Surfaces and p-adic fields



Nadav Gropper

Mansfield

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2022

This thesis is dedicated to my wonderful grandparents: Yakov, Ora, Eliezer and Ruth

Acknowledgements

I would first like to thank my wonderful supervisors Konstantin Ardakov and Minhyong Kim, for their help throughout my DPhil. I'd also like to thank the staff at the maths department and at Mansfield college. Thanks to my examiners Kobi Kremnitzer and Tomer Schlank for useful comments and corrections. I was fortunate to have lots of supports for my family and friends, and help from many great people in the mathematical community, during my DPhil and in previous studies, I would not have been able to complete this without this support. There are so many people I am so so thankful for, which is why I was nervous to write this acknowledgment, I will try and name some (in probably a chatoic order), but there are many more I am thankful for: Vladimir Berkovich, Ehud de-Shalit, Uri Bader, Tsachik Gelander, Dima Gurevich, Itay Glazer, Yotam Hendel, Ido Grayevsky, Jonathan Fruchter, Alyosha Latyntsev, Jay Swar, Zhenhua Wu, Adam Keilthy, Richard Mathers, Adam Jones, Ioan Stanciu, James Timmins, Arun Soor, George Robinson, Noam Kantor, Jane Tan, Monika Kudlinska, Adele Jackson, Alice Kerr, Christoph Weis, Izar Alonso, Magdalena Drozdz, Matthew Steggles, Alex Richards, Izzy Archer, George Atkinson, Joe Baynes, Eddy Yeo, Maisie Vollans, Roman Kucera, Elise Raphael, Barbora Sojkova, Maria Ordovas, Emmie Hine, Elise Ogden, Shira Ben David, Aviv Hendler, Ran Huet, Valeri Kremer, Alex Volk and the PFT staff, Gizmo, Coco and Hazel Emmett, Suki and Kathryn Emmett-McGrath, Sarah, Maoz, Omri, Shir, Shani, Lucy and Luna Gropper, and so so many more

Abstract

Under the philosophy of arithmetic topology, one would like to have an analogy between surfaces S, and p-adic fields K.

In the following we describe a point of view which helps look at surfaces and p-adic fields in a "uniform way", and show that results on mapping class groups can be extended to this point of view, and thus be applied to G_K, the absolute Galois groups of the p-adic field K.

By moving both groups to the world of pro-p groups (for G_K we take its maximal pro-p quotient, and for $\pi_1(S)$ we take its pro-p completion), we see they both are pro-p Poincare duality groups of dimension 2, also known as Demuskin groups. Such groups have a very nice classification in terms of generators and relations.

Next, in order to move geometric ideas to a purely group theoretic setting, we use the language of graphs of groups and Bass-Serre trees.

By restating results for surfaces purely in such a manner, we can (after proving a few technical results) get similar results for p-adic fields.

We start by examining discrete groups with Demuskin type relations, for which we show a few pro-p rigidity type results.

Using this we show that all splittings of a Demuskin group come from a discrete splitting, which in turn helps us show that Dehn twists make sense in such a context.

This gives us a family of infinite order Outer automorphisms of $G_K(p)$, the maximal pro-p quotient of G_K, which are "arithmetic Dehn twists". On the other hand, when specializing this to Demuskin groups with $q = \infty$, one gets back the usual definition of Dehn twists on surfaces.

We also get a curve complex for p-adic fields, namely the complex whose edges are graph of groups with $G_K(p)$ as their fundamental group, and 2 vertices have an edge between them if the graphs corresponding to the

vertices are compatible. By the relations between discrete and pro-p Demuskin groups, we get a nice way to understand said curve complex.

Contents

1 Introduction **1**

2 General Motivation **5**

2.1 Arithmetic topology 5

2.2 Rigidity and anabelian geometry 6

2.2.1 explicit outer automorphism 10

2.3 Mapping class groups of surface 15

2.3.1 Generators of the mapping class group and the curve complex 18

2.4 Teichmuller spaces and Galois representations 18

3 From curves to graphs of groups **20**

3.1 Splittings of groups and graphs of groups 20

3.2 Intersection of Splittings 23

3.3 Dehn twists for discrete groups 26

3.4 Profinite groups and graphs 28

4 Main Results **33**

4.1 Background on Poincare duality groups 33

4.2 Demuskin groups 34

4.2.1 Splittings of discrete Demuskin groups 35

4.3 Pro-p rigidity for Demuskin type relations 38

4.3.1 p-efficient splittings 38

4.3.2 Complexes of cyclic splittings 42

Chapter 1

Introduction

The purpose of this paper is to explain a new point of view, which furthers the analogies of arithmetic topology, and allows for a more "uniform" approach towards p-adic fields K, and surfaces S.

Earlier reasons for such analogs, come from studying of the structure of absolute Galois groups of p-adic fields, one gets a presentation very similar to that of a surface group.

A family of groups containing both, is pro-p Poincare Duality groups of dimension 2, which are also known as Demuskin groups.

Another place where the similarities continue is when looking at 3-dimensional hyperbolic manifolds, such manifold have Mostow's rigidity theorem, which states that a complete finite volume n-dimensional hyperbolic manifold is determined by its fundamental group.

One has a similar theorem for number fields, which states that the absolute Galois group of a number field determines the field (see [31, 47]).

The automorphism in definition 21, defined in [33] is an important example in anabelian geometry, showing that there is no direct analogue for results such as [47, 31] and is the only constructed outer automorphism of G_K, the absolute Galois group of K, the author could find.

The argument given in [33] only shows that the automorphism is an outer automorphism for G_K, but it does not work for powers of that automorphism.

If one looks at representations which are trivial mod p, we get that the representation factors through $G_K(p)$, the maximal pro-p quotient of G_K (i.e the Galois group of the maximal p-extension).

One can define at a similar construction to 21, which gives an automorphism of $G_K(p)$, but again it is not immediate it will be outer.

Remark 1. One of our interests in $Out(G_K)$ is its action on deformation spaces of Galois representations, if one looks at representations which are trivial mod p, we get that the representation factors through the maximal pro-p quotient of G_K, $G_K(p)$.

Going back to surfaces, one has their mapping class group, which can also be seen as $Out(\pi_1(S))$ for a surface S (see fact 26).

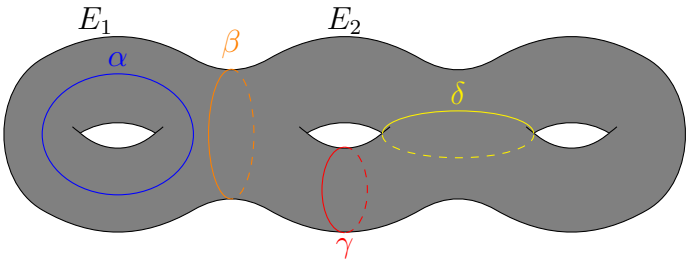
The theory of mapping class groups of surfaces is extremely rich, and has given many interesting properties of actions on Teichmuller spaces (which are deformation spaces of representations of surface groups).

The problem with generalizing such theories, is that they are intrinsically extremely geometrical, and so one would like to know if and how we can define all such objects in a group theoretical way.

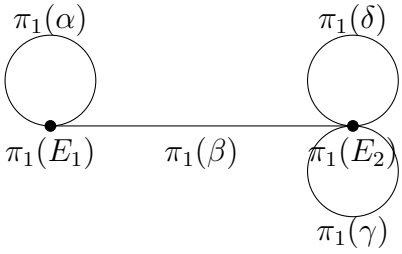
In the case of the mapping class group, we have its building blocks which are Dehn twists around simple closed curves, which one of the main results in this paper is explaining what their generalization to Demuskin groups is, and showing that indeed they make sense in such a setting.

As we explain in fact 34, one can think of curves on a surface, as splittings of $\pi_1(S)$. By splitting of a group G, we mean writing G as a fundamental group of some graph of groups (and not in the sense of split exact sequences). The main splittings we will focus on, are 1-edge graphs of groups (which are in a sense the building blocks of all graphs of groups). These correspond to either an amalgamated free product or to an HNN extension.

To illustrate this, look at the following set of curves on a genus 3 surface



the above will correspond to the following graph of groups



Next, given a splitting one can associate a Dehn twist to it, which is an automorphism of the group (this need not be outer in general).

Using these we try and follows the ideas presented for surfaces, and rewrite the proofs in a similar manner to Demuskin groups, but now using the language of splittings of a group rather than of curves on a surface.

The first section explains what is known and not known already, in arithmetic topology, anabelian geometry and mapping class groups of surfaces.

The second section gives a more in depth look into splittings of a group, and the more combinatorial approach of graphs of groups and Bass-Serre theory.

With the main definitions being that of splittings (definition 42) and of a Dehn twist (definition 50), which will be the objects of study for section 4.

Remark 2. Let us emphasis, that although we restrict ourselves to surface groups and p-adic fields in this thesis, the point of view of graphs of groups and splittings can be used to bring geometry to many more groups, and we think that the point of view we give here can be used to further the global analogy of arithmetic topology as well.

In the final section we focus on Demuskin groups (which as mentioned above, are a family of pro-p groups, which include $G_K(p)$ and the pro-p completion of $\pi_1(S)$) and show our **main results**:

Theorem. *Let G be a Demuskin group, then there exists a family of discrete groups $\mathcal{G}_{r'}$, such that every splitting of G over $\mathbb{Z}_p$, comes from a splitting over $\mathbb{Z}$ of one of the $\mathcal{G}_{r'}$. Furthermore, the splitting of G over $\mathbb{Z}_p$ have a "nice" form, in the sense that they are the pro-p completions of the splittings described in in definition 79. (For a more precise statement, see theorem 101)*

Theorem. *Let G and $\mathcal{G}_{r'}$ be as in the previous theorem, then we have an injection $Out_D(\mathcal{G}_{r'}) \hookrightarrow Out(G)$ (where the subscript D, denotes the subgroup generated by Dehn twists coming from "nice" splittings, as defined in definition 79)*

Theorem. *Let G be a Demuskin group, let α be a splitting of G over $\mathbb{Z}_p$ and let T_α denote the Dehn twist of α, which is an automorphism of G (as defined in 52). Then for every integer k, we have that the image of T_α^k in $Out(G)$ is non-trivial.*

Note that the above theorem gives a large family of non trivial example of outer automorphisms of $G_K(p)$ (which will include the analogue of the Outer automorphism appearing in [33], defined in definition 21, as explained in example 51).

We also note that all the proofs will also have a geometric flavour to them, and can be seen as direct generalizations of classical results about Dehn twists of surfaces.

Remark. Other than the theorems mentioned above, the author thinks that another important contribution of this thesis is by expanding the arithmetic topology dictionary, and by giving a new and more uniform way for discussing surfaces and p-adic fields. In a sense, the author sees this thesis as more of a 'proof of concept' of this way of thinking, and as a first part in a bigger project of extending results about surfaces to p-adic fields (and vice versa), which will include further papers, some of which are already in writting.

Thus, we finish the introduction with a table to help readers find the corresponding guiding case for surfaces in [8]:

	Primer on Mapping class groups [8]	Current paper
Mapping class group	section 2.1	$Out(G)$
simple closed curve	section 1.2.2	splitting of π_1 (def. 42)
intersection of curves	section 1.2.3	Definition 46
The change of coordinates principle	section 1.3	Theorem 101
Definition of Dehn twists	section 3.1.1	Definition 50
Formula for the conjugate of a Dehn twist	Fact 3.7	Lemma 96
Dehn twists are elements of $Out(\pi_1)$	proposition 3.1	Corollary 108
Dehn twists of non-intersection commute	Fact 3.9	Lemma 56
Curve complex	section 4.1	Definition 43

Chapter 2

General Motivation

2.1 Arithmetic topology

As stated in the introduction, arithmetic topology draws an analogy between primes and knots, surfaces and p-adic fields and number fields and 3-manifolds.

In this subsection we will give a very brief overview, for much more information see [30].

For example, class field theory for a number field K can be stated as a sort of 3-dimensional Poincare duality in the étale cohomology of $Spec(O_K)$ ([27]).

Mazur pointed out this line of thought and the analogy between a knot and prime in [26].

Looking at étale homotopy groups for prime fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ we get: groups: $\pi_1^{et}(Spec(\mathbb{F}_p)) = \hat{\mathbb{Z}}, \pi_i^{et}(Spec(\mathbb{F}_p) = 0$ (i≥ 2) (where $\hat{\mathbb{Z}}$ is the pro-finite completion of $\mathbb{Z}$) and so we regard $Spec(\mathbb{F}_p)$ as an arithmetic analogue of a circle S^1.

Since $Spec(\mathbb{Z})$ has étale cohomological dimension 3 (up to 2-torsion) and $\pi_1^{et}(Spec(\mathbb{Z})) = 1$, it can be viewed as the 3-sphere.

We thus get that the embeddings $Spec(\mathbb{F}_p) \hookrightarrow Spec(\mathbb{Z})$ can be viewed as the arithmetic analogue of a knot, i.e. an embedding $S^1 \hookrightarrow S^3$.

The analogies between knots and primes, 3-manifolds and number rings were later studied more by Kapranov ([20]) and Reznikov ([37],[38]) .

In the view of the analogy above, a knot group $G_K = \pi_1(S^3 \backslash K))$ corresponds to a "prime group" $G_{\{(p)\}} = \pi_1^{et}(Spec(\mathbb{Z}) \backslash \{(p)\})$.

More generally, a link L corresponds to a finite set of primes, S, and the link group $G_L = \pi_1(S^3 \backslash L)$ corresponds to $G_S = \pi_1^{et}(Spec(\mathbb{Z}) \backslash S)$, the Galois group of the maximal Galois extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. Under this we see that the absolute Galois group of $\mathbb{Q}$ can be seen as the fundamental group of the 3-sphere minus infinitely many knots.

One has Kapranov-Reznikov-Mazur dictionary:

Arithmetic	Topology
$Spec(O_K) \cup \{\infty\}$ $Spec(\mathbb{Z}) \cup \{\infty\}$	3 manifold M S^3
$Spec(\mathbb{F}_\mathfrak{p}) \subset Spec(O_K)$ primes $\mathfrak{p}_1, ..., \mathfrak{p}_n$	Knot $K \subset M$ Link $K_1 \cup ... \cup K_n$
$\mathfrak{p}$-adic integers $Spec(O_{K_\mathfrak{p}})$ $\pi_1^{et}(Spec(O_{K_\mathfrak{p}})) =< \sigma >$	tubular neighborhood of K, $V(K)$ $\pi_1(V(K)) =< \beta >$
$\mathfrak{p}$-adic field $Spec(K_\mathfrak{p})$ $\pi_1^{et,tame}(Spec(K_\mathfrak{p})) =< \sigma, \tau : \tau^{p-1}[\tau, \sigma] = 1 >$	the torus $\partial V(K)$ $\pi_1(\partial V(K)) =< \alpha, \beta : [\alpha, \beta] = 1 >$
class group H_K	$H_1(M, \mathbb{Z})$
units $O_K^\times$	$H_2(M, \mathbb{Z})$
Maximal Galois group unramified outside S: $\pi_1^{et}(Spec(O_K) \backslash \{(\mathfrak{p}_1, ..., \mathfrak{p}_n)\}$	Link group: $\pi_1(M \backslash K_1 \cup .. \cup K_n)$
Legendre symbol	Linking number
p-adic L-function	Alexander polynomial of K

Under this, a lot of the local structure is not accounted for. For example it only looks at the tamely ramified part, and always corresponds a p-adic field to a genus 1 surface.

We hope to enrich the above dictionary in this paper to take into account for all the Galois group of a p-adic field, and to associate different genus surfaces, depending on the degree of the extension over $\mathbb{Q}_p$.

2.2 Rigidity and anabelian geometry

Another interesting setting where the analogy between arithmetic and topology continues, and is of special interest to us is Mostow rigidity theorem and Uchid-Neukirch [31][47] theorem in anabelian geometry.

First we have the following rigidity theorem of Mostow:

Theorem 3. *Let M and N be complete finite-volume hyperbolic manifolds of dimension $n \geq 3$.*

If $\pi_1(M) \cong \pi_1(N)$, then M and N are isometric.

Similarly in anabelian geometry, one studies how much information about a space X is contained already in its first étale homotopy group $\pi^1_{ét}(X, x)$.

The term "anabelian" is comes from the idea that "the less abelian $\pi^1_{ét}(X, x)$ is, the more information it carries about X".

We want $\pi^1_{\acute{e}t}(X,x)$ to be very not abelian, one example that helps see why we want this is that of elliptic curves.

Let E be an elliptic curve over an algebraically closed field of characteristic 0, it has $\pi^1_{\acute{e}t}(E,x) = \hat{\mathbb{Z}}^2$, where we take any base geometric point x. Thus we have, $\pi^1_{\acute{e}t}(E,x)$ does not distinguish between elliptic curves. Similarly, for finite fields $\mathbb{F}_p$ we have $\pi^1_{\acute{e}t}(\mathbb{F}_p,x) = \hat{\mathbb{Z}}$, and thus again, $\pi^1_{\acute{e}t}$ does not distinguish between finite fields.

An algebraic variety whose isomorphism class is entirely determined by $\pi^1_{\acute{e}t}(X,x)$ is called an anabelian variety.

Uchida [47] and Neukirch [31], proved that Number fields are anabelian. This can be seen as an arithmetic analogue of Mostow's rigidity theorem:

Theorem 4. *Let F and F' be number fields.*

If $\pi^1_{\acute{e}t}(F) = Gal(\bar{F}/F) \cong Gal(\bar{F}'/F') = \pi^1_{\acute{e}t}(F')$, then F' and F are isomorphic, and we have a bijection:

$$Isom_{\mathbb{Q}}(F,F') \to Out(G_F, G_{F'})$$

A similar statement was proven for p-adic fields by Mochizuki [29]:

Theorem 5. *Let K and K' be finite extensions of $\mathbb{Q}_p$. Let $Isom_{\mathbb{Q}_p}(K,K')$ denote the set of $\mathbb{Q}_p$-algebra isomorphisms of K with K'.*

Let $Out_{Filt}(G_K, G_{K'})$ denote the set of outer isomorphisms of filtered groups between the absolute Galois groups of K and K' equipped with the filtrations defined by the higher (i.e., with index > 0) ramification groups in the upper numbering.

Then the natural morphism

$$Isom_{\mathbb{Q}_p}(K,K') \to Out_{Filt}(G_K, G_{K'})$$

induced by "looking at the morphism induced on absolute Galois groups" is a bijection.

The extra condition on the ramification filtration is a necessary one, and there are non isomorphic p-adic fields with isomorphic absolute Galois groups.

Example 6. The fields $\mathbb{Q}_p(\mu_p, \sqrt[p]{p})$ and $\mathbb{Q}_p(\mu_p, \sqrt[p]{p+1})$ are not isomorphic, but have isomorphic absolute Galois groups (this example and more can be found in [18]).

In fact there are non trivial elements in $Out(G_K)$ for any p-adic fields K, as we will explain in the next subsection.

This again fits with the topological case in the sense that p-adic fields can be thought as analogues of surfaces.

In the surface setting we do not have Mostow's rigidity, and $Out(\pi_1(S))$ for a surface S is a very interesting object, also known as the mapping class group of S.

Remark 7. In 1984 Grothendieck[11], made the following important conjecture which motivated the theory of anabelian geometry:

Conjecture 8. *All hyperbolic curves over number fields are anabelian varieties.*

For algebraic curves over finite fields, over number fields and over p-adic field the statement was eventually completed by Mochizuki [28].

We now give Sketch of main parts of the proof:

First, using duality of $\mathbb{Z}_p$-modules of finite length equipped with a continuous G_K-action, one has a natural isomorphism of Galois cohomology modules

$$H^i(K, M) = H^{2-i}(K, M^\vee(1))$$

for $i \geq 0$ (where (1) is a Tate twist, and $\vee$ denotes the Pontrjagin dual).

If M is isomorphic as a $\mathbb{Z}_p$-module to $\mathbb{Z}/p^n\mathbb{Z}$ (for some $n \geq 1$), then it follows from the above isomorphism that M is isomorphic as a G_K-module to $\mathbb{Z}/p^n\mathbb{Z}(1)$ if and only if $H^2(K, M) \cong \mathbb{Z}/p^n\mathbb{Z}$. This is a group-theoretic condition on M.

Thus, we conclude that the isomorphism class of the G_K-module $\mathbb{Z}_p(1)$ can be recovered group-theoretically from G_K.

We also have that the cyclotomic character $\chi : G_K \to \mathbb{Z}_p$ can be recovered entirely group-theoretically from G_K.

Using results from class field theory one also gets that the number q of elements in the residue field of O_K, and well as the absolute degree $[K : \mathbb{Q}_p]$ of K, can be recovered entirely group-theoretically from G_K.

Now let $H \subseteq G_K$ be an open subgroup. Let $L \supseteq K$ be the extension field of K corresponding to H. Using the above to L and H, we see that the number q_L of elements in the residue field of O_L can be recovered group-theoretically from $H \subseteq G_K$.

Note, moreover, that L is unramified over K if and only $q_L = q^{[G_K:H]}$.

Thus, we get that the inertia subgroup $I_K \subseteq G_K$ can be determined group-theoretically from G_K.

Denote by $G_K^v \subseteq G_K$ the higher ramification group associated to the number v in the upper numbering. Let us denote by $U_K^v \subseteq U_K$ the subgroup $1 + m_K^n$, where $m_K \subseteq O_K$ is the maximal ideal, and n is the unique integer for which $n - 1 < v \leq n$.

Then it is well-known ([45] Theorem 1, p. 155) that the image of G_K^v in G_K^{ab} is equal to U_K^v.

Let e_K be the ramification index of K over $\mathbb{Q}_p$. By above it can be recovered group-theoretically from G_K.

Suppose that we are given (in addition to G_K) the subgroup $G_K^v \subseteq G_K$ for some $v = re_K$, where $r \geq 2$ is an integer. Then it follows that we know the subgroup $U_K^v \subseteq U_K$.

Moreover, it follows that the submodule $p^{-r}U_K^v \subseteq U_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ corresponds to the submodule $O_K \subseteq K$ under the isomorphism induced by the p-adic logarithm.

Now let us denote by $\hat{\bar{K}} = \mathbb{C}_K$ the p-adic completion of the field K.

Then one can obtain the following result:

Proposition 9. *Suppose that we are given the following group-theoretic data: the topological group G_K, together with the indexed filtration G_K^v for all $v > 0$.*

Then the K-modules $O_{\bar{K}}$, and $\mathbb{C}_K$ can be recovered group-theoretically from this group-theoretic data.

Next, we will see a consequence of this proposition.

Let V be a finite dimensional $\mathbb{Q}_p$-vector space equipped with a continuous action by G_K.

Corollary 10. *Given a continuous $\mathbb{Q}_p[G_K]$-vector space of finite $\mathbb{Q}_p$-dimension, the issue of whether or not V is Hodge-Tate (as well as the invariants $dim_K V\{q\}$) can be determined entirely group-theoretically from the filtered group G_K.*

We are especially interested in the following type of representation: Let E be a finite Galois extension of $\mathbb{Q}_p$ containing K.

Suppose that the G_K-module V is equipped with an E-action, and that V has dimension one over E.

Thus, $End_E(V) = E$, and the K action on V is given by some representation $\rho_V : G_K \to E^\times$, which factors through G_K^{ab}.

We call the $E[G_K]$-module V uniformizing if the restriction of V to some open subgroup I of U_K is the morphism $I \to E^\times$ induced by restricting some morphism of fields $K \hookrightarrow E$ to $I \subseteq U_K \subseteq K$.

By class field theory, it follows that uniformizing V exist. By [46], Chapter III, Appendix, ï¿œ5, V is uniformizing if and only if $dim_K V\{1\} = [E : K]; dim_K V\{0\} = [E : K]([K : \mathbb{Q}_p] - 1)$. Thus, we obtain the following

Corollary 11. *Given a continuous $E[G_K]$-module V of E-dimension 1, the issue of whether or not V is uniformizing can be determined entirely group-theoretically from the filtered group G_K.*

Let K and K' be local p-adic fields. Let us assume that we are given an isomorphism $\alpha : K \cong K'$ of filtered groups.

Let V be a uniformizing $E[G_K]$-module, for some Galois extension E of $\mathbb{Q}_p$ which contains both K and K'.

Note that we can regard V also as an $E[G_{K'}]$-module. Moreover, by Corollary 11, it follows that V is also a uniformizing $E[G_{K'}]$-module.

Thus, it follows that there exist open submodules $I \subseteq U_K$ and $I' \subseteq U_{K'}$ such that the isomorphism $U_K \cong U_{K'}$ induced by α, maps I onto I', and moreover, the resulting isomorphism $\alpha_I : I \to I'$ fits into a commutative diagram:

$$\begin{array}{ccc} I & \xrightarrow{\alpha_I} & I' \\ \downarrow & & \downarrow \\ E^\times & \xrightarrow{id_{E^\times}} & E^\times \end{array}$$

where the vertical morphisms are induced by field inclusions.

Lemma 12. *If $I \subseteq U_K$ is an open subgroup, then the $\mathbb{Q}_p$-vector space generated by I in K is equal to K.*

Since I (respectively, I'), regarded as a subset of $U_K \subseteq K$ (respectively, $U_{K'} \subseteq K'$), generates K (respectively, K') as a $\mathbb{Q}_p$-vector space, it thus follows that K and K' may be realized as the same subfield of E.

So now we get theorem 5:

That the morphism of the theorem is injective follows by the fact that the centralizer of G_K in $G_{\mathbb{Q}_p}$ is trivial.

Now let us show that the morphism is surjective.

Let $\alpha : G_K \cong G_{K'}$ be an isomorphism that is compatible with the filtrations. Then as above we constructed a field isomorphism $\alpha_K : K \cong K'$.

To get that the morphism induced by α_K is equal to the original α (up to composition with an inner isomorphism), one uses the construction of the analogues $\alpha_L : L \cong L'$ of α_K for corresponding finite extensions L and L' of K and K'.

2.2.1 explicit outer automorphism

In this subsection we will go over a structure theorem for Galois groups of p-adic fields, which will later be used to construct outer morphisms of $G_{\mathbb{Q}_p}$ (this can be found in [33], end of Chapter 7).

Theorem 13 ((Jannsen-Wingberg)). *Let K be a p-adic field, with $N = [K : \mathbb{Q}_p]$, q the cardinality of the residue field of K, p^s the order of the group of all p-power roots of unity in K^{tr}, the maximal tamely ramified extension of K.*

The group $Gal(K^{tr}/K)$ is generated by σ, τ satisfying $\sigma\tau\sigma^{-1} = \tau^q$, and denote by $g, h \in \mathbb{Z}_p$ the image of σ, τ respectivly, under the cyclotomic character.

Then the group G_K has $N + 3$ generators (where $N = [K : \mathbb{Q}_p]$), $\sigma, \tau, x_0, ..., x_N$, with the following relations/conditions:

A) The closed normal subgroup generated by $x_0, ..., x_N$ is a pro-p-group.

B) The elements σ, τ satisfy the tame relation $\sigma\tau\sigma^{-1} = \tau^q$.

C) i) If N is even $x_0^\sigma =< x_0, \tau >^g x_1^{p^s}[x_1, x_2]...[x_{N-1}, x_N]$

ii) If N is odd $x_0^\sigma =< x_0, \tau >^g x_1^{p^s}[x_1, y_1][x_2, x_3]...[x_{N-1}, x_N]$

where $< x_0, \tau >= (x_0^{h^{p-1}}\tau x_0^{h^{p-2}}...x_0^h\tau)^{\frac{\pi}{p-1}}$ and where y_1 is a certain element in the subgroup generated by x_1, σ, τ.

Remark 14. In a sense this would mean that this should correspond to a surface of genus $\frac{N}{2} + 1$.

For the full proof we refer to [17] and [6], it is based on a theory of H. Koch [22] which axiomizes the fact that for every finite, tamely ramified extension L/K the group $G_L(p)$ is a Demuskin group.

Each such Koch groups has invariants n, p, s, α .

There are two main steps to the proof:

1. Proving two Koch groups with the same invariants are isomorphic.

2. The abstract pro-finite group, defined above, is a Koch group with the same invariants as G_K and so they are isomorphic.

We will now go over the main ideas of the proof.

Let H is an open normal subgroup of $\mathcal{G} = Gal(K^{tr}/K)$ contained in the kernel of χ_{tr} (the cyclotomic character from $\mathcal{G}$), so that μ_{p^s} is contained in the fixed field L of H, and denote by $G = \mathcal{G}/H = Gal(L/K)$.

We have that $G_L(p) = Gal(L(p)/L)$, is the Galois group of the maximal p-extension of L, it is the maximal pro-p-factor group of G_L and is a Demuskin group.

For these groups we have the following known properties.

I. - $dimH^1(G_L, \mathbb{F}_p) < \infty$, $dimH^2(G_L, \mathbb{F}_p) = 1$ and $H^1(G_L, \mathbb{F}_p) \times H^1(G_L, \mathbb{F}_p) \xrightarrow{\cup} H^2(G_L, \mathbb{F}_p)$ is a non degenerate anti-symmetric bilinear form.

II. - Looking at $H^1(H,\mathbb{F}_p)$ as a 1-dimensional subspace of the symplectic space $H^1(G_L,\mathbb{F}_p)$ we have an isomorphism of G-modules $H^1(H,\mathbb{F}_p)^\perp/H^1(H,\mathbb{F}_p) \cong \mathbb{F}_p[G]^n$.

With respect to the induced non-degenerate bilinear form this G-module is a direct sum of two totally isotropic G-submodules.

III. - $(G_L(p)^{ab})_{tor} \cong \mu_{p^s}$ as a G-module.

Remark 15. Condition I expresses the fact that $G_L(p)$ is a Demuskin group.

By class field theory $H^1(G_L,\mathbb{F}_p)$ is dual to $L^*/L^{*^p} = (\pi)/(\pi)^p \times U^1/(U^1)^p$ where π is a prime element of K and U^1 is the group of principal units of L.

The cup product goes to the Hilbert symbol on L^*/L^{*^p} and $U^1/(U^1)^p$ contains

$$H^1(H,\mathbb{F}_p)^\perp/H^1(H,\mathbb{F}_p)$$

as a subspace of dimension 1 which is isomorphic to $\mathbb{F}_p[G]$.

The last isomorphism is a result of Iwasawa. The assertion on the the direct sum of totally isotropic submodules property is due to Koch.

Using the above axioms we can define a Koch group:

Definition 16. Let $\mathcal{G}$ be a profinite group, generated by two elements σ,τ such that $\sigma\tau\sigma^{-1} = \sigma^q$ and let $\alpha : G \to (\mathbb{Z}/p^s\mathbb{Z})^*$ be a character.

Remark 17. For the case of $\mathcal{G}$ being $Gal(K^{tr}/K)$ and α is the cyclotomic character.

Definition 18. A Koch group over $\mathcal{G}$ of degree n , of torsion p^s and character α is a pro-finite group X together with a surjective homomorphism $\Phi : X \to \mathcal{G}$ such that for each open normal subgroup $H \subset G$ in the kernel of α, conditions I, II, III hold for $G_{L(H)} := \Phi^{-1}(H)$, where μ_{p^s} is replaced by the twisted $\mathcal{G}$ module $\mathbb{Z}/p^s\mathbb{Z}(\alpha)$

For these Demuskin formation we have now the following uniqueness theorem, which was announced by Koch and was proved in full detail and even larger generality by Wingberg [52].

Theorem 19 ((Kock, Wingberg)). *Two Koch groups X and Y over G with the same invariants n, p, s and α are isomorphic.*

We will explain the main ideas of the proof in a more field theoretic situation.

We would like to reconstruct G_K by means of the axioms I, II, III.

Since $Gal(\bar{K}/K^{tr})$ is a pro-p group we have that $\bar{K} = \cup_{L\subset K^{tr}} L(p)$ and hence $G_K = \underset{\leftarrow H}{lim} Gal(L(p)/K)$.

Ans so it is enough to show the group $Gal(L(p)/K)$ is reconstructed by the axioms.

To do this, look at the short exact sequence $1 \to Gal(L(p)|L) \to Gal(L(p)|K) \to G \to 1$ and the cental series of the Demuskin group $G_L(p) = Gal(L(p)/L)$

$$G_L^0(p) = G_L(p), G_L^i(p) := [G_L^{i-1}(p), G_L(p)] \cdot (G_L^{i-1}(p))^{p^s}$$

Let L_i be the fixed field of $G_L^i(p)$, i.e. L_i/L_{i-1} is the maximal abelian extension of exponent p^s.

We have $1 \to Gal(L_i/L) \to Gal(L_i/K) \to G \to 1$.

Since $Gal(L(p)/K) = \underset{\leftarrow}{lim} Gal(L_i/K)$ we reduce to reconstruction of $Gal(L_i/K)$ from the axioms.

This is done inductively on i and with base cases $i = 1, 2$.

In the case $i = 1$ we have to reconstruct the group $Gal(L_1/L)$ as a G-module from the axioms and to determine the cocycle of the group extension in $H^2(G, Gal(L_1/L))$.

Now $Gal(L_1/L)$ is dual to $H^1(G_L, \mathbb{Z}/p^s)$ and this is close to the G-module

$$H^1(H, \mathbb{Z}/p^s)/H^1(H, \mathbb{Z}/p^s) = \mathbb{Z}/p^s[G],$$

and can give the G-structure of $Gal(L_1/L)$.

But one has to determine $H^1(G_L, \mathbb{Z}/p^s)$ not only as a G-module but also as a symplectic G-module, and also to keep track of that part of $Gal(L_1/L)$ which comes from the torsion part of $G_L(p)^{ab}$.

For this, there is a function called, the Bockstein operator

$$H^1(G_L, \mathbb{Z}/p^s) \overset{B}{\to} H^2(G_L, \mathbb{Z}/p^s)$$

whose image is dual to this torsion part in $Gal(L_1/L)$.

To determine the cocycle in $H^2(G, Gal(L_1/L))$ associated to $1 \to Gal(L_1/L) \to Gal(L_1/K) \to G \to 1$, one looks at the p-Sylow group G_p of G.

It is cyclic, and has $H^2(G_p, Gal(L_1/L)) = H^2(G_p, L^*/(L^*)^{p^s}) = H^0(G^p, L^*/(L^*)^{p^s})$.

The cocycle is then represented by a prime element π of K.

The selection of this prime element can be done group theoretically by taking a section $\mathcal{G}^{ab} \to G_K^{ab}$.

In this way $Gal(L_1/K)$ is completely characterized by the axioms.

We will omit the slightly more complicated $i = 2$ case.

The induction step then uses some solutions to certain embedding problems, which then completes the proof of theorem 19.

The next step for proving theorem 13, is to construct an abstract Koch group X with the same invariants n, p^s, α as G_K.

This is done as follows:

Let F_{n+1} be the free pro-finite group of $n+1$ generators $z_0, ..., z_n$ and let $F_{n+1} * \mathcal{G}$ be the free pro-finite product of F_{n+1}, with $\mathcal{G} = Gal(K^{tr}/K)$.

We then have an exact sequence $1 \to Z \to F_{n+1} * \mathcal{G} \to \mathcal{G} \to 1$, where Z is the normal subgroup generated by $z_0, ..., z_n$. Let P be the maximal pro-p-factor group of Z.

The kernel of $Z \to P$ is normal in $F_{n+1} * \mathcal{G}$ and let $F(n+1, \mathcal{G})$ be the quotient by that kernel. We obtain $1 \to P \to F(n+1, \mathcal{G}) \to \mathcal{G} \to 1$ where P is a normal subgroup of $F(n+1, \mathcal{G})$ generated by $x_0, ..., x_n$ the images of $z_0, ..., z_n$.

The group $F(n+1, \mathcal{G})$ is in a sense universal among the split group extensions of $\mathcal{G}$ by a pro-p group.

We now consider the element $r = x_0^{-\sigma} < x_0, \tau >^g x_1^{p^s}[x_1, x_2][x_3, x_4]...[x_{n-1}, x_n]$ in $F(n+1, \mathcal{G})$, where $< x_0, \tau >= (x_0^{h^{p-1}} \tau x_0^{h^{p-2}} ... x_0^h \tau)^{\frac{\pi}{p-1}}$, and g, h are the images of σ, τ under α respectivly. One can show $r \in P$.

We now take $X = F(n+1, \mathcal{G})/ < r >$, and one can prove:

Theorem 20. *X is a Koch group over $\mathcal{G}$ of degree n , torsion p^s and character α.*

In [33] (chapter 7 section 5) an example of a non trivial outer automorphisms of G_K is constructed, thus showing that the extra filtration preserving condition in theorem 5 is necessary.

It is easier to describe and show it is outer for $N = [K : \mathbb{Q}_p] > 1$.

Let $\sigma, \tau, x_0, ..., x_N$ be the generators of G_K described in theorem 13.

Definition 21. Define $\psi : G_K \to G_K$ by $\psi(y) = y$ for $y = \sigma, \tau, x_0, ..., x_{N-1}$ and $\psi(x_N) = x_N x_{N-1}$.

Remark 22. In example 51 we see that for the right choice of splitting, the above construction is also a Dehn twist in the sense of definition 50.

This is then an automorphism of G_K,since $[x_{N-1}; x_N] = [x_{N-1}; x_N x_{N-1}]$ and so the generators $\sigma, \tau, x_0, ..., x_{N-1}, x_N x_{N-1}$ satisfy both relations if $N > 1$.

Now suppose that is an inner automorphism, i.e. there is an element $\rho \in G_K$ such that $\psi(z) = z^\rho$ for all $z \in G_K$.

Denote by V_K^i the i-th term of the p-central series of the ramification group V_K with $V_K^1 = V_K$.

Since $x_{N-1}^\rho = \psi(x_{N-1}) = x_{N-1}$ and since $x_{n-1} V_K^2$ generates a free $\mathbb{F}_p[[G_K]]$ module in V_K/V_K^2 , by [17], we obtain that $\rho \in V_K$.

It follows that $x_N V_K^2 = x_N x_{N-1} V_K^2$ which is a contradiction. Thus, if $N = [K : \mathbb{Q}_p] > 1$, we have constructed a nontrivial outer automorphism of G_K.

The case $K = \mathbb{Q}_p$ is more difficult. It is constructed in a similar manner, but also uses the following result from [52].

Theorem 23. *Let $\psi_3 : G_K/V_K^3 \to G_K/V_K^3$ be an automorphism of G_K/V_K^3 which induces the identity on the factor group G_K/V_K.*

Then there exists an automorphism of G_K which coincides with ψ_3 modulo V_K^2.

2.3 Mapping class groups of surface

We would like to have some arithmetic theory similar to the theory of mapping class groups, and more specifically the mapping class group of a surface (for more information on the subject we refer to [9].

Let S be a connected, closed, orientable surface and $\mathrm{Homeo}^+(S)$ the group of orientation-preserving, or positive, homeomorphisms of S ((that restrict to the identity on ∂S if S has a boundary).

This group has a natural topology, the compact-open topology. It can be defined easily by a distance function: if we are given a metric d on S inducing its topology then the function defined by

$$\delta(f, g) = \sup_{x \in S} (d(f(x), g(x))$$

is a distance inducing the compact-open topology on $\mathrm{Homeo}^+(S)$.

The connected component of the identity for this topology is denoted $\mathrm{Homeo}_0(S)$. By definition it is equal to the homeomorphisms of S which are isotopic to the identity and it is a normal subgroup of the group of positive homeomorphisms.

Definition 24. We define the mapping class group of S as the group

$$\mathrm{MCG}(S) = \mathrm{Homeo}^+(S)/\mathrm{Homeo}_0(S)$$

Modifying the definition to include all homeomorphisms we obtain the extended mapping class group $\mathrm{MCG}^{\pm}(S)$.

Note that these groups are countable, and the extended mapping class group $\mathrm{MCG}^{\pm}(S)$, contains the mapping class group as a subgroup of index 2.

Remark 25. This definition can also be made in the differentiable category: if we replace all instances of "homeomorphism" above with "diffeomorphism" we obtain the same group, that is the inclusion $\mathrm{Diff}^+(S) \subset \mathrm{Homeo}^+(S)$ induces an isomorphism between the quotients by their respective identity components.

If S is closed and f is a homeomorphism of S then we can define an automorphism f_* of the fundamental group $\pi_1(S, x_0)$ as follows: fix a path γ between x_0 and $f(x_0)$ and for a loop α based at x_0 representing an element $[\alpha] \in \pi_1(S, x_0)$ define $f_*([\alpha])$ to be the element of the fundamental group associated to the loop $\bar{\gamma} * f(\alpha) * \gamma$.

This automorphism depends on the choice of γ , but only up to conjugation. Thus we get a well-defined map Φ from $\mathrm{Homeo}(S)$ to the outer automorphism group $\mathrm{Out}(\pi_1(S, x_0))$.

Fact 26. *The map* Φ *is a morphism and its kernel is exactly the subgroup* $\mathrm{Homeo}_0(S)$.

The Dehn–Nielsen–Baer theorem [4, 34] states that it is in addition surjective.

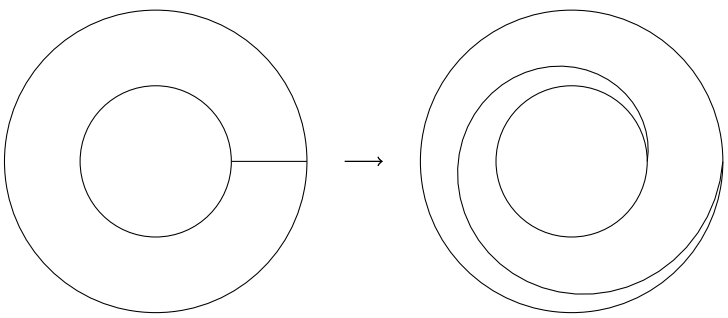
In particular, it implies that the extended mapping class group $\mathrm{MCG}^{\pm}(S)$ *is isomorphic to the outer automorphism group* $\mathrm{Out}(\pi_1(S))$.

The image of the mapping class group is an index 2 subgroup of the outer automorphism group, which can be characterized by its action on homology.

A closed curve in a surface S is a continuous map $S^1 \to S$, it is simple if the map in injective. A closed curve is called essential if it is not homotopic to a point, a puncture, or a boundary component. We will usually identify a closed curve with its image in S.

Consider the annulus $A = S^1 \times [0, 1]$, we embed it in the plane with polar coordinates via $(\theta, t) \mapsto (\theta, t + 1)$, and take the orientation induced by the standard orientation of the plane. Define $T : A \to A$ be the "left twist map" of A given by the formula $T(\theta, t) = (\theta + 2\pi t, t)$ (note that taking instead $\theta - 2\pi t$ would give a right twist).

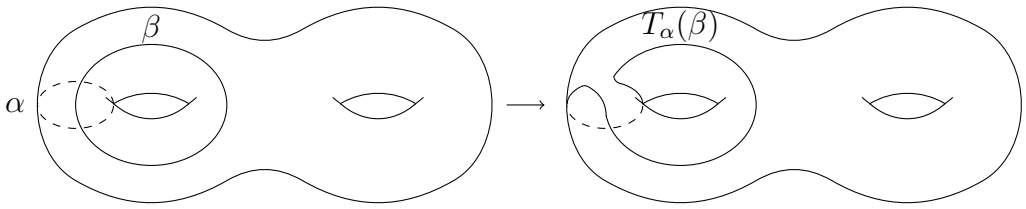
The map T is an orientation-preserving homeomorphism that fixes the boundary of A point-wise.



Definition 27. Let α be simple closed curve on S and let N be a regular neighborhood of α and take ϕ be an orientation preserving homeomorphism then there is a homeomorphism f from A to the canonical annulus A_0, sending C to a circle with the counterclockwise orientation.

Define a homeomorphism T_α of S as follows: on $S \setminus N$ it is the identity, and on N it is equal to $\phi^{-1} \circ T \circ \phi$.

The class of T_α in the mapping class group $\mathrm{MCG}(S)$ does not depend on the choice of ϕ made above, and the resulting element is called the Dehn twist about α.



Remark 28. One would like to think of the map ψ from Definition 21, as some sort of arithmetic Dehn twist.

If α is not null-homotopic this mapping class is nontrivial, and more generally the Dehn twists defined by two non-homotopic curves are distinct elements in the mapping class group.

In the mapping class group of the torus identified with $\mathrm{SL}_2(\mathbb{Z})$ the Dehn twists correspond to unipotent matrices.

For example, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ corresponds to the Dehn twist about a horizontal curve in the torus.

The mapping class group is generated by the subset of Dehn twists about all simple closed curves on the surface.

The Dehn–Lickorish theorem states that it is sufficient to select a finite number of those to generate the mapping class group. This generalises the fact that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

In particular, the mapping class group of a surface is a finitely generated group.

The least possible cardinality of Dehn twists generating the mapping class group of a closed surface of genus $g \geq 2$ is $2g + 1$; this was proven later by Humphries.

Theorem 29. *(Nielsen, Thurston) An element $g \in \mathrm{MCG}(S)$ is either:*

- Of finite order

- Reducible: there exists a set of disjoint closed curves on S which is preserved by the action of g

- Pseudo-Anosov.

The main content of the theorem is that a mapping class which is neither of finite order nor reducible must be pseudo-Anosov (which is a dynamical property).

2.3.1 Generators of the mapping class group and the curve complex

An important first step to understanding the mapping class group, is the fact that it is generated by a finite amount of Dehn twists.

To prove that, one introduces the curve complex.

Definition 30. The curve complex is a simplicial complex associated to a surface S.

Vertices are free homotopy classes of essential simple closed curves on S, and $v_1, ..., v_n$ distinct vertices span a simplex if and only if they can be homotoped to be pairwise disjoint.

Masur and Minsky proved that he curve complex is hyperbolic, and they proceeded to use that fact to derive new information about mapping class groups.

The curve complex is acted on nicely by the mapping class group, and one can show that $MCG(S)$ is generated by $stab_v$ and h where v, w are two vertices with an edge between them, and $h(v) = w$.

2.4 Teichmuller spaces and Galois representations

An important space associated to a surface is its Teichmuller space:

Definition 31. Given a surface S the Teichmï¿œller space $T(S)$ is the space of marked complex (equivalently, conformal or complete hyperbolic) structures on S.

These can be represented by pairs (X, f) where X is a Riemann surface and $f : S \to X$ a homeomorphism, modulo a suitable equivalence relation.

There is an action of the group $\text{Homeo}^+(S)$ on such pairs, which descends to an action of $\text{MCG}(S)$ on Teichmï¿œller space.

This action has many interesting properties; for example it is properly discontinuous (though not free).

The action extends to the Thurston boundary of Teichmï¿œller space, and the Nielsen-Thurston classification of mapping classes can be seen in the dynamical properties of the action on Teichmï¿œller space together with its Thurston boundary. Namely:

Finite-order elements fix a point inside Teichmï¿œller space (more concretely this means that any mapping class of finite order in MCG(S) can be realized as an isometry for some hyperbolic metric on S); Pseudo-Anosov classes fix the two points on the boundary corresponding to their stable and unstable foliation and the action is minimal (has a dense orbit) on the boundary; Reducible classes do not act minimally on the boundary.

One can also think of $T(S)$ as a space of representations of $\pi_1(S)$ in the following sense:

Theorem 32. *The space $T(S)$ can be identified with a connected component in the representation space $Rep(\pi_1(S), PSL(2,\mathbb{R})) = Hom(\pi_1(S), PSL(2,\mathbb{R}))/PSL(2,\mathbb{R})$, where $PSL(2,\mathbb{R})$ acts by conjugation.*

This brought people to define higher Teichmuller spaces in the following way:

Let G be a simple Lie group G of higher rank, (such as $PSL(n,\mathbb{R})$ for $n \geq 3$).

A higher Teichmï¿œller space is a subset of $Hom(\pi_1(S), G)/G$ which is a union of connected components that consist entirely of discrete and faithful representations.

For nice enough G, these higher spaces were also shown to have proper actions of the mapping class group

We thus expect that in the arithmetic setting, the role of the Teichmuller space will be some deformation space of Galois representations.

For deformations of the trivial representation mod p this is the same as representations of $G_K(p)$, since all representations which are trivial mod p factor through $G_K(p)$

Remark 33. As seen in the previous section, the methods used in the proof of theorem 5 involve p-adic Hodge theory, and special type of Hodge-Tate representations.

Looking at outer automorphism of $G_K(p)$ we also hope we could say more about different p-adic Hodge theory structures sitting inside the space of Galois representations.

Chapter 3

From curves to graphs of groups

3.1 Splittings of groups and graphs of groups

Recall from that a simple closed curve on a surface S is a continuous injective map $S^1 \to S$.

Fact 34. *A simple closed curve on a surface S, gives rise to a splitting of $\pi_1(S)$ as an amalgamated free product over $\mathbb{Z}$, or as an HNN extension over $\mathbb{Z}$.*

In fact all splittings over $\mathbb{Z}$ of $\pi_1(S)$, into HNN extensions and amalgamated free products, arise in such a way, and so we have a bijection between isotopy classes of simple closed curves, and such splittings of $\pi_1(S)$ over $\mathbb{Z}$.

This can be found in [53] theorem 4.12.1.

The above leads us to a way to generalize ideas related to simple closed curve to a any group.

First, let us recall some basic definitions:

Definition 35. (amalgamated free product) Let A, B and C be groups with monomorphisms $\varphi_1 : C \to A$, $\varphi_2 : C \to B$. We define the amalgamated free product of A and B over C, denoted by $A *_C B$, to be the group generated by A and B together with the relation $\varphi_1(c)\varphi_2(c)^{-1} = 1$ for all $c \in C$.

Definition 36. (HNN extension) Let A be a group and $C \subset A$ be a subgroup, and let $\theta : C \to A$ be a monomorphism. We define the HNN (G. Higman, B. H. Neumann, H. Neumann) extension of A relative to θ, denoted by $A*_\theta$ to be the group generated by A and an element t with the relation $\theta(c) = tct^{-1}$ for all $c \in C$. The new generator t is called the stable letter.

Using graphs of groups one can think of both of these ideas together:

Definition 37. A graph X, consists of a set of vertices $V(X)$, and a set of (oriented) edges $E(X)$, an edge reversal map $e \mapsto \bar{e}$ such that $e \neq \bar{e}$ and $\bar{\bar{e}} = e$ for all edges (that is each edge has an orientation, and we also have the reverse orientation edge as part of the graph) and a map $v : E(X) \to V(X)$ sending an edge to its terminal vertex (the initial vertex of an edge is thus $v(\bar{e})$.

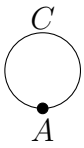
Definition 38. A graph of groups, $(X, \boldsymbol{G})$, is a connected graph X together with a function $\boldsymbol{G}$, which assigns a group $\boldsymbol{G}_v$ for all vertices of the graph $V(X)$, and $\boldsymbol{G}_e$ for all edges $e \in E(X)$ such that $\boldsymbol{G}_e = \boldsymbol{G}_{\bar{e}}$, and for each edge $e \in E(X)$ we also have a monomorphism $\varphi_e : \boldsymbol{G}_e \to \boldsymbol{G}_{v(e)}$ where $v(e)$ is the terminal vertex of e.

Given a graph of groups $(X, \boldsymbol{G})$, let $T \subset X$ be a maximal subtree of X. We define the fundamental group $\pi_1(X, \boldsymbol{G}, T)$ of $(X, \boldsymbol{G})$ at T, to be the group generated by the vertex groups G_v for all $v \in V(X)$ and the elements t_e for all $e \in E(X)$ subject to the following relations:

1. $t_{\bar{e}} = t_e^{-1}$ for all $e \in E(X)$
2. $t_e \varphi_e(c) t_e^{-1} = \varphi_{\bar{e}}(c)$ for all $e \in E(X)$ and $c \in \boldsymbol{G}_e$
3. $t_e = 1$ for all $e \in E(T)$.

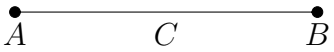
Remark 39. The above definition of fundamental group is independent of the choice of maximal subtree T.

We can now see that for a graph of groups with 1 edge and 1 vertex



the fundamental group gives us an HNN extension $A*_C$.

For a graph of groups with 1 edge and 2 vertices



the fundamental group gives us an amalgamated free products $A *_C B$.

Definition 40. Let $(X, \boldsymbol{G})$, $(X', \boldsymbol{G}')$ be a graph of groups. An isomorphism of $(X, \boldsymbol{G})$ to $(X', \boldsymbol{G}')$ is a tuple of the form $(H_X, (H_v)_{v \in V(X)}, (H_e)_{e \in E(X)}, (\delta(e))_{e \in E(X)})$, where:

- $H_X : X \to X'$ is a graph isomorphism,
- $H_v : \boldsymbol{G}_v \to \boldsymbol{G}'_{H_X(v)}$ is a group isomorphism,
- $H_e = H_{\bar{e}} : \boldsymbol{G}_e \to \boldsymbol{G}'_{H_X(e)}$ is a group isomorphism,

• $\delta(e)$ is an element of $\boldsymbol{G}'_{v(H_X(e))}$, with the additional compatibility requirement that

$H_{v(e)}(\varphi_e(c)) = \delta(e)\varphi_{H_X(e)}(H_e(c))\delta(e)^{-1}$ for all $e \in E(X), c \in \boldsymbol{G}_e$.

Given a graph of groups $(X, \boldsymbol{G})$, one can associate the Bass-Serre covering tree $\tilde{X}$, which is a certain tree with a $\pi_1(X, \boldsymbol{G})$ action on it, without edge inversion. This is a kind of universal cover of $(X, \boldsymbol{G})$, and one has that $\tilde{X}/\pi_1(X, \boldsymbol{G})$ is isomorphic to $(X, \boldsymbol{G})$.

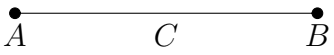
Similarly, given a tree T for which a group G acts on without edge inversion, one has a notion of the graph of group quotient T/G, for which the Bass-Serre covering is T.

To make this more precise, the graph X of groups quotient will be the quotient graph T/G, and vertex and edge groups will be isomorphic to the vertex and edge stabilizers of vertices and edges of T under the G action.

In such a way we can move between the notion of trees with a group action on them, and graphs of groups.

One can also see that two graphs of groups are isomorphic if their Bass-Serre trees have a G-equivariant graph isomorphism.

Example 41. Let $(X, \boldsymbol{G})$ be a graph of groups with a single edge e and two vertices v_1, v_2, with $\boldsymbol{G}_e = C$, $\boldsymbol{G}_{v_1} = A$,$\boldsymbol{G}_{v_2} = B$ with monomorphisms $\varphi_1 : \boldsymbol{G}_e \to \boldsymbol{G}_{v_1}$, $\varphi_2 : \boldsymbol{G}_{\bar{e}} \to \boldsymbol{G}_{v_2}$.



We have $\pi_1(X, \boldsymbol{G}) \cong A *_C B = G$.

In this case we would have $\tilde{X}$would be the tree with $V(\tilde{X}) = \{gA : g \in G\} \amalg \{gB : g \in G\}$, two vertices gA and fB have an edge between them if there is $a \in A$ such that $fB = gaB$. The degree of a vertex gA will be $[A : \varphi_1(C)]$ and of gB it will be $[B : \varphi_2(C)]$.

Definition 42. Given a group G, we define its set of splittings $Split(G)$ to be the set of isomorphism classes of 1 edge graphs of groups (i.e. HNN extensions and amalgamated free products), with fundamental group isomorphic to G.

The set of $\mathbb{Z}$ splittings, $Split(G, \mathbb{Z})$, are splittings for which all edge stabilizers are isomorphic to $\mathbb{Z}$.

Definition 43. We define the curve complex of G, denoted by $\mathcal{C}(G)$, to be the complex whose vertices are $\alpha \in Split(G, \mathbb{Z})$, and n vertices $v_1, ..., v_n$ span an n-dimensional simplex if and only if they are pairwise non-intersecting (i.e. compatible), in other words, if there is a graph of groups with n edges, all having edge group $\mathbb{Z}$, such that it is a refinement of all v_i.

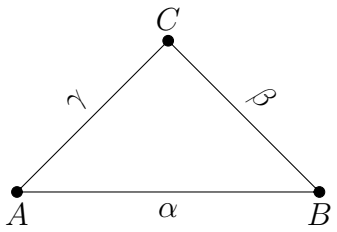
3.2 Intersection of Splittings

We would also like to understand when do two simple closed curves intersect using the splitting language.

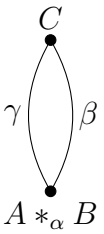
Definition 44. Let $(X, \boldsymbol{G})$ be a graph of groups and let T be a subgraph, we define a new graph $(X/T, \boldsymbol{G}(X/T))$, the graph obtained by collapsing the tree , to have vertices $V(X)\backslash V(T) \cup v_T$ where v_T is a new vertex representing T. And the edges to be all edges between $V(X)\backslash V(T)$ as in X together with edges between v_T and $V(X)\backslash V(T)$ if there was an edge joining a vertex in $V(X)\backslash V(T)$ to a vertex in T.

The groups for the edges and vertices of $X\backslash T$ are as in the original $(X, \boldsymbol{G})$ and the group for the new vertex v_T is the fundamental group of $(T, \boldsymbol{G}|_T)$.

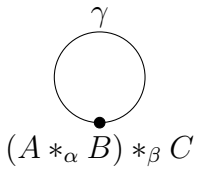
Example 45. We can us the above to compute the fundamental group of the following graph of groups:



We start by collapsing the edge of α and so we get



next collapsing the edge of β we get



and thus the fundamental group is: $((A *_\alpha B) *_\beta C)*_\gamma$.

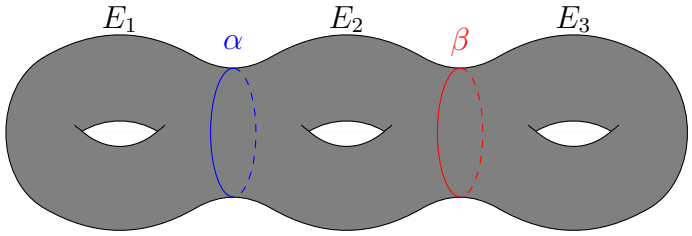
Definition 46. We call two splittings compatible, or non-intersecting if there is a graph of groups such that collapsing one edge (collapsing the subgraph given by the edge and its two vertices) gives us the first splitting and collapsing another gives us the second. We say $i(\alpha, \beta) = 0$ if they are compatible, and we say $i(\alpha, \beta) \neq 0$ if they are not compatible.

For example, two free products $A * B = G = A' * B'$ are compatible if and only if there is a splitting of $G = C * D * F$ such that $(C * D) = A, F = B$ and $C = A', (D * F) = B'$.

Non-compatible splittings are also called intersecting.

One can show (see [41]) that two curves intersect if and only if the corresponding splittings intersect.

Example 47. Suppose we have the situation as shown in the picture below:

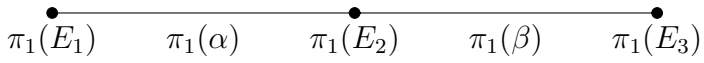


Namely a group $G = \pi_1(S_3)$ and two non intersecting curves α (the blue curve) and β (the red curve). Cutting along them we get three subsurfaces E_1, E_2, E_3.

The splitting of α will then be $\pi_1(E_1) *_{\pi_1(\alpha)} \pi_1(E_2 \cup E_3)$ and of β this would be $\pi_1(E_1 \cup E_2) *_{\pi_1(\beta)} \pi_1(E_3)$.

The two curves can easily be seen to be non intersecting, and both of these can be realized at the same time as $G = \pi_1(E_1) *_{\pi_1(\alpha)} \pi_1(E_2) *_{\pi_1(\beta)} \pi_1(E_3)$.

In a graph of groups form this would be:

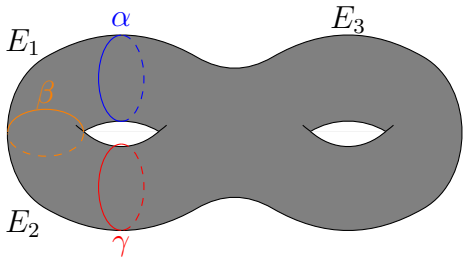


Example 48. Let us go back to example 45 and see what a geometric interpretation of it could be, say on a genus 2 surface.

First note that any graph of groups coming from collapsing the one in example 45 would of course not intersect the collapsings, by definition.

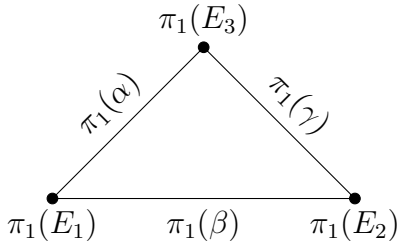
From the form of the splitting, we get that the curves corresponding to the edges will be non separating curves, such that cutting any two of them would separate the surface into two components, and cutting all three would give us 3 components.

From the above we see that a possible picture would be the following picture:



and so we see that in fact, we have cut 3 times along the same homotopy class of a simple closed curve, which of course does not intersect itself.

The graph of groups can be written as follows:



Remark 49. One can actually take this a step further and measure how non compatible splittings are and define an intersection number for them.

Let T_1 and T_2 be two simplicial trees with an action of a group G on them, let $C \subset T_1 \times T_2$ be the smallest non-empty closed invariant (under the diagonal action) subset of $T_1 \times T_2$ having convex fibers (a subset $E \subset T_1 \times T_2$ has convex fibers if for both $i \in \{1, 2\}$ and every $x \in T_i$, $E \cap p_i^{-1}(x)$ is convex where p_i is the canonical projection).

This is also known as the core or the Guirardel core of the two graphs (see [12] for more information).

We define the intersection number $i(T_1, T_2)$ to be the covolume of the core.

If the two splittings don't intersect if and only if their core is 1-dimensional.

A common refinement for them is then $\hat{C}$, the smallest connected invariant subset of $T_1 \times T_2$ having convex fibers.

Note that there is an equivalent way using almost invariant subsets of the group G associated to the splitting, the intersection number of the splittings is then determined by intersections of certain sets and cosets. (see [41]).

Again it is known this is compatible with the notions of interesections number of simple closed curves on a surface.

We hope to use such notations in later works to better understand the relations between Dehn twists coming from intersecting splittings.

Define the translation length function $l_T : G \to \mathbb{R}$, of an action of G on a tree T to be:

$$l_T(g) = inf_{p \in T} d_T(p, pg)$$

An element g is said to be elliptic with respect to the G-tree T if $l_T(g) = 0$, in which case it fixes a point, and hyperbolic if the translation length $l_T(g)$ is positive.

Let $\alpha = A *_{<c>} B$ (or $A*_{<c>}$) and $\beta = A' *_{<c'>} B'$ (or $A'*_{<c'>}$) be one edge $\mathbb{Z}$-splittings of a group G.

Define the translation length of α on β to be:

We say that a β is hyperbolic with respect to α if the action of c' on T, the Bass-Serre tree of α, doesn't fix a point. (note that by [40] this is true if and only if β is hyperbolic with respect to α).

If this is the case, then the action of c' instead preserves a line in T, and it acts on it by translation of length $l_T(c')$.

So we see that β is hyperbolic with respect to α, if $l_T(c') > 0$, for T, the Bass-Serre tree of α.

This will also be equivalent to having that c' is not contained in a conjugate of A or B.

By remark 3.4 in [41], if α is hyperbolic with respect to β then the splittings intersect.

3.3 Dehn twists for discrete groups

Definition 50. Given a group and a $\mathbb{Z}$ splitting $A *_{<c>} B$, we define the Dehn twist δ to be the automorphism $\delta(a) = a, \delta(b) = \varphi(c) b \varphi(c)^{-1}$ for all $a \in A, b \in B$.

Similarly given an HNN extension $A*_\theta$ where $\theta :< c > \to A$ we define the Dehn twist δ to be $\delta(a) = a$ for all $a \in A$ and $\delta(t) = ct$.

Example 51. Let n be an even number and let G be the group with the following presentation: $G =< x_1, x_2, ..., x_n : x_1^p[x_1, x_2]...[x_{n-3}, x_{n-2}][x_{n-1}, x_n] = 1 >$. Let A be the free group on $n-1$ generators $x_1, ..., x_{n-1}$, and let θ be the map sending x_{n-1} to $x_1^p[x_1, x_2]...[x_{n-3}, x_{n-2}]x_{n-1}$, we thus get the splitting of G as the HNN extension $A*_\theta = \{x_{1,...,}x_{n-1}, t | tx_{n-1}t^{-1} = x_1^p[x_1, x_2]...[x_{n-3}, x_{n-2}]x_{n-1}\}$. The Dehn twist associated to this splitting will act as follows: $x_i \mapsto x_i$ for all $1 \leq i \leq n-1$, and $x_n \mapsto x_{n-1}x_n$.

One easily sees this is very similar to the outer automorphism constructed in definition 21.

Note that for $A' =< x_1, ..., x_{n-2}, x_n >$ and θ', we have get another splitting of G as an HNN extension $A'*_{\theta'} = \{x_{1,...,}x_{n-2}, x_n, t | tx_nt^{-1} = x_1^p[x_1, x_2]...[x_{n-3}, x_{n-2}]x_n\}$, and one can see easily check they intersect.

Definition 52. The above definition of a Dehn twist is the same as the automorphism of a graph of groups $(X, \boldsymbol{G})$ given by $H_X = id_X$,$H_v = id_{\boldsymbol{G}_v}$, $H_e = id_{\boldsymbol{G}_e}$ and δ is such that there is an element γ_e in the center $Z(\boldsymbol{G}_e)$ for each edge group such that $\delta(e) = \varphi_e(\gamma_e)$. A collection $(\gamma_e)_{e \in E(X)}$ with each $\gamma_e \in Z(\boldsymbol{G}_e)$ and a base point $v \in V(X)$ defines a Dehn twist.

In other words, take $\gamma_e \in Z(\boldsymbol{G}_e)$ for each $e \in E(X)$ and choose a base point x_0 of X. Then the Dehn twist of (γ_e, x_0) will act on $\pi_1(X, \boldsymbol{G}, T)$ as follows:

$$t_e \to \gamma_e t_e$$
$$g_v \to \gamma_{e_1}...\gamma_{e_n} g_v \gamma_{e_n}^{-1}...\gamma_{e_1}^{-1}$$

for all t_e for which $e \notin T$, and for all $g_v \in \boldsymbol{G}_v$ where $e_1..e_n$ the path in T from x_0 to v.

Remark 53. One gets from the definition above that:

-The action on the group of the base point is trivial.

-Changing base point from x_0 to x_1 will change the Dehn twist by conjugation by $\gamma_{f_1}...\gamma_{f_n}$ for a path $f_1...f_n$ in T between x_0 and x_1.

-The definition is compatible with definition 50. For an amalgamated product, the choice of base point will be the one with the group A.

-Let T' be a subtree of X, we will get that Dehn twists for $(X/T', \boldsymbol{G}(X/T')$ are the same as Dehn twists for $(X, \boldsymbol{G})$ taking $\gamma_t = 1$ for all $t \in T'$.

Later when we look at graphs of groups with cyclic edge groups, the collection (γ_e) will be the edge group generators.

Remark 54. Once again this is all compatible and equal to the Dehn twists coming from simple closed curves.

Given all of this one can ask when do Dehn twists give us non trivial mapping classes, or non trivial outer automorphisms of G.

We finish the subsection with two lemmas about intersections of splittings.

Lemma 55. *Conjugation doesn't change whether two splittings intersect or not*

Proof. See [41] remark 1.9. □

Lemma 56. *If two splittings α, β don't intersect, then their Dehn twists commute*

Proof. Since the the splittings don't intersect they have a common refinement. Then their Dehn twists can be realized on their common refinement, as in definition 52, looking at that definition, we can see that the Dehn twists must commute (see remark 53). □

3.4 Profinite groups and graphs

Definition 57. A topological space T is a profinite space if it is the inverse limit of finite discrete spaces, and so T is profinite if it is compact, Hausdorff and totally disconnected.

Definition 58. Given a discrete group G, one can define its profinite completion $\hat{G}$ to be the limit of G/N over all finite index normal subgroup $N \lhd G$ and pro-p completion to be the limit of G/N over all normal subgroups N with $|G/N| = p^r$ for some integer r.

Remark 59. The above actually gives a functor from the category of discrete groups to that of profinite/pro-p groups. This completion Functor is right exact.

Definition 60. We call a group G residually finite (resp. residually p), if for every element $1 \neq g \in G$, there is a homomorphism $\varphi : G \to H$ to a finite group (resp. p-group), such that $\varphi(g) \neq 1$.

Remark 61. A group is residually finite (resp. residually p) if and only if the natural map to its profinite (resp. pro-p) completion is injective.

Definition 62. A topological graph X is a topological space X, together with a subset of vertices $V(X)$ and two incidence maps $v_0, v_1 : X \to V(X)$ which are the identity on $V(X)$ (these are the maps sending an edge to its terminal and inital vertices). It is called a profinite graph if X is a profinite space, the subset of vertices $V(X)$ is closed (and hence profinite) and the two incidence maps $v_0, v_1 : X \to V(X)$ are continuous.

If $E(X) = X\backslash V(X)$ is closed, it is enough to define v_0 and v_1 continuously on $E(X)$. In general, the set of edges $E(X)$ of a profinite graph X need not be a closed (and therefore compact) subset of X.

Finite abstract graphs are profinite graphs. A morphism of profinite graphs is a morphism of abstract graphs which is also continuous.

Fact 63. *Every profinite graph X can be represented as an inverse limit of finite quotient graphs of X.*

Using the above fact of representing a profinite graph as an inverse limit of finite graphs, one can define the free profinite $\mathbb{F}_p$ on the space, and then similarly to the abstract situation, one can define a chain complex and homology groups of X with coefiecents in $\mathbb{F}_p$.

A profinite graph X is said to be a pro-p tree if X is connected (if and only if $H_0(X, \mathbb{F}_p) = 0$) and $H_1(X, \mathbb{F}_p) = 0$. Thus X is a pro-p tree if and only if $C(X, \mathbb{F}_p)$ is an exact sequence.

Fact 64. *(a) Every connected subgraph of a pro-p tree is a pro-p tree.*

(b) An inverse limit of pro-p trees is a pro-p tree.

(c) Let $X_i, i \in I$, be a family of pro-p subtrees of a pro-p tree T. Then the subgraph $X = \cap_i X_i$ is a pro-p tree (possibly empty).

Let G be a pro-p group and X a profinite graph. Suppose that G acts continuously on the profinite space X from the left.

We say that G acts on the profinite graph X (from the left) if $v_i(gx) = gv_i(x)$ for all $g \in G$,$x \in X$ and $i = 0, 1$.

Define $G_x = \{g \in G : gx = x\}$ to be the stabilizer of an element $x \in X$.

Let $\varphi_X : G \times X \to X$ be the map defined by $\varphi_X(g, x) = gx$ and $pr_G : G \times X \to G$ be the projection.

Then $G_x = pr_G(\varphi_X^{-1}(x) \cap (G \times \{x\}))$, and so G_x is a closed subgroup of G.

If the stabilizer G_x of every element $x \in X$ is trivial, we say that G acts freely on X.

If a pro-p group G acts on a profinite graph R, then the space $G\backslash X = \{Gx : x \in X\}$ of G-orbits with the quotient topology is a profinite space which admits a natural profinite graph structure as follows:

$V(G\backslash X) = G\backslash V(X), v_i(Gx) = Gv_i(x)$ for $i = 0, 1$.

So one has a natural epimorphism $X \to G\backslash X$ of profinite graphs.

If $N \lhd G$, there is an action of G/N on $N\backslash X$ defined in the standard way: $(gN)(Nx) = Ngx$ for $g \in G$, $x \in X$.

Let a pro-p group G act on a profinite graph X and let $N \lhd G$, consider the natural action of G/N on $N\backslash X$ defined above. Then the stabilizers in G/N are epimorphic images of the corresponding stabilizers in G.

Example 65. Let G be a pro-p group and S a closed subset of G containing 1.

Define the Cayley graph $X(G,S)$ as follows: $X(G,S) = G \times S$, $V(X(G,S)) = G \times \{1\}$, $v_0(g,s) = (g,1)$, $v_1(g,s) = (gs,1)$ for all $g \in G$,$s \in S$.

Then $X(G,S)$ is a profinite graph. Define a left action of G on $X(G,S)$ by setting $g' \cdot (g,s) = (g'g,s)$ for all $(g,s) \in G \times S, g' \in G$.

Clearly $gv_i(x) = v_i(g(x))$ for all $g \in G, x \in X(G,S)$ and $i = 0,1$, so G acts freely on the Cayley graph $X(G,S)$.

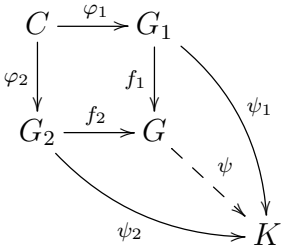
Definition 66. Let A, B and C be pro-p groups and $\varphi_1 : C \to A$, $\varphi_2 : C \to B$, be monomorphisms of pro-p groups.

The amalgamated free pro-p product of A and B with amalgamated subgroup C is a pushout in the category of pro-p groups

$$\begin{array}{ccc} C & \xrightarrow{\varphi_1} & A \\ {\scriptstyle\varphi_2}\downarrow & & \downarrow{\scriptstyle f_1} \\ B & \xrightarrow{f_1} & A *_C B \end{array}$$

In other words, a pro-p group $G = A *_C B$, satisfying the following universal property:

For any pair of homomorphisms $\psi_1 : A \to K$,$\psi_2 : B \to K$ into a pro-p group K with $\psi_1\varphi_1 = \psi_2\varphi_2$, there exists a unique homomorphism $\psi : G \to K$ such that the following diagram is commutative:



It follows from the existence and uniqueness of push outs that an amalgamated free pro-p product exists and it is unique.

Definition 67. Let A be a pro-p group and $\theta : C' \to C$ a continuous isomorphism from a pro-p group to a closed subgroups of A, the pro-p HNN extension of A with

respect to (θ, C), is a pro-p group $G = HNN(A, \theta, C) = A*_\theta$, with an element $t \in G$ and a homomorphism $\varphi : A \to G$, with the following universal property:

For any pro-p group K, any $k \in K$ and any homomorphism $\psi : A \to K$ satisfying $k\psi((c))k^{-1} = \psi(\theta(c))$ for all $c \in C'$, there is a unique homomorphism $\omega : G \to K$ such that the diagram

$$\begin{array}{ccc} G & & \\ {\scriptstyle\varphi}\uparrow & \searrow^{\omega} & \\ H & \xrightarrow{\psi} & K \end{array}$$

is commutative and $\omega(t) = k$.

Remark 68. Note that the above universal properties are the same as the ones for discrete HNN and amalgamated products, but now in the category of pro-p groups.

Also note that it is enough to check the universal property just for finite p-groups K.

Definition 69. We again define a Dehn twist of HNN extensions and amalgamated free products, but now for pro-p/profinite versions:

Given a group and a $\mathbb{Z}_p$ splitting $A *_{<c>} B$, we define the Dehn twist δ to be the automorphism $\delta(a) = a, \delta(b) = \varphi(c)b\varphi(c)^{-1}$ for all $a \in A, b \in B$. This extends to $A *_{<c>} B$ by the universal property

Similarly given an HNN extension $A*_\theta$ where $\theta :< c >\to A$ we define the Dehn twist δ to be $\delta(a) = a$ for all $a \in A$ and $\delta(t) = ct$. Again this extends to $A*_\theta$ by the universal property.

Definition 70. More generally, let $(X, \boldsymbol{G})$ be a finite graph of profinite groups, and let $T \subset X$ be a maximal subtree X.

The profinite fundamental group of the graph of groups $(X, \boldsymbol{G})$ with respect to T, is a profinite group $\pi_1(X, \boldsymbol{G}, T)$, and a map

$$\psi : \coprod_{v \in V(X)} \boldsymbol{G}_v \amalg \coprod_{e \in E(X)} < t_e > \to \pi_1(X, \boldsymbol{G}, T)$$

such that $\varphi(t_e) = 1$ for all $e \in E(T)$ and $\psi(t_e\varphi_e(c)t_e^{-1}) = \psi(\varphi_{\bar{e}}(c))$ for all $e \in E(X)$ and $c \in \boldsymbol{G}_e$, and such that $(\pi_1(X, \boldsymbol{G}, T), \psi)$ are universal with respect to these properties.

The above exists and is independent of the maximal subtree T, and in fact is equal to

$$((\coprod_{v \in V(X)} \boldsymbol{G}_v) \amalg F)/N$$

where F is the free profinite group generated by t_e for all $e \in E(X)$ and N is the smalled closed normal subgroup of $\coprod_{v \in V(X)} \boldsymbol{G}_v) \amalg F$ containing $\{t_e : e \in E(T)\} \cup \{\varphi_{\bar{e}}(c)^{-1} t_e \varphi_e(c) t_e^{-1} : e \in E(X), c \in \boldsymbol{G}_e\}$. This all also works similarly for finite graphs of pro-p groups (see [39] Section 6).

Similarly to classical Bass-Serre theory, we have the following (this can also be found in [39] Section 6):

Theorem 71. *Let $(X, \boldsymbol{G})$ be a finite graph of profinite groups. Then there exists a unique profinite tree $S((X, \boldsymbol{G}))$, called the standard graph of $(X, \boldsymbol{G})$, on which $\pi_1(X, \boldsymbol{G})$ acts, such that the qoutient graph $\pi_1((X, \boldsymbol{G}))\backslash S((X, \boldsymbol{G}))$ is isomorphic to X, and such that the stabiliser of a point $s \in S(X, \boldsymbol{G})$, is a conjugate of $Im(\boldsymbol{G}_{p(s)} \to \pi_1(X, \boldsymbol{G}))$, where $p : S((X, \boldsymbol{G})) \to X$ is the projection map.*

Conversely an action of a profinite group on a profinite tree for which the quotient is a finite graph, gives rise to a decomposition of the profinite group as a finite graph of profinite groups.

Remark 72. Note that one has fundamental groups for graphs of pro-p groups, depends on a universal property, coming from $\boldsymbol{G}(v)$ and t_e. So a similar definition for a Dehn twists of graphs of pro-p groups can be defined (similar to 52). Also note that in general, it is not the case that it is just a pro-p completion of a discrete Dehn twist.

Chapter 4

Main Results

4.1 Background on Poincare duality groups

We now turn our focus to Demuskin groups, which are part of a larger class of pro-p groups, which satisfy a version of Poincare duality.

Definition 73. Let G be an infinite pro-p group.

Then G is a poincare duality group of dimension n if:

- $dim_{\mathbb{F}_p} H^i(G, \mathbb{F}_p) < \infty$ for all $i \leq n$

- $dim_{\mathbb{F}_p} H^n(G, \mathbb{F}_p) = 1$

- for all $0 \leq i \leq n$ the cup product $H^i(G, \mathbb{F}_p) \times H^{n-i}(G, \mathbb{F}_p) \to H^n(G, \mathbb{F}_p)$ is a non-degenerate bilinear form.

These above conditions are equaivalent to a more "standard" poincare duality as follows:

Definition 74. Let G be a profinite group of cohomological dimension n, such that for every G-module A which is a finite group, $H^n(G, A)$ is finite.

Define the dualizing module to be the torsion group G-module I, which represents the functor $A \mapsto H^n(G, A)^*$

We have the following proposition, which can be found in [44]:

Proposition 75. *Let G be an n-dimensional Poincare pro-p group, then it has a dualizing module I, and we have:*

(a) I is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as an abelian group.

(b) The canonical homomorphism $i : H^n(G, I) \to \mathbb{Q}/\mathbb{Z}$ is an isomorphism of $H^n(G, I)$ with $\mathbb{Q}_p/\mathbb{Z}_p$ (as a subgroup of $\mathbb{Q}/\mathbb{Z}$).

(c) For all finite G-modules A and for all integers i, the cup-product

$$H^i(G, A) \times H^{n-i}(G, Hom(A, I)) \to H^n(G, I) = \mathbb{Q}_p/\mathbb{Z}_p$$

gives a duality between the finite groups $H^i(G, A)$ and $H^{n-i}(G, Hom(A, I))$.

Denote by U_p the group of p-adic units. We have that U_p is the automorphism group of I. Since G acts on I, we have that this action is given by a canonical homomorphism

$$\chi : G \to U_p$$

This homomorphism is continuous; it determines I (up to isomorphism), we call χ the orientation character of G. This character is an important invariant of a Poincare duality group.

Example 76. If G is a p-adic analytic group of dimension n, which is compact and torsion-free, then G is a Poincare group of dimension n (see [24]).

Let G be a Poincare pro-p group of dimension $n > 0$.

Every open subgroup of G is also a Poincare duality group of dimension n.

Let H be a proper closed subgroup of G, then $Res : H^n(G, \mathbb{F}_p) \to H^n(H, \mathbb{F}_p)$ is 0.

If we also have that $[G : H] = \infty$ (i.e. that H is not open), then we get that the cohomological dimension of H is $\leq n$. In particular, every closed subgroup of infinite index of a Demuskin group is a free pro-p-group.

Let G be a Demuskin group and let H be an open subgroup of G. One has:

$$rank(H) - 2 = [G : H](rank(G) - 2).$$

4.2 Demuskin groups

We now turn to Poincare duality groups of dimension 2, which are also known as Demuskin groups.

Such groups, are in fact one relator groups, which are actually fully determined by two invariants associated to a Demuskin group: the minimal number of (topological) generators, and an extra invariant, which depends on the orientation character, which is either ∞ or a power of the prime p. To be more precise, this invariant is the higest power p^r, such that the induced map $\chi : G \to Aut(\mathbb{Z}_p/p^r\mathbb{Z}_p)$ is trivial.

Theorem 77. *([5]) Let G be a Demushkin group with d' generators and orientation character which vanishes mod p^r but not mod p^{r+1}, and suppose that $p \neq 2$.*

Then d' is even, $d' = 2d$, and G is isomorphic to F/R, where F is a free pro-p group with basis $x_1, y_1, ..., x_d, y_d$ and R is generated as a normal closed subgroup by $x_1^{p^r}[x_1, y_1]...[x_d, y_d]$.

For $r = \infty$ (i.e. trivial orientation character), we replace x_1^∞ by the identity (and so the relation is just the usual surface group relation $[x_1, y_1]...[x_d, y_d] = 1$).

Furthermore all groups having such presentations are Demushkin.

In the case when G is a Demushkin group with $p = 2$, the classification was completed by Serre [42] and Labute [23].

Our interest in Demuskin groups comes from two reasons, for discrete groups, the only Poincare duality groups of dimension 2 are surface groups.

The other and more important reason is the following classification of the maximal pro-p quotient of the absolute Galois group of a p-adic field (or the Galois group of the maximal p-extension);

Theorem 78. *Let K be a p-adic field, of degree N over $\mathbb{Q}_p$, and suppose $p \neq 2$:*

1) If $\mu_p \nsubseteq K$, then $G_K(p)$ is a free pro-p group of rank $N + 1$

2)If $\mu_p \subseteq K$, let r be the maximal power such that $\mu_{p^r} \subseteq K$ (i.e. $\mu_{p^{r+1}} \nsubseteq K$), then $G_K(p)$ is a Demuskin group on $N + 2$ generators and invariant p^r (note that N must be even since $\mu_p \subseteq K$), and dualizing module, the group of all roots of unity in the maximal p-extension of K.

In other words, $G_K(p)$ is the pro-p group on the generators $x_1, y_1, ..., x_{\frac{N}{2}+1}, y_{\frac{N}{2}+1}$ and relation $x_1^{p^r}[x_1, y_1]...[x_{\frac{N}{2}+1}, y_{\frac{N}{2}+1}]$.

For the rest of the chapter we will, assume that $p \neq 2$, and denote by G a Demushkin group, and by $\mathcal{G}_{r'}$ for $r' \geq r$ to be the discrete groups with $2d$ generators and 1 relation $x_1^q[x_1, y_1]...[x_d, y_d]y_d^{-p^{r'}}$. When $r' = \infty$ we simply denote it by $\mathcal{G}$.

4.2.1 Splittings of discrete Demuskin groups

Definition 79. Define $Split_D(\mathcal{G}_{r'}, \mathbb{Z})$ to be the union $Split_{D,amalg}(\mathcal{G}_{r'}, \mathbb{Z})$, the set of splittings of $\mathcal{G}_{r'}$ into $F_{2n} *_{<c>} F_{d-2n}$ where c maps to $x_1^q[x_1, y_1]...[x_n, y_n]$ in F_{2n} and to $y_d^{p^{r'}}[y_d, x_d]..[y_{n+1}, x_{n+1}]$ in F_{d-2n} for some basis x_i, y_i, and $Split_{D,HNN}(\mathcal{G}_{r'}, \mathbb{Z})$, the set of splittings into $A*_\theta$ where A be the free group on $n-1$ generators $x_1, ..., x_{d-1}, y_{d-1}, y_d$, and let θ be the map sending y_d to $y_d^{-p^{r'}}x_1^{p^r}[x_1, y_1]...[x_{d-1}, y_{d-1}]y_d$.

We denote by $Aut_D(\mathcal{G}_{r'})$ the subgroup of $Aut(\mathcal{G}_{r'})$ generated by Dehn twists T_α, for $\alpha \in Split_D(\mathcal{G}_{r'}, \mathbb{Z})$, the image of $Aut_D(\mathcal{G}_{r'})$ in $Out(\mathcal{G}_{r'})$ will be denoted by $Out_D(\mathcal{G}_{r'})$.

Remark 80. We restrict ourselves to such splittings, since we do not know how to classify all splittings of the discrete group, and in a sense we don't need to for our applications.

For Demushkin groups, these are the only splittings, by [50] theorem 5.18 together with [51] theorem 3.3, and so when we will look at Dehn twists of the pro-p case, the only restriction we have is that the edge stabilizers are cyclic.

Theorem 81. *Fix a basis $x_1, y_1..., x_d, y_d$, let α be the splitting of $\mathcal{G}$ into $A*_\theta$ where A be the free group on $d-1$ generators $x_1, y_1..., x_d$, and let θ be the map sending x_d to $x_1^p[x_1, y_1]...[x_{d-1}, y_{d-1}]x_d$ then T_α^k is non trivial in $Out(\mathcal{G})$.*

Proof. Let β be the splitting $B =< x_1, y_1...x_{d-1}, y_{d-1}, y_d >$ and θ' we have $B*_{\theta'} = \{x_1, y_1...x_{d-1}, y_{d-1}, y_d, t | t x_n t^{-1} = x_1^p[x_1, y_1]...[x_{d-1}, y_{d-1}]y_d\}$.

Looking at the translation length of the action of x_d on the tree of β we see that it is positive, since x_d is not conjugate to any element of B, hence the splittings α and β intersect.

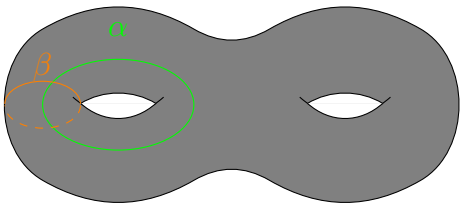
Again we have that the translation length of the action of $T_\alpha^k(y_d)$ on the tree of β is positive, since $y_d x_d^k$ is not conjugate to any element of B and so the splittings $T_\alpha^k(\beta)$ and β intersect.

Now assume that T_α^k was inner, i.e. acted by conjugation.

Since conjugation does not change whether two splittings intersect or not (lemma 55), and any splitting does not intersect itself, we get a contradiction.

Hence T_α^k is outer. □

Remark 82. In the above, when $r = \infty$ we get the following picture for α and β:



Theorem 83. *Let α be the splitting of $\mathcal{G}_{r'}$ into $F_{2n} *_{<c>} F_{2d-2n}$ where c maps to $x_1^q[x_1, y_1]...[x_n, y_n]$ in F_{2n} and to $y_d^{p^{r'}}[y_d, x_d]..[y_{n+1}, x_{n+1}]$ in F_{2d-2n} then T_α^k is non trivial in $Out(\mathcal{G}_{r'})$.*

Proof. Similarly to theorem 35:

Let β be the splitting $B =< x_1, y_1, ..., x_n, y_{n+1}, x_{n+2}, y_{n+2}, .., x_d, y_d, b >$ where $b = y_n^{-1}x_{n+1}$ with gluing map

$$\theta'(b^{-1}x_n^{-1}by_{n+1}) = x_n^{-1}[y_{n-1}, x_{n-1}]...[y_1, x_1]x_1^q y_d^{p^{r'}}[y_d, x_d]...[y_{n+2}, x_{n+2}]y_{n+1}$$

and so we have

$$B*_{\theta'} = \{B, t | \begin{array}{c} tb^{-1}x_n^{-1}by_{n+1}t^{-1} = \\ x_n^{-1}[y_{n-1}, x_{n-1}]...[y_1, x_1]x_1^q y_d^{p^{r'}}[y_d, x_d]...[y_{n+2}, x_{n+2}]y_{n+1} \end{array} \}$$

where t would be x_{n+1} in $\mathcal{G}_{r'}$.

Looking at the translation length of the action of $x_{n+1}^{-1}y_n x_n^{-1}y_n^{-1}x_{n+1}y_{n+1}$ on the tree of α we see that it is positive, since it is not conjugate to any element of $< x_1, ..., y_n >$ or of $< x_{n+1}, ..., y_d >$ (due to x_n and y_{n+1} both having sum of powers non zero), hence the splittings α and β intersect.

Again we have that the translation length of the action of $T_\alpha^k(b^{-1}x_n^{-1}by_{n+1})$ on the tree of β is positive, since $x_{n+1}^{-1}\gamma^k y_n x_n^{-1}y_n^{-1}\gamma^{-k}x_{n+1}y_{n+1}$ is not conjugate to any element of B, where $\gamma = x_1^q[x_1, y_1]...[x_n, y_n]$ (due to the appearances of y_n "away from x_{n+1}" in the middle of the word, coming from γ).

For example when $k = 1$ we have:

$$x_{n+1}^{-1}x_1^q[x_1, y_1]..[x_{n-1}, y_{n-1}][x_n, y_n]x_n^{-1}[y_{n-1}, x_{n-1}]...[y_1, x_1]x_1^{-q}x_{n+1}y_{n+1}$$

which is clearly not conjugate to elements of B, and so the splittings $T_\alpha^k(\beta)$ and β intersect.

Note that one can also see that $T_\alpha^k(\beta)$ and β intersect since if they wouldn't then we would get that $T_{T_\alpha^k(\beta)}$ and T_β commute (by lemma 56).

But by lemma 96 we have $T_{T_\alpha^k(\beta)} = T_\alpha^k T_\beta T_\alpha^{-k}$, and a direct computation (say using Dehn's algorithm for the word problem) would show that $T_\alpha^k T_\beta T_\alpha^{-k} T_\beta(x_{n+1}) \neq T_\beta T_\alpha^k T_\beta T_\alpha^{-k}(x_{n+1})$.

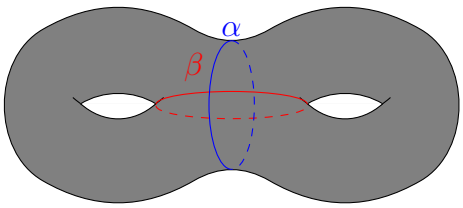
Now assume that T_α^k was inner, i.e. acted by conjugation.

Since conjugation does not change whether two splittings intersect or not (lemma 55), and any splitting does not intersect itself, we get a contradiction.

Hence T_α^k is outer. □

Remark 84. Note that for having amalgamated free products we need $d > 1$, similar to how we need the genus of a surface to be great than 1 to have separating curves.

Remark 85. In the above, when $r = \infty$ we get something almost like the following picture for α and β (only almost like it, since β got some extra "twisting" in its presentation to make it easier to work with):



4.3 Pro-p rigidity for Demuskin type relations

4.3.1 p-efficient splittings

We now describe a property which will allow us to move from showing properties of a discrete group $\mathcal{G}$ to a Demuskin group G.

Definition 86. A graph of discrete groups $\mathscr{G} = (X, F)$ is p-efficient if $\pi_1(\mathscr{G})$ is residually p, each group F_x is closed in the pro-p topology on $\pi_1(\mathscr{G})$, and $\pi_1(\mathscr{G})$ induces the full pro-p topology on each F_x.

Remark 87. Let (X, F) be a graph of discrete groups, e.g. if X is one edge this is either $F_1 *_L F_2$ or $F_1 *_L$. If it is p-efficient, then we would get that $(X, \hat{F})$ is an injective graph (i.e. the vertex groups inject to the fundamental group) of pro-p groups and the pro-p completion of $\pi_1(X, F)$ is $\pi_1(X, \hat{F})$, where by $\hat{}$ we mean pro-p completions, and the second π_1 is the fundamental group in the category of graphs of pro-p groups.

In the case of one edge graphs this would mean $\widehat{F_1 *_L F_2} \cong \hat{F}_1 *_{\hat{L}} \hat{F}_2$ and $\widehat{F_1 *_L} \cong \hat{F}_1 *_{\hat{L}}$, where the amalgamated free product/HNN extension, on the left side of each isomorphism, is in the category of discrete groups, and the right side is in the category of pro-p groups.

In other words, if a graph of groups is p-efficient then taking fundamental groups commutes taking pro-p completions, and the discrete fundamental group injects into the pro-p one.

Proposition 88. *Every group $\mathcal{G}_{r'}$ is residually p.*

Proof. by [10]. □

Proposition 89. *Let $\alpha \in Split_D(\mathcal{G}_{r'}, \mathbb{Z})$. Then for any s, there is a p-group quotient of $\mathcal{G}$ such that the image of c, a generator of $\mathcal{G}_e$, is p^s torsion. In particular, $\mathcal{G}$ induces the full pro p topology on $\mathcal{G}_e$.*

Proof. If α is an HNN extension, then c is a non trivial primitive element in $\mathcal{G}^{ab}$ and so any map $\mathcal{G} \twoheadrightarrow \mathbb{Z}/p^s$, sending c to 1 will do.

Otherwise, we have a basis for which $\alpha = F_{2n} *_{<c>} F_{2d-2n}$ where c maps to $x_1^q[x_1, y_1]...[x_n, y_n]$ in F_{2n} and to $[x_{n+1}, y_{n+1}]...[x_d, y_d]y_d^{-p^{r'}}$ in F_{2d-2n}.

If $r', r \geq s$, we define maps from F_{2n}, F_{2d-2n} to the Heisenberg group with coefficient in $\mathbb{Z}/p^s$

$$\mathcal{H}(\mathbb{Z}/p^r) = \{\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z}/p^s\}$$

sending x_{n+1}, x_1 to $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, y_{n+1}, y_1 to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ and the rest of x_i, y_i to the identity. Thus we have the image of c will be which is of order exactly p^s. The map $\mathcal{G} \to \mathcal{H}(\mathbb{Z}/p^s) *_{\mathbb{Z}/p^s} \mathcal{H}(\mathbb{Z}/p^s) \to \mathcal{H}(\mathbb{Z}/p^s)$ where the final map identifies the two copies of $\mathcal{H}(\mathbb{Z}/p^s)$ is the required quotient.

If $r < s \leq r'$, then we send F_{2n} to $\mathbb{Z}/p^{r+s}$, sending all generators to the identity, hence c to an element of order p^s, and we send F_{2d-2n} to $\mathcal{H}(\mathbb{Z}/p^{r+s})$, but now send x_{n+1} to $\begin{pmatrix} 1 & p^r & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

The image of the map $\mathcal{G} \to \mathcal{H}(\mathbb{Z}/p^{r+s}) *_{\mathbb{Z}/p^{r+s}} \mathbb{Z}/p^{r+s} = \mathcal{H}(\mathbb{Z}/p^{r+s})$ is the required quotient.

If $r' < s$ then we send F_{2n} and F_{2d-2n} to $\mathbb{Z}/p^{r'+s}$, sending all generators to the identity, except x_1 which is sent to $p^{r'-r}$ hence c to an element of order p^s, which gives us the required quotient of $\mathcal{G}$. □

Definition 90. Let P be a finite p-group. A chief series for P is a sequence $1 \leq P_n \leq P_{n-1} \leq ... \leq P_2 \leq P_1 = P$ of normal subgroups of P such that each quotient P_i/P_{i+1} is either trivial or isomorphic to Z/pZ.

We first need the following theorem of Higman [13]:

Theorem 91. *Let A and B be finite p-groups with common subgroup $A \cap B = U$. Then $A *_U B$ is residually p if and only if there are chief series $\{A_i\}$ and $\{B_i\}$ of A and B respectively such that $\{U \cap A_i\} = \{U \cap B_i\}$. In particular, $A *_U B$ is residually p when U is cyclic.*

Proposition 92. *A splitting in $Split_{D,amalg}(\mathcal{G}_{r'}, \mathbb{Z})$, $\mathcal{G}_{r'} = G_1 *_L G_2$ is a p-efficient splitting.*

Proof. Let $H \lhd_p G_1$ and $P_1 = G_1/H$, and suppose $LH/H \cong Z/p^rZ$. By Proposition 89 there is a p-group quotient $G_2 \to P_2$ such that the image of L is also isomorphic to Z/p^rZ. The quotient $P_1 *_{Z/p^rZ} P_2$ obtained is residually p (by theorem 91), so it has a p-group quotient Q distinguishing all the elements of P_1.

The kernel of the composite map $G_1 \to \mathcal{G} \to P_1 *_{Z/p^rZ} P_2 \to Q$ is H, so $\mathcal{G}$ induces the full pro-p topology on G_1, and similarly for G_2.

Given $g \in \mathcal{G}\backslash G_1$, we can write $g = a_1b_2 \cdots a_nb_n$ where $a_i \in G_1$, $b_i \in G_2$ and all are not in L, except possibly $b_n = 1$ or $a_1 \in L$.

Next, we have $H_i \lhd_p G_i$ such that the images of every a_j (resp. b_j) in $P_1 = G_1/H_1$ is (resp. $P_2 = G_2/H_2$) not in the image of L.

By proposition 89 we can actually take H_i to be such that the image of L is Z/p^rZ in both P_i.

By construction the image $\phi(g)$ is not in P_1, where $\phi : \mathcal{G} \to P_1 *_{Z/p^r} P_2$ the quotient map.

Since $P_1 *_{Z/p^r} P_2$ is residually p (by theorem 91), we can find a p-group quotient Q of $P_1 *_{Z/p^r} P_2$ distinguishing $\phi(g)$ from P_1.

The map $\mathcal{G} \to Q$ distinguishes g from G_1 and so G_1 is p-separable in $\mathcal{G}$, and similarly for G_2. □

We now need the following theorem of Chatzidakis [2]:

Theorem 93. *Let P be a finite p-group, let A and B be subgroups of P, and let $f : A \to B$ be an isomorphism.*

Suppose that P has a chief series $\{P_i\}$ such that $f(A \cap P_i) = B \cap P_i$ for all i and the induced map $f_i : AP_i \cap P_{i-1}/P_i \to BP_i \cap P_{i-1}/P_i$ is the identity for all i.

Then P embeds in a finite p-group T in which f is induced by conjugation. Hence the HNN extension $P*_f$ is residually p.

Proposition 94. *A splitting in $Split_{D,HNN}(\mathcal{G}_{r'}, \mathbb{Z})$, $\mathcal{G}_{r'} = H*_\theta$, for $\theta : A \to B$ the isomorphism of cyclic groups, is a p-efficient splitting.*

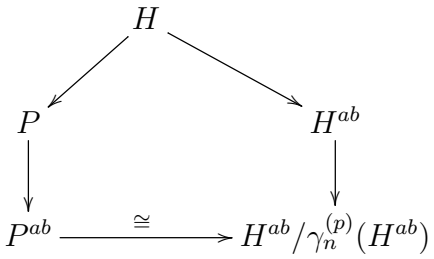
Proof. Let $x_1, ..., x_{d-1}, y_{d-1}, y_d$, be generators of $\mathcal{G}_{r'}$ such that $A = y_d$ and $B = y_d^{-p^{r'}} x_1^{p^r} [x_1, y_1]...[x_{d-1}, y_{d-1}]y_d$.

First we will prove that $\mathcal{G}_{r'}$ induces the full pro-p topology on H.

Let $P = H/\gamma_n^{(p)}(H)$ be one of the lower central p-quotients of H, and let $\phi : H \to P$ be the quotient map.

Let a and b denote generators of $\phi(A)$ and $\phi(B)$ respectively, and

Since commutator subgroups and terms of the lower central p-series are verbal subgroups, there is a commuting diagram:



and so $P^{ab} = H^{ab} \otimes Z/p^{n-1}Z$.

The image of a in P thus has order at least p^{n-1}, also by definition of the lower central series any element of P has order at most p^{n-1}.

Hence the image of A in P injects into P^{ab}.

Since P is a characteristic quotient of H and there is an automorphism of H taking a to b, the order of b will also be p^{n-1}.

Furthermore, if we denote by $\bar{a}, \bar{b}$ the image of a and b in $P^{ab}/ < \psi(x_1) >$, where ψ is the map from H to P^{ab}. We have $\bar{a}^{-p^{r'}}\bar{a} = \bar{b}$.

Now construct a chief series $\{P_i\}$ for P whose first n terms are the preimages of the terms of a chief series for $P^{ab}/ < \psi(x_1) >$ which intersects to a chief series on the subgroup of $P^{ab}/ < \psi(x_1) >$ generated by the image of a.

Then for $i \geq n$, we have $\phi(A) \cap P_i = \phi(B) \cap P_i = 1$ and for $i < n$ the conditions of theorem 93 hold by construction.

Hence $P*_{\phi(A)}$ is residually p, and we may take a p-group quotient $P*_{\phi(A)} \to Q$ in which no element of P is killed.

The kernel of the composite map $H \to G \to P*_{\phi(A)} \to Q$ is $\gamma_n^{(p)}(H)$ as required.

To show that H is p-separable in G, proceed as in the proof of proposition 92: write $g \in G \backslash H$ as a reduced word in the sense of HNN extensions, and take a sufficiently deep lower central p-quotient $P = H/\gamma_n^{(p)}(H)$ so that the image of g in $P*_{\phi(A)}$ is again a reduced word not in P.

As shown above, $P*_{\phi(A)}$ is residually p, so admits a p-group quotient Q distinguishing the image of g from the image of P.

This quotient Q of G exhibits that H is p-separable in G. □

We get from the above:

Corollary 95. *Every $\mathbb{Z}$ splitting of $\mathcal{G}_{r'}$ in $Split_D(\mathcal{G}_{r'}, \mathbb{Z})$ is p-efficient .*

Lemma 96. *Let α be a splitting of G, and let $\phi \in Aut(G)$ then: $T^k_{\phi(\alpha)} = \phi T^k_\alpha \phi^{-1}$.*

Proof. Let α be a splitting of G into an amalgamated free product $G_1 *_H G_2$, from the universal property of amalgamated free products, (see definition 66) we get that it is enough to show $T^k_{\phi(\alpha)} = \phi T^k_\alpha \phi^{-1}$ on the two subgroups $\phi(G_1), \phi(G_2)$.

Since Dehn twists act trivially on the first factor, then we get $T^k_{\phi(\alpha)} = \phi T^k_\alpha \phi^{-1}$ on $\phi(G_1)$.

On $\phi(G_2)$, $T^k_{\phi(\alpha)}$ acts by conjugation by $(\phi(h))^k$ where h is the fixed generator of H.

Let $\phi(g) \in \phi(G_2)$, then $\phi T^k_\alpha \phi^{-1}(\phi(g)) = \phi(T^k_\alpha(g)) = \phi(h^{-k}gh^k) = (\phi(h))^{-k}\phi(g)(\phi(h))^k$, hence again the action is by conjugation by $(\phi(h))^k$.

From this we get $T^k_{\phi(\alpha)} = \phi T^k_\alpha \phi^{-1}$ for α an amalgamated free product.

The case of α an HNN extension is very similar, using the universal property of HNN extensions (see definition 67).

□

Corollary 97. *If $\alpha, \beta \in Split(G, \mathbb{Z}_p)$ are in the same $Aut(G)$ orbit, then T^k_α is inner if and only if T^k_β is inner.*

Proof. Let $\phi \in Aut(G)$ be the automorphism for which $\phi(\alpha) = \beta$ and assume T^k_α is the automorphism given by conjugation by $g \in G$.

Let $x \in G$, then $T^k_\beta(x) = T^k_{\phi(\alpha)}(x) = \phi T^k_\alpha \phi^{-1}(x) = \phi(g^{-1}\phi^{-1}(x)g) = \phi(g^{-1})\phi(\phi^{-1}(x))\phi(g) = \phi(g^{-1})x\phi(g)$, and so we get T^k_β is inner, given by conjugation by $\phi(g)$.

The other direction follows in a similar manner. □

4.3.2 Complexes of cyclic splittings

We now show that actually any splitting of G "comes from" a splitting of $\mathcal{G}_{r'}$ for some $r' \geq r$.

Definition 98. For splittings x and y we say $x \leq y$ if x is a refinement of y.

Theorem 99. *For every $r' \geq r$ we have a $Aut(\mathcal{G}_{r'})$ -equivariant map $j : Split_D(\mathcal{G}_{r'}, \mathbb{Z}) \to Split(G, \mathbb{Z}_p)$ with the further properties that $x \leq y$ if and only if $j(x) \leq j(y)$ and if $z \in Split(G, \mathbb{Z}_p)$ has $z \leq j(y)$ then $z = j(x)$ for some $x \leq y$.*

Proof. Construction of i:

Take $\alpha \in Split_D(\mathcal{G}_{r'}, \mathbb{Z})$ for some r', it is is p-efficient by corollary 95.

Therefore by [39] propositions 6.5.3 and 6.5.4 there is an induced splitting of G as an injective graph of pro-p groups with procyclic edge groups.

The standard tree dual to this splitting (see [39] theorem 6.5.2) is a representative of an element $j(\alpha)$ of $Split(G, \mathbb{Z}_p)$.

Note that the Bass-Serre tree of the splitting α of $\mathcal{G}_{r'}$ is naturally embedded as an abstract subgraph of the Bass-Serre tree of $j(\alpha)$ which is dense in the topology on it, by again [39] propositions 6.5.4.

We have $x \leq y$ if and only if $j(x) \leq j(y)$, due to the fact that $x \leq y$ if only if the graph of groups decomposition of $\mathcal{G}_{r'}$ corresponding to x is obtained from the decomposition corresponding to y by collapsing some sub-graphs-of-groups; the same collapsed subgraph can be found in $j(x) \leq j(y)$.

If $z \leq j(y)$ the graphs of groups of z is obtained from $j(y)$ by collapsing some sub-graphs-of-groups; doing such collapses on the graph of discrete groups corresponding to y, we get the required x. □

Remark 100. The property on refinements gives us that the map is actually a map between the complexes $\mathcal{C}_D(\mathcal{G}_{r'})$ and $\mathcal{C}(G)$.

We now want:

Theorem 101. *The map*

$$j : \amalg_{r' \geq r} Split_{D,amalg}(\mathcal{G}_{r'}, \mathbb{Z})/Aut(\mathcal{G}) \amalg Split_{D,HNN}(\mathcal{G}, \mathbb{Z})/Aut(\mathcal{G}) \to Split(G, \mathbb{Z}_p)/Aut(G)$$

is a bijection which has 1 *orbit for HNN-extension, and exactly 1 orbit for each pair of integers* $r' \geq r$ *and* $1 \leq n \leq d$.

Proof. Let α be either the HNN extension from theorem 81 or 83 for some integer n between 1 and d.

We will show that any $\beta \in Split(G, \mathbb{Z}_p)$ has some $\psi \in Aut(G)$ such that $\psi(\beta) = j(\alpha)$.

Take such $\beta \in Split(G, \mathbb{Z}_p)$.

Suppose first that β is an amalgamated pro-p product $G_1 *_L G_2$.

From the classification of PD^2 pairs in [51] Theorem 3.3, and theorem 5.18 in [50], we have that there is some basis, such that G_1 is free of rank $2n$ and G_2 is free of rank $2d - 2n$, and for which the image of L in G_1 is $x_1^{p^s}[x_1, y_1]...[x_n, y_n]$ and in G_2 is $y_d^{p^{s'}}[y_d, x_d]...[y_{n+1}, x_{n+1}]$, for some s and s'.

Since the dualizing module of the pairs , is the restriction of G, we have $s, s' \geq r$.

On the other hand, if both $s, s' > r$ we would have that mod p^r both maps are trivial, and so from the universal property of amalgamated products, we would get that so is χ_G, in contradiction to the definition of r.

Thus either $s' = r$ or $s = r$. Suppose $s = r$.

Take $\alpha \in Split_{D,amalg}(\mathcal{G}_{r'}, \mathbb{Z})$ to be $\mathcal{G}_{r'} = F_{2n} *_{L'} F_{2d-2n}$ for $r' = s'$ and for $2n = rk(G_1)$ and $L' =< c >$ is cyclic and we map c to $x_1^q[x_1, y_1]...[x_n, y_n]$ in F_{2n} and to $y_d^{p^{r'}}[y_d, x_d]..[y_{n+1}, x_{n+1}]$ in F_{d-2n} for some basis x_i, y_i.

Looking at $j(\alpha)$ we get isomorphisms from (G_1, L) to $j((F_{2n}, L'))$ and (G_2, L) to $j((F_{2d-2n}, L'))$ as pairs of groups (see [50]) , which glue together to an automorphism of G sending $j(\alpha)$ to β.

Given another splitting β' of $G = G_1' *_{L''} G_2'$ for which there is $\varphi \in Aut(G)$ for which $\varphi(\beta') = \beta$, we must have (after possibly changing between G_1' and G_2') that G_1' is free of rank $2n$ and G_2' is free of rank $2d - 2n$, and for which the image of L in G_1 is $x_1^{p^s}[x_1, y_1]...[x_n, y_n]$ and in G_2 is $y_d^{p^{s'}}[y_d, x_d]...[y_{n+1}, x_{n+1}]$, for the same s and s' of G_1, G_2 .

For the case of β is an HNN extension G_1*_L, one needs to be a bit more careful in finding two isomorphisms to F_{2d-1} such that they will glue properly to an automorphism of G.

Such gluing works, the proof for which is the same as the end of part (3) of theorem 4.6 of [51]. □

Remark 102. The above theorem, gives us that every splitting comes from some known list of splittings, this is similar to the case of pro-p completions of surface groups as seen in [51].

Due to the $\mathcal{G}_{r'}$ having isomorphic pro-p completions, but probably they are not isomorphic as discrete groups, we need to take them all. On the other hand, since we want a bijection, and HNN extensions all have only a single orbit, we need to take HNN extensions only from one $\mathcal{G}_{r'}$, we choose $r' = \infty$ for convenience.

We now need two final lemma about splittings of G:

Lemma 103. *Let $\alpha \in Split_{D,amalg}(\mathcal{G}_{r'}, \mathbb{Z})$, and β a splitting having non trivial intersection with α. Let c be the generator of the edge of β, then there is a homomorphism $\varphi : G \to P$ such that P is a finite p-group, and $\varphi(c)$ is not conjugate to $\varphi(T_\alpha^k(c))$.*

Proof. The lemma is the same as proposition 4.5 in [35] (there it was proven for surfaces), where $g = c$, $h = \varphi(T_\alpha^k(c))$ and the splitting is α.

Since we are looking to separate an element from its images under the Dehn twist of α, we see that we are exactly in case 3 of the proof of proposition 4.5 in [35], and for such a case, the exact same proof follows for our groups $\mathcal{G}_{r'}$. □

Lemma 104. *Let $\alpha \in Split_{D,HNN}(\mathcal{G},\mathbb{Z})$, then there is a splitting β having non trivial intersection with α, such that there is a homomorphism $\varphi : G \to P$ such that P is a finite p-group, and $\varphi(c)$ is not conjugate to $\varphi(T_\alpha^k(c))$, where c is the generator of the edge of β.*

Proof. After change of coordinates, we can assume α is the splitting of $\mathcal{G}$ into $A*_\theta$ where A be the free group on $d-1$ generators $x_1, y_1 ..., x_d$, and let θ be the map sending x_d to $x_1^p[x_1,y_1]...[x_{d-1},y_{d-1}]x_d$.

Let β be the splitting $B =< x_1, y_1, .., x_{d-1}, y_d, b >$ where $b = y_{d-1}^{-1}x_d$ and $\theta'(b^{-1}x_{d-1}^{-1}by_d) = x_{d-1}^{-1}[y_{d-2}, x_{n-2}]...[y_1,x_1]x_1^q y_d$ is the gluing map we have:

$$B*_{\theta'} = \{B, t| \begin{array}{c} tb^{-1}x_{d-1}^{-1}by_d t^{-1} = \\ x_{d-1}^{-1}[y_{d-2}, x_{n-2}]...[y_1,x_1]x_1^q y_d \end{array} \}$$

where t would be x_d in $\mathcal{G}$.

Note that for the same reason as in theorem 81 we would get $T_\alpha^k(\beta) \neq \beta$.

Let $c = x_d^{-1}y_{d-1}x_{d-1}^{-1}y_{d-1}^{-1}x_d y_d$.

Then the statement of our lemma is the same as proposition 4.5 in [35] (there it was proven for surfaces), for $g = c$, $h = \varphi(T_\alpha^k(c))$ and the splitting is $F_{2d-2}*_{x_1^q[x_1,y_1]...[x_{d-1},y_{d-1}]=[y_d,x_d]} F_2 = \gamma$.

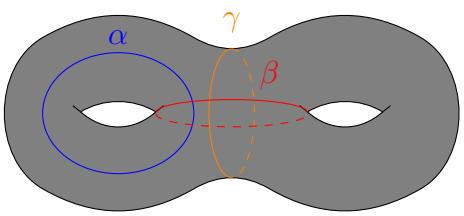
Writing c under the splitting $F_{2d-2} *_{x_1^q[x_1,y_1]...[x_{d-1},y_{d-1}]=[y_d,x_d]} F_2$, we get

$$c = (x_d^{-1})(y_{d-1}x_{d-1}^{-1}y_{d-1}^{-1})(x_d y_d)$$

and $\varphi(T_\alpha^k(c)) = (x_d^{-1})(y_{d-1}x_{d-1}^{-1}y_{d-1}^{-1})(x_d x_d^k y_d)$.

We see that we are either in case 2 of proposition 4.5 in [35], and since on F_2 the edge is $\gamma = [y_d, x_d]$ we have lemma 4.8, and so the same rest of the proof works, or in case 3 of the proof of proposition 4.5 in [35], and again for such a case, the exact same proof follows for our group $\mathcal{G}$.

Note that the above almost corresponds to the following picture (again only almost since β got put in a presentation which is easier to work with):



□

Lemma 105. *The action of $Out_D(\mathcal{G}_{r'})$ on $Split(G,\mathbb{Z}_p)$ is faithful.*

Proof. First, by the proof of theorem 83 and lemma 104, we get that T_α^k has a splitting $\beta \in Split(\mathcal{G}, \mathbb{Z})$ such that $T_\alpha^k(\beta) \neq \beta$. We would like to show that for that β we also have $T_\alpha^k(j(\beta)) \neq j(\beta)$.

Due to j being $Aut(\mathcal{G})$ equivariant, we get that we want to show $j(T_\alpha^k(\beta)) \neq j(\beta)$.

Let c be the generator of the edge of β, we would like to show that c and $T_\alpha^k(c)$ are not conjugate in G.

We already know from $T_\alpha^k(\beta) \neq \beta$ that they are not conjugate in $\mathcal{G}$.

By lemma 103 or 104 we get that $T_\alpha^k(c)$ and c are not conjugate in G and we are done. □

Theorem 99 and lemma 105 gives us:

Corollary 106. *The natural map $\phi : Out_{Dehn}(\mathcal{G}) \to Out(G)$ is an injection.*

Since all splittings are p-efficient, we get:

Corollary 107. *We have that $\phi(T_x^k) = T_{j(x)}^k$, and so if T_x^k is outer, then so is $T_{j(x)}^k$.*

Corollary 108. *Given $\alpha \in Split(G, \mathbb{Z})$, one has that $T_\alpha^k \neq 0$ in $Out(G)$, for any $k \neq 0$.*

Proof. Let $\alpha \in Split(G, \mathbb{Z}_p)$, by theorem 101 we have $\phi \in Aut(G)$ such that $\phi(\alpha) = j(x)$ for some $x \in Split_D(\mathcal{G}_{r'}, \mathbb{Z})$ for some r'.

By theorems 81 and 83, T_x^k is outer, and so by lemma 107, so is $T_{j(x)}^k$.

By corollary 97 we get that T_α^k is outer, as required. □

Bibliography

[1] Mladen Bestvina, Ken Bromberg, and Koji Fujiwara. Constructing group actions on quasi-trees and applications to mapping class groups. *Publications mathématiques de l'IHÉS*, 122(1):1–64, 2015.

[2] Zoé Maria Chatzidakis. Some remarks on profinite hnn extensions. *Israel Journal of Mathematics*, 85(1):11–18, 1994.

[3] Matt Clay and Alexandra Pettet. Twisting out fully irreducible automorphisms. *Geometric and Functional Analysis*, 20(3):657–689, 2010.

[4] M Dehn. "papers on group theory and topology"(trans. by j. stillwell), 1987.

[5] SP Demushkin. The group of a maximal p-extension of a local field. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 25(3):329–346, 1961.

[6] Volker Diekert. Über die absolute galoisgruppe dyadischer zahlkörper. *Journal für die reine und angewandte Mathematik*, 350:152–172, 1984.

[7] Marcus Du Sautoy, Dan Segal, and Aner Shalev. *New horizons in pro-p groups*, volume 184. Springer Science & Business Media, 2012.

[8] Benson Farb and Dan Margalit. *A primer on mapping class groups (pms-49)*. Princeton university press, 2011.

[9] Albert Fathi, François Laudenbach, and Valentin Poénaru. *Thurston's Work on Surfaces (MN-48)*, volume 48. Princeton University Press, 2012.

[10] D Gildenhuys. One-relator groups that are residually of prime power order. *Journal of the Australian Mathematical Society*, 19(4):385–409, 1975.

[11] Alexandre Grothendieck. Esquisse d'un programme. *London Mathematical Society Lecture Note Series*, pages 5–48, 1997.

[12] Vincent Guirardel. Core and intersection number for group actions on trees. *arXiv preprint math/0407206*, 2004.

[13] Graham Higman. Amalgams of p-groups. *Journal of Algebra*, 1(3):301–305, 1964.

[14] Yuichiro Hoshi. Topics in the anabelian geometry of mixed-characteristic local fields. *Hiroshima Mathematical Journal*, 49(3):323–398, 2019.

[15] Yuichiro Hoshi and Yu Nishio. On the outer automorphism groups of the absolute galois groups of mixed-characteristic local fields. 2020.

[16] Nikolai V Ivanov. Algebraic properties of the teichmuller modular group. In *Doklady Akademii Nauk*, volume 275, pages 786–789. Russian Academy of Sciences, 1984.

[17] Uwe Jannsen and Kay Wingberg. Die struktur der absoluten galoisgruppe p-adischer zahlkörper. *Inventiones mathematicae*, 70(1):71–98, 1982.

[18] Moshe Jarden and Jürgen Ritter. On the characterization of local fields by their absolute galois groups. *Journal of Number Theory*, 11(1):1–13, 1979.

[19] Ilya Kapovich and Martin Lustig. Geometric intersection number and analogues of the curve complex for free groups. *Geometry & Topology*, 13(3):1805–1833, 2009.

[20] M Kapranov. Analogies between number fields and 3-manifolds. *unpublished note*, 1996.

[21] Helmut Koch. Uber galoissche gruppen von p-adischen zahlkorpern. *Mathematische Nachrichten*, 29(1-2):77–111, 1965.

[22] Helmut V Koch. The galois group of a p-closed extension of a local field. In *Doklady Akademii Nauk*, volume 238, pages 19–22. Russian Academy of Sciences, 1978.

[23] John P Labute. Classification of demushkin groups. *Canadian Journal of Mathematics*, 19:106–132, 1967.

[24] Michel Lazard. Groupes analytiques p-adiques. *Publications Mathématiques de l'IHÉS*, 26:5–219, 1965.

[25] Alexander Lubotzky. Combinatorial group theory for pro-p groups. *Journal of Pure and Applied Algebra*, 25(3):311–325, 1982.

[26] Barry Mazur. Remarks on the alexander polynomial. *Unpublished notes*, 64, 1963.

[27] Barry Mazur. Notes on étale cohomology of number fields. In *Annales scientifiques de l'École Normale Supérieure*, volume 6, pages 521–552, 1973.

[28] Shinichi Mochizuki. The profinite grothendieck conjecture for closed hyperbolic curves over number fields. *Journal of Mathematical Sciences-University of Tokyo*, 3(3):571–628, 1996.

[29] Shinichi Mochizuki. A version of the grothendieck conjecture for p-adic local fields. *International Journal of Mathematics*, 8(4):499–506, 1997.

[30] Masanori Morishita. *Knots and primes: an introduction to arithmetic topology*. Springer Science & Business Media, 2011.

[31] Jürgen Neukirch. Kennzeichnung derp-adischen und der endlichen algebraischen zahlkörper. *Inventiones mathematicae*, 6(4):296–314, 1969.

[32] Jürgen Neukirch. The absolute galois group of a p-adic number field. *Asterisque*, 94:153–164, 1982.

[33] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer Science & Business Media, 2013.

[34] Jakob Nielsen et al. Untersuchungen zur topologie der geschlossenen zweiseitigen flächen. *Acta Mathematica*, 50:189–358, 1927.

[35] Luis Paris. Residual p properties of mapping class groups and surface groups. *Transactions of the American Mathematical Society*, 361(5):2487–2507, 2009.

[36] F Pop. Lectures on anabelian phenomena in geometry and arithmetic. *Non-abelian fundamental groups and Iwasawa theory*, pages 1–55, 2011.

[37] Alexander Reznikov. Three-manifolds class field theory (homology of coverings for a nonvirtually b 1-positive manifold). *Selecta Mathematica*, 3(3):361–399, 1997.

[38] Alexander Reznikov. Embedded incompressible surfaces and homology of ramified coverings of three-manifolds. *Selecta Mathematica*, 6(1):1–39, 2000.

[39] Luis Ribes. *Profinite graphs and groups*. Springer, 2017.

[40] Eliyahu Rips. Cyclic splittings of finitely presented groups and the canonical jsj-decomposition. In *Proceedings of the International Congress of Mathematicians: August 3–11, 1994 Zürich, Switzerland*, pages 595–600. Springer, 1995.

[41] Peter Scott and Gadde A Swarup. Splittings of groups and intersection numbers. *Geometry & Topology*, 4(1):179–218, 2000.

[42] Jean-Pierre Serre. Structure de certains pro-p-groupes. *Séminaire Bourbaki*, 63:357–364, 1962.

[43] Jean-Pierre Serre. Arbres, amalgames, sl2. 1977.

[44] Jean-Pierre Serre. *Galois cohomology*. Springer, 1979.

[45] Jean-Pierre Serre. Local class field theory. In *Local Fields*, pages 188–203. Springer, 1979.

[46] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. AK Peters/CRC Press, 1997.

[47] Kôji Uchida. Isomorphisms of galois groups. *Journal of the Mathematical Society of Japan*, 28(4):617–620, 1976.

[48] Karen Vogtmann. What is... outer space? *Notices-American Mathematical Society*, 55(7):784, 2008.

[49] Gareth Wilkes. Virtual pro-p properties of 3-manifold groups. *Journal of Group Theory*, 20(5):999–1023, 2017.

[50] Gareth Wilkes. Relative cohomology theory for profinite groups. *Journal of Pure and Applied Algebra*, 223(4):1617–1688, 2019.

[51] Gareth Wilkes. Classification of pro-p pd2 pairs and the pro-p curve complex. *Groups, Geometry, and Dynamics*, 14(3):917–948, 2020.

[52] Kay Wingberg. Der eindeutigkeitssatz für demuškinformationen. *Inventiones mathematicae*, 70(1):99–113, 1982.

[53] Heiner Zieschang, Elmar Vogt, and Hans-Dieter Coldewey. *Surfaces and planar discontinuous groups*, volume 835. Springer, 2006.