reader...) shows that the two pieces of $P(v')$ actually cross for some value $z_0 \in [0,1]$, i.e. there is a point of the form $(0, x_0, 1, \infty, x_0)$ on the path $P(v')$, a fact which comes in handy below.



Let us show that $P(v)^{-1}v = \bar{p}$ and $P(v')^{-1}v' = \bar{p}\,x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$. The case of v is immediate from the figures: the path v followed by $P(v)^{-1}$ has the point starting at μ perform a loop homotopic to the identity, while the point starting at ϵ slides from ϵ to $1-\epsilon$, which is just the path $\bar{p}$. Along v' followed by $P(v')^{-1}$, the points starting at μ and ϵ follow a more complicated procedure which we can write as the braid given in the following figure, with the convention that when a marked point passes above another, the corresponding braid strand passes behind, and when it passes below, the braid strand passes in front. The braid we obtain is a pure braid which means it starts and ends at Q; in order to obtain $P(v')^{-1}v'$ we have to compose this braid with the path $\bar{p}$. The upper part of the braid follows the meanderings of the path v', and the lower half continues it with $P(v')^{-1}$. One cannot of course deduce this braid merely from the figures above, it is necessary to use the explicit parametrization of v' and the parametrization of $P(v')^{-1}$ obtained from it, i.e. to have a sort of "kinematic" version of the path, in order to confirm the fact remarked above that the two pieces of the path cross for some value $z_0 \in [0,1]$, i.e. that there is a point $(0, x_0, 1, \infty, x_0)$ on $P(v)^{-1}$.



This braid is given by $x_{25}x_{45}$; using the identity $x_{51} = x_{23}x_{24}x_{34}$ valid in $K(0,5)$, we find that this is equal to the now-familiar expression $x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$, which means precisely that $P(v')^{-1}v' = \bar{p}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$, as desired. Now, from the two equalities $P(v)^{-1}v = \bar{p}$ and $P(v')^{-1}v' = \bar{p}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}$, we will deduce the cocycle form (III') of f. Consider first the case $\chi(\sigma) \equiv 1$ or 4 mod 5. Then $\sigma(v) = vk$ and $\sigma(\bar{p}) = \bar{p}\,f(x_{12}, x_{23})$, so applying σ to both sides of the equality $P(v)^{-1}v = \bar{p}$ and using equation (5), we obtain

$$P(vk)^{-1}vk = P(k)^{-1}P(v)^{-1}vk = P(k)^{-1}\bar{p}k = \bar{p}\rho(k)^{-1}k = \bar{p}\,f(x_{12}, x_{23}).$$

In the case $\chi(\sigma) \equiv 2$ or 3 mod 5, we have $\sigma(v) = v'k$ and so similarly, we obtain

$$P(v'k)^{-1}v'k = P(k)^{-1}\bar{p}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}k = \bar{p}\rho(k)^{-1}x_{34}x_{51}^{-1}x_{45}x_{12}^{-1}k = \bar{p}\,f(x_{12}, x_{23}).$$

Thus $f(x_{12}, x_{23})$ has the form of (III') of theorem 2. This concludes our proof that the elements $f \in \hat{F}_2'$ belonging to pairs (λ, f) associated to $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ have the forms (I'), (II') and (III'), so in particular they lie in $\widehat{GT}$. To see that the map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to$

$\widehat{GT}$ obtained this way is a group homomorphism, it suffices to note that elements $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ give automorphisms of $\hat{F}_2$ via their couples (λ, f), by sending $x \mapsto x^\lambda$ and $y \mapsto f^{-1}y^\lambda f$, and multiplication of elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ corresponds to composition of these automorphisms, which gives the multiplication of formula (2), i.e. that of $\widehat{GT}$.

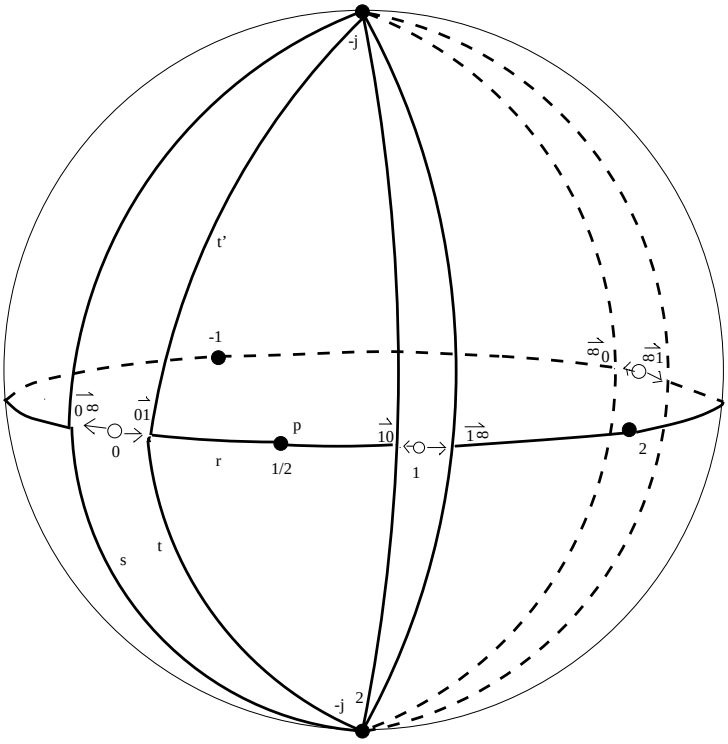
Now, since the elements of $\widehat{GT}$ give automorphisms of $\hat{F}_2$ via $x \mapsto x^\lambda$ and $y \mapsto f^{-1}y^\lambda f$, the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act as automorphisms of $\hat{F}_2$. Now, $\hat{F}_2$ is the algebraic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, which is a variety defined over $\mathbb{Q}$, so we have a split exact sequence

$$1 \to \hat{\pi}_1(\mathbb{P}^1 - \{0, 1, \infty\} \otimes \overline{\mathbb{Q}}) \simeq \hat{F}_2 \to \hat{\pi}_1(\mathbb{P}^1 - \{0, 1, \infty\}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1.$$

This gives an outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\hat{F}_2$, i.e. a canonical homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\hat{F}_2)$, which lifts in many ways to homomorphisms $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\hat{F}_2)$. The most striking property of our homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{GT} \subset \mathrm{Aut}(\hat{F}_2)$ is that it lifts the canonical homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\hat{F}_2)$ (cf. theorem 1 of the appendix to [I2]). Since by Belyi's theorem, the homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Out}(\hat{F}_2)$ is *injective* (cf. for example [S], II), our homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{GT}$ is also injective. ♣

Proof of the corollary to theorem 2. Let $F = (\lambda, f)$ be an element of $\widehat{GT}$, so it takes the forms in theorem 2 according to the congruences of λ. Then in analogy to what happens for $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\widehat{GT}$ acts naturally on the path r on $\mathcal{M}_{0,4}$ by sending it to rg, and on t by sending it to $t\tilde{h}$ where $\tilde{h} = hx^{-m}$ if $\lambda \equiv 1 \bmod 3$ and to $t'\tilde{h}$ where $\tilde{h} = yhx^{-m}$ if $\lambda \equiv 2 \bmod 3$. Moreover, F acts on the path v on $\mathcal{M}_{0,5}$ by sending it to vk if $\lambda \equiv 1$ or $4 \bmod 5$ and to $v'k$ if $\lambda \equiv 2$ or $3 \bmod 5$.

As described at the end of the introduction, this action of $\widehat{GT}$ on these paths is natural in that it probably extends to an automorphism of the full algebraic fundamental groupoids of $\mathcal{M}_{0,4}$ and $\mathcal{M}_{0,5}$ based at tangential base points and points of special automorphism group, and indeed it is probably the complete group of automorphisms of these groupoids satisfying some simple conditions. We can show that this is the case for $n = 4$. Let Θ and Ω be the two generators of $\mathrm{Aut}(\mathcal{M}_{0,4})$ given above. Generically, any point of $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0, 1, \infty\}$ has six images under $\mathrm{Aut}(\mathcal{M}_{0,4})$. The points of $\mathbb{P}^1 - \{0, 1, \infty\}$ having special automorphism group are the points which do not have six distinct images under the action of this group, i.e. they are fixed under some automorphisms. It is easily determined that $1/2$ is the only fixed point of Θ, -1 of $\Omega\Theta$ and 2 of $\Omega^2\Theta$. The fixed points of Ω and Ω^2 are $-j$ and $-j^2$, so the five points $\{1/2, 2, -1, -j, -j^2\}$ give the complete set of points of $\mathbb{P}^1 - \{0, 1, \infty\}$ with special automorphism group. Let $\tilde{\mathcal{B}}_4$ denote the union of the six tangential base points and the five points of special automorphism group. A generating set of paths for the fundamental groupoid $\pi_1(\mathcal{M}_{0,4}; \mathcal{B}_4)$ forms a sort of pumpkin, as in the following figure:



These paths are simply the basic paths r, s and t together with all their images under the six automorphisms of $\mathbb{P}^1 - \{0, 1, \infty\}$. For any two points a and b in $\tilde{\mathcal{B}}_4$, the set of paths in $\pi_1(\mathcal{M}_{0,4}; \tilde{\mathcal{B}}_4)$ from a to b is given by any one path from a to b precomposed with the set of loops in the local group (isomorphic to F_2) based at a. The algebraic fundamental groupoid $\hat{\pi}_1(\mathcal{M}_{0,4}; \tilde{\mathcal{B}}_4)$ is obtained from the topological fundamental groupoid by replacing the local group (isomorphic to F_2) at each point by its profinite completion $\hat{F}_2$, so that the set of pro-paths from a to b is given by a choice of a path from a to b lying in the topological fundamental groupoid, formally precomposed with all elements of $\hat{\pi}_1(\mathcal{M}_{0,4}; a)$.

Proposition 11. *$\widehat{GT}$ is an automorphism group of the fundamental groupoid $\hat{\pi}_1(\mathcal{M}_{0,4}; \tilde{\mathcal{B}}_4)$.*

Proof. In order to show that $\widehat{GT}$ is an automorphism group of this fundamental groupoid, we first define the action of $\widehat{GT}$ on each path as above, namely if $F = (\lambda, f) \in \widehat{GT}$, we set

$$\tilde{h} = \begin{cases} hx^{-m} & \text{if } \lambda \equiv 1 \bmod 3 \\ yhx^{-m} & \text{if } \lambda \equiv 2 \bmod 3, \end{cases}$$

and $F(r) = rg$, $F(t) = t\tilde{h}$ resp. $t'\tilde{h}$ if $\lambda \equiv 1$ resp. $2 \bmod 3$, and $F(s) = F(t)x^m t^{-1} s$, so $F(s^{-1}t) = s^{-1}tx^{-m}$. Since $f = \theta(g)^{-1}g$ and $p = \Theta(r)^{-1}r$, we obtain $F(p) = pf$. In order to check that F really an automorphism of the groupoid, we need to check that all relations in the groupoid are respected by this action (a relation in the groupoid is a non-trivial chain of paths forming a loop homotopic to the identity). Up to the action of automorphisms (which commute with $\widehat{GT}$), the set of relations in the fundamental groupoid $\pi_1(\mathcal{M}_{0,4})$ is

generated by the following two relations among the generating paths r, s and t:

$$r^{-1}\Theta(r)\Omega(s^{-1})t = 1$$

and

$$t^{-1}s\Omega^2(\Theta(r)^{-1}rt^{-1}s)\Omega(\Theta(r)^{-1}rt^{-1}s)\Theta(r)^{-1}r = 1.$$

The first relation can be written $\Theta(r)^{-1}r = \Omega(s)^{-1}t$. Applying F to both sides, we see that it is respected by the action of F if and only if

$$\theta(g)^{-1}g = \begin{cases} \omega(h)^{-1} & \text{if } \lambda \equiv 1 \bmod 3 \\ \omega(h)^{-1}xyh & \text{if } \lambda \equiv 2 \bmod 3. \end{cases}$$

But this is the case by hypothesis.

In the second relation, we may use the identity $\Theta(r)^{-1}r = p$ to rewrite the relation as $t^{-1}s\Omega^2(pt^{-1}s)\Omega(pt^{-1}s)p = 1$. Let us apply F to the left-hand side of this relation, recalling that $t^{-1}\Omega(t)\Omega(w)\Omega(t)^{-1}t = \omega(w)$ and thus $t^{-1}\Omega^2(t)\Omega^2(w)\Omega^2(t)^{-1}t = \omega^2(w)$ for all $w \in \hat{F}_2$. We obtain

$$x^m t^{-1}s\Omega^2(p)\Omega^2(fx^m)\Omega^2(t^{-1}s)\Omega(p)\Omega(fx^m)\Omega(t^{-1}s)pf = 1.$$

Using the identity $p = \Omega(s)^{-1}t$ this simplifies to

$$t^{-1}\Omega^2(t)\Omega^2(fx^m)\Omega^2(t)^{-1}t \cdot t^{-1}\Omega(t)\Omega(fx^m)\Omega(t)^{-1}t \cdot fx^m = 1,$$

which is equal to $\omega^2(fx^m)\omega(fx^m)fx^m = 1$, by relation (II) of the definition of $\widehat{GT}$. Thus the second relation is also respected by the action of $\widehat{GT}$, which concludes the proof. ♣

Acknowledgments. Discussions with Jean-Pierre Serre were essential to the proof of proposition 3, much of which is due to arguments of his, contained in letters which we hope to publish shortly in a collection of articles. Our statement of proposition 5 and our understanding of it are due to Claus Scheiderer, who wrote the appendix to this article. We thank them both warmly. Joan Birman and Bill Harvey were also unstintingly generous with their help for which we are very grateful. Finally, thanks are due to the referee whose detailed suggestions clarified many obscure points.

References

[B] J. Birman, *Braids, Links and Mapping Class Groups*, Ann. of Math. Studies, vol. **82**, Princeton Univ. Press, 1975.

[Br] K. Brown, *Cohomology of Groups*, GTM **87**, Springer-Verlag, 1994.

[De] P. Deligne, Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbb{Q}$, 79-298; Publ. MSRI no. 16, Springer-Verlag, 1989.

[D] V.G. Drinfel'd, On quasitriangular quasi-Hopf algebras and a group closely connected with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Leningrad Math. J.* Vol. 2 (1991), No. 4, 829-860.

[EL] M. Emsalem, P. Lochak, The action of the absolute Galois group on the moduli space of spheres with four marked points, in *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Notes **200**, Cambridge University Press, 1994.

[HM] C. McLachlan, W. Harvey, On mapping-class groups and Teichmüller spaces, Proc. London Math. Soc. **(3)30** (1975), 496-512.

[HS] D. Harbater, L. Schneps, Estimating Galois orbits of dessins, preprint.

[I1] Y. Ihara, Braids, Galois groups, and some arithmetic functions, Proceedings of the ICM, Kyoto, Japan, 1990, 99-120.

[I2] Y. Ihara, On the embedding of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $\widehat{GT}$, in *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Notes **200**, Cambridge Univ. Press, 1994.

[IM] Y. Ihara, M. Matsumoto, On Galois Actions of Profinite Completions of Braid Groups, in *Recent Developments in the Inverse Galois Problem*, M.Fried et al. Eds., AMS, 1995.

[LS] P. Lochak and L. Schneps, The Grothendieck-Teichmüller group and automorphisms of braid groups, in *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Notes **200**, Cambridge Univ. Press, 1994.

[N] H. Nakamura, Galois ridigity of pure sphere braid groups and profinite calculus, *J. Math. Sci. Univ. Tokyo* **1** (1994), 71-136.

[PS] Triangulations, Courbes Algébriques et Théorie des Champs, issue of *Panoramas et Synthèses*, publication of the SMF, to appear.

[Q] D.Quillen, Rational Homotopy Theory, *Ann. Math.* **90**, 1969, 205-295.

[S] L. Schneps, Dessins d'enfants on the Riemann sphere, in *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lecture Notes **200**, Cambridge Univ. Press, 1994.

[S1] J-P. Serre, *Cohomologie galoisienne*, Springer Lecture Notes **5**, Springer-Verlag, 1964-1994.

[S2] J-P. Serre, letters, to appear.

[S3] J-P. Serre, *Arbres, Amalgames,* SL_2, Astérisque **46**, 1977.

[SGA1] Revêtements étales et groupe fondamental, Springer Lecture Notes **244**, Springer-Verlag, 1971.

URA 762 du CNRS, Ecole Normale Supérieure, 45 rue d'Ulm, 75005 Paris

UMR 741 du CNRS, Laboratoire de Mathématiques, Faculté des Sciences de Besançon, 25030 Besançon Cedex