Geometric Group Theory

written by Panos Papazoglou

modified and coloured-in by André Henriques

Colour coding:

gray: stuff that you can safely skip over – not exam material

green: stuff that I'm adding to the notes

blue: exercises

Contents

Chapter 1

Introduction

Geometric group theory is a descendant of combinatorial group theory, which in turn is the study of groups using their presentations. So one studies mainly infinite, finitely generated groups and is more interested in the class of finitely presented groups. Combinatorial group theory was developed in close connection to low dimensional topology and geometry.

The fundamental group of a compact manifold is finitely presented. So finitely presented groups give us an important invariant that helps us distinguish manifolds. Conversely topological techniques are often useful for studying groups. Dehn in 1912 posed some fundamental algorithmic problems for groups: The word problem, the conjugacy problem and the isomorphism problem. He solved these problems for fundamental groups of surfaces using hyperbolic geometry. Later the work of Dehn was generalized by Magnus and others, using combinatorial methods.

In recent years, due to the fundamental work of Stallings, Serre, Rips, Gromov powerful geometric techniques were introduced to the subject and combinatorial group theory developed closer ties with geometry and 3-manifold theory. This led to important results in 3-manifold theory and logic.

Some leitmotivs of combinatorial/geometric group theory are:

1. Solution of the fundamental questions of Dehn for larger classes of groups. One should remark that Novikov and Boone in the 50's showed that Dehn's problems are unsolvable in general. One may think of finitely presented groups as a jungle. The success of the theory is that it can deal with many natural classes of groups which are also important for topology/geometry. As we said the first attempts at this were combinatorial in nature, one imposed the so-called small cancelation conditions on the presentation. This was subsequently geometrized using van-Kampen diagrams by Lyndon-Schupp.

Gromov in 1987 used ideas coming from hyperbolic geometry to show that algorithmic problems can be solved for a very large ('generic') class of groups (called hyperbolic groups). It was Gromov's work that demonstrated that the geometric point of view was very fruitful for the study of groups and created geometric group theory. We will give a brief introduction to the theory of hyperbolic groups in the last sections of these notes.

2. One studies the structure of groups, in particular the subgroup structure. Ideally one would want to describe all subgroups of a given group. Some particular questions of interest are: existence of subgroups of finite index, existence of normal subgroups, existence of free subgroups and of free abelian subgroups etc.

Another structural question is the question of the decomposition of a group in 'simpler' groups. One would like to know if a group is a direct product, free product, amalgamated product etc. Further one would like to know if there is a canonical way to decompose a group in these types of products. The simplest example of such a theorem in the decomposition of a finitely generated abelian group as a direct product of cyclic groups.

In this course we will focus on an important tool of geometric group theory: the study of groups via their actions on trees, this is related to both structure theory and the subgroup structure of groups.

3. Construction of interesting examples of groups. Using amalgams and HNN extensions Novikov and Boone constructed finitely presented groups with unsolvable word and conjugacy problem. We mention also the Burnside question: Are there infinite finitely generated torsion groups? What about torsion groups of bounded exponent? The answer to both of these is yes (Novikov) but to this date it is not known whether there are infinite, finitely presented torsion groups.

Some of the recent notable successes of the theory is the solution of the Tarski problem by Sela and the solution of the virtually Haken conjecture and the virtually fibering conjecture by Agol-Wise.

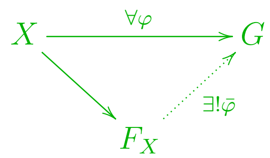
The Tarski problem was an important problem in Logic asking whether the free groups of rank 2 and 3 have the same elementary theory i.e. whether the set of sentences which are valid in F_2 is the same with the set of sentences valid in F_3. Somewhat surprisingly the positive solution to this uses actions on Trees and Topology (and comprises more than 500 pages!).

The solution of the virtually Haken conjecture and the virtually fibering conjecture by Agol-Wise implies that every closed 3-manifold can be 'build' by gluing manifolds that are quite well understood topologically and after the fundamental work of Perelman completed our picture of what 3-manifolds look like. More explicitly an obvious way to construct 3-manifolds is by taking a product of a surface with [0, 1] and then gluing the two boundary surface pieces by a homeomorphism. The result of Agol-Wise shows that every 3-manifold can be build from pieces that have a finite sheeted cover that is either S^3 or of the form described in the previous sentence.

Chapter 2

Free Groups

Definition 2.1. Let X be a subset of a group F. We say that F is a *free group with basis* X if any function φ from X to a group G can be extended uniquely to a homomorphism $\bar{\varphi} : F \to G$.



I explained how the existence of free objects is something that's not at all special to groups. There's free non-associative algebras, there's free Lie algebras, there's free monoids, there's free vector spaces, etc. They all satisfy universal properties very similar to the one above, satisfied by free groups.

One may remark that the trivial group $\{e\}$ is a free group with basis the empty set. Also the infinite cyclic group $C =< a >$ is free with basis $\{a\}$. Indeed if G is any group and if $\varphi(a) = g$ then φ is extended to a homomorphism by

$$\bar{\varphi}(a^n) = \varphi(a)^n, \ \ n \in \mathbb{Z}$$

It is clear that this extension is unique. So $\{a\}$ is a free basis of C. We remark that $\{a^{-1}\}$ is another free basis of C.

Proposition 2.1. *Let X be a set. Then there is a free group $F(X)$ with basis X.*

Proof. We consider the set $S = X \sqcup X^{-1}$ where $X^{-1} = \{s^{-1} : s \in X\}$. A word in X is a finite sequence $(s_1, ..., s_n)$ where $s_i \in S$. We denote by e the empty sequence. We usually denote words as strings of letters, so eg if (a, a^{-1}, b, b) is a word we write simply

$aa^{-1}bb$ or $aa^{-1}b^2$. Let W be the set of words in S. We define an equivalence relation $\sim$ on W generated by:

$$uaa^{-1}v \sim uv, \; ua^{-1}av \sim uv \quad \text{for any } a \in S, \, u, v \in W$$

So two words are equivalent if we can go to one from the other by a finite sequence of insertions and/or deletions of consecutive inverse letters.

Let $F := W/\sim$ be the set of equivalence classes of this relation. We denote by $[w]$ the equivalence class of $w \in W$. If

$$w = (a_1, ..., a_n), \; v = (b_1, ..., b_k)$$

then we define the product wv of w, v by

$$wv = (a_1, ..., a_n, b_1, ..., b_k)$$

We remark that if $w_1 \sim w_2$, $v_1 \sim v_2$ then $w_1v_1 \sim w_2v_2$, so we define multiplication on F by $[w][v] = [wv]$. We claim that F with this operation is a group. Indeed $e = [\emptyset]$ is the identity element and if $w = (b_1, ..., b_n)$ the inverse element is given by $w^{-1} = (b_n^{-1}, ..., b_1^{-1})$. Here we follow the usual convention that if $s^{-1} \in X^{-1}$ then $(s^{-1})^{-1} = s$. It is clear that associativity holds:

$$([w][u])[v] = [w]([u][v])$$

since both sides are equal to $[wuv]$.

If $w \in W$ we denote by $|w|$ the length of w (eg $|aa^{-1}ba| = 4$). We say that a word w is *reduced* if it does not contain a subword of the form aa^{-1} or $a^{-1}a$ where $a \in X$. To complete the proof of the theorem we need the following:

Lemma 2.1. *Every equivalence class $[w] \in F$ has a unique representative which is a reduced word.*

I proved this by constructing an action of the free group F on the set W of reduced words. Let Π denote the group of all permutations of W. Given an element $x \in X$, we construct a permutation $\pi_x : W \to W$ as follows. It acts as $w \mapsto xw$ if w does not start by x^{-1}, and as $w \mapsto v$ if w word of the form $w = x^{-1}v$ for some reduced word v. The map $\pi_x : W \to W$ is a bijection (that's the most non-trivial part of the argument), and so we get a map $X \to \Pi : x \mapsto \pi_x$. By the universal property of free groups, this extends to a homomorphism $\tilde{\pi} : F \to \Pi$.

Now let us assume that w_1 and w_2 are two reduced words that represent the same element F, namely $[w_1] = [w_2]$ in F. Then $\tilde{\pi}_{[w_1]} = \tilde{\pi}_{[w_2]}$, and so $w_1 = \tilde{\pi}_{[w_1]}(e) = \tilde{\pi}_{[w_2]}(e) = w_2$.

Proof. It is clear that $[w]$ contains a reduced word. Indeed one starts with w and eliminates successively pairs of the form aa^{-1} or $a^{-1}a$ till none are left. What this lemma says is that the order under which eliminations are performed doesn't matter. This is quite obvious but we give here a formal (and rather tedious) argument.

It is enough to show that two distinct reduced words w, v are not equivalent. We argue by contradiction. If w, v are equivalent then there is a sequence

$$w_0 = w, w_1, ..., w_n = v$$

where each w_{i+1} is obtained from w_i by insertion or deletion of a pair of the form aa^{-1} or $a^{-1}a$. We assume that for the sequence w_i the sum of the lengths $L = \sum |w_i|$ is the minimal possible among all sequences of this type going from w to v. Since w, v are reduced we have that $|w_1| > |w_0|$, $|w_{n-1}| > |w_n|$. It follows that for some i we have

$$|w_i| > |w_{i-1}|, \ |w_i| > |w_{i+1}|$$

So w_{i-1} is obtained from w_i by deletion of a pair a, a^{-1} and w_{i+1} is obtained from w_i by deletion of a pair b, b^{-1}. If these two pairs are distinct in w_i then we can delete b, b^{-1} first and then add a, a^{-1} decreasing L. More precisely if we have for instance

$$w_i = u_1bb^{-1}u_2aa^{-1}u_3, \ w_{i-1} = u_1bb^{-1}u_2u_3, \ w_{i+1} = u_1u_2aa^{-1}u_3$$

we can replace w_i by $u_1u_2u_3$. In this way L decreases by 4, which is a contradiction.

Now if the pairs a, a^{-1}, b, b^{-1} are not distinct we remark that $w_{i-1} = w_{i+1}$ which is again a contradiction. □

We can now identify X with the subset $\{[s] : s \in X\}$ of F. Let G be a group and let $\varphi : X \to G$ be any function. Then we define a homomorphism $\bar{\varphi} : F \to G$ as follows: if $s^{-1} \in X^{-1}$ we define $\bar{\varphi}(s^{-1}) = \varphi(s)^{-1}$. If $w = s_1...s_n$ is a reduced word we define

$$\bar{\varphi}([w]) = \varphi(s_1)...\varphi(s_n)$$

It is easy to see that $\bar{\varphi}$ is a homomorphism. We remark finally that this extension of φ is unique by definition. So $F(X) = F$ is a free group with basis X. □

Using the lemma above we can identify the elements of F with the reduced words of W.

Remark 2.1. In the sequel if w is any word in X (not necessarily reduced) we will also consider w as an element of the free group $F(X)$. This could cause some confusion as it is possible to have $w \neq v$ as words but $w = v$ in $F(X)$.

Exercise 1. Let $x_1, x_2, \ldots, x_n \in G$ be elements of a group. Show, using the associativity axiom, that any two parenthesizations of the word $x_1x_2\ldots x_n$ evaluate to the same element of G. In other words, show that regardless of the order by which one performs the product $x_1x_2\ldots x_n$, the outcome in G is always be the same.

Hint: Given an arbitrary parenthesization, show that it evaluates to the same element as the standard 'leftmost' parenthesization. Proceed by induction on the number of opening parentheses that occur at the beginning.

Here's a proof that, if $\phi : G \to H$ is a homomorphism, then the equation $\phi(g^{-1}) = \phi(g)^{-1}$ follows from the axioms $\phi(1) = 1$ and $\phi(gh) = \phi(g)\phi(h)$:

$$\begin{aligned}\phi(g^{-1}) &= \phi(g^{-1})1 = \phi(g^{-1})(\phi(g)\phi(g)^{-1}) \\ &= (\phi(g^{-1})(\phi(g))\phi(g)^{-1} = \phi(g^{-1}g)\phi(g)^{-1} = \phi(1)\phi(g)^{-1} = 1\phi(g)^{-1} = \phi(g)^{-1}.\end{aligned}$$

Exercise 2. Prove, by relying only on the three axioms $g1 = g = 1g$, $gg^{-1} = g^{-1}g = 1$, and $g(hk) = (gh)k$, that the equation

$$(gh)^{-1} = h^{-1}g^{-1}$$

always holds in a group. The proof should be a string of equalities of the form $(gh)^{-1} = \ldots = h^{-1}g^{-1}$, where each equality is an instance of one of the above axioms (in the same spirit as the proof of $\phi(g^{-1}) = \phi(g)^{-1}$, in green above).

Corollary 2.1. *Every group is a quotient group of a free group.*

Proof. Let G be a group. We consider the free group with basis G, $F(G)$. If $\varphi : G \to G$ is the identity map $\varphi(g) = g$, then φ can be extended to an epimorphism $\bar{\varphi} : F(G) \to G$. If $N = ker\,(\bar{\varphi})$ then

$$G \cong F(G)/N$$

□

If X is a set we denote by $|X|$ the cardinality of X.

Proposition 2.2. *Let $F(X), F(Y)$ be free groups on X, Y. Then $F(X)$ is isomorphic to $F(Y)$ if and only if $|X| = |Y|$.*

Proof. Assume that $|X| = |Y|$. We consider a 1-1 and onto function $f : X \to Y$. Let $h = f^{-1}$. The maps f, h are extended to homomorphisms $\bar{f}, \bar{h}$ and $\bar{f} \circ \bar{h}$ is the identity on $F(Y)$ while $\bar{h} \circ \bar{f}$ is the identity on $F(X)$ so $\bar{f}$ is an isomorphism.

Conversely assume that $F(X)$ is isomorphic to $F(Y)$. If X, Y are infinite sets then the cardinality of $F(X)$, $F(Y)$ is equal to the cardinality, respectively of X, Y. So if these groups are isomorphic $|X| = |Y|$. Otherwise if, say, $|X|$ is finite, we note that there are $2^{|X|}$ homomorphisms from $F(X)$ to $\mathbb{Z}_2$. Since $F(X) \cong F(Y)$ we have that $2^{|X|} = 2^{|Y|}$ so $|X| = |Y|$. □

Remark 2.2. Let $F(X)$ be a free group on X. If A is any set of generators of $F(X)$ then $|A| \geq |X|$.

Indeed if $|A| < |X|$ then there are at most $2^{|A|}$ homomorphisms from $F(X)$ to $\mathbb{Z}_2$, a contradiction.

If F is a free group with free basis X then the *rank* of F is the cardinality of X. We denote by F_n the free group of rank n.

The word problem

If F is a free group with free basis X then we identify the elements of F with the words in X. This is a bit ambiguous as equivalent words represent the same element. The word problem in this case is to decide whether a word represents the identity element. This is of course trivial as it amounts to checking whether the word reduces to the empty word after cancelations.

The conjugacy problem

Definition 2.2. If $w = s_1 ... s_n$ is a word then the cyclic permutations of w are the words:

$$s_n s_1 ... s_{n-1},\ s_{n-1} s_n ... s_{n-2},\ .....,\ s_2 ... s_n s_1$$

A word is called *cyclically reduced* if it is reduced and all its cyclic permutations are reduced words.

We remark that a word w on S is cyclically reduced if w is reduced and $w \neq xvx^{-1}$ for any $x \in S \sqcup S^{-1}$.

Proposition 2.3. *Let $F(X)$ be a free group. Every word $w \in F(X)$ is conjugate to a cyclically reduced word. Two cyclically reduced words w, v are conjugate if and only if they are cyclic permutations of each other.*

Proof. Let r be a word of minimal length that is conjugate to w. If $r = xux^{-1}$ then r is conjugate to u and $|u| < |r|$ which is a contradiction. Hence r is cyclically reduced.

Let w now be a cyclically reduced word. Clearly every cyclic permutation of w is conjugate to w. We show that a cyclically reduced word conjugate to w is a cyclic permutation of w. We argue by contradiction.

Let g be a word of minimal length such that the reduced word v representing $g^{-1}wg$ is cyclically reduced but is not a cyclic permutation of w. If the word gvg^{-1} is reduced then it is not cyclically reduced. But $w = gvg^{-1}$ and w is cyclically reduced so gvg^{-1} is not reduced. If $g = s_1 ... s_n$, $s_i \in X \cup X^{-1}$ then either $v = s_n^{-1}u$ or $v = us_n$. If $v = s_n^{-1}u$ then

$$gvg^{-1} = s_1 ... s_{n-1}(us_n^{-1})(s_1 ... s_{n-1})^{-1}$$

By our assumption that g is minimal length we have that us_n^{-1} is a cyclic permutation of w. But then $v = s_n^{-1}u$ is also a cyclic permutation of w. We argue similarly if $v = us_n$. □

Using this proposition it is easy to solve algorithmically the conjugacy problem in a free group.

Remark 2.3. A word g is cyclically reduced if and only if gg is reduced. Clearly if a word w is reduced then $w = uvu^{-1}$ where v is cyclically reduced.

Proposition 2.4. *A free group F has no elements of finite order.*

Proof. Let $g \in F$. Then g is conjugate to a cyclically reduced word h. Clearly g, h have the same order. We remark now that h^n is reduced for any $n \in \mathbb{N}$ so $h^n \neq e$, ie the order of g is infinite. □

Proposition 2.5. *Let F be a free group and $g, h \in F$. If $g^k = h^k$ for some $k \geq 1$ then $g = h$.*

Proof. Let's say that $g = ug_1u^{-1}$ with $u \in F$ and g_1 cyclically reduced. Then $g_1^k = (u^{-1}gu)^k = (u^{-1}hu)^k$. Let h_1 be the reduced word equal to $u^{-1}hu$.

If h_1 is not cyclically reduced then $g_1^k \neq h_1^k$ since h_1^k is not cyclically reduced. Otherwise

$$g_1^k = h_1^k \implies g_1 = h_1$$

since g_1^k, h_1^k are reduced words. Hence $g = h$. □

Exercise 3. Recall that the index $[G : H]$ of a subgroup $H < G$ is the cardinality of the quotient set G/H.

Show that an index two subgroup is always normal. Show that the free group of rank r, F_r, has $2^r - 1$ subgroups of index 2. *Hint:* Consider homomorphisms to $\mathbb{Z}/2$.

Exercise 4. 1. Show that F_2 has a free subgroup of rank 3.

2. Show that F_2 has a free subgroup of infinite rank.
3. Show that F_2 has an infinite index free subgroup of rank 2.

The proof of Proposition 2.2 relies on the fact that given two sets X and Y, we have $|2^X| = |2^Y| \implies |X| = |Y|$. When X and Y are infinite, this is not at all obvious to me (I don't know how to prove it, and so it might even be false). Here's a proof that works equally well when the sets are finite or infinite:

Exercise 5. Given a group G, show that the subgroup $N = \langle S \rangle$ generated by the subset

$$S := \{g \in G \,|\, g = h^2 \text{ for some } h \in G\}$$

is a normal subgroup of G. Show that the quotient group G/N is abelian. Show that G/N is a vector space over the field $\mathbb{F}_2$.

Show that when $G = F_X$ is the free group on some set X, and N is as above, then the image of X in G/N forms a basis of G/N as an $\mathbb{F}_2$-vector space. Conclude that $|X| = \dim_{\mathbb{F}_2}(G/N)$ is an invariant of F_X, and that $F_X \cong F_Y \implies |X| = |Y|$.

Hint: To show that the elements of X are linearly independent in G/N, construct suitable linear maps $G/N \to \mathbb{F}_2$.

Exercises 1–5 are due on Tuesday Jan 26th.

Chapter 3

Presentations

Definition 3.1. A *presentation* P is a pair $P = \langle S|R\rangle$ where S is a set and R is a set of words in S. The group defined by P is the quotient group

$$G = F(S)/\langle\langle R\rangle\rangle$$

where $\langle\langle R\rangle\rangle$ is the smallest normal subgroup of the free group $F(S)$ that contains R. By abuse of notation we write often $G = \langle S|R\rangle$.

Remark 3.1. From corollary 2.1 it follows that every group has a presentation.

In class, I showed that if H is a normal subgroup of G (denoted $H \triangleleft G$), then the operation $gH \cdot g'H := gg'H$ is well defined on G/H.

Exercise 6. Let G be a group, and let $H < G$ be a subgroup. Show that *if* the operation

$$\cdot : G/H \times G/H \to G/H\,, \qquad gH \cdot g'H := gg'H$$

is well defined, *then* $H \triangleleft G$.

A group G is called *finitely generated* if there are finitely many elements of G, $g_1, ..., g_n$ such that any element of g can be written as a product of $g_i^{\pm 1}$, $i = 1, ..., n$. Clearly if G is finitely generated then G has a presentation $\langle S|R\rangle$ with S finite. We say that a group $G = \langle S|R\rangle$ is *finitely related* if R is finite. If both S and R are finite we say that G is *finitely presented*. S is the set of generators and R is the set of relators of the presentation. Sometimes we write relators as equations, so instead of writing r we write $r = 1$ or even $r_1 = r_2$, which is of course equivalent to $r_1 r_2^{-1} = 1$.

Examples. 1. A presentation of $\mathbb{Z}$ is given by $\langle a|\ \rangle$.

2. A presentation of $\mathbb{Z}_n$ is given by $\langle a|a^n\rangle$.

3. A presentation of the free group $F(S)$ is given by $\langle S| \ \rangle$.

4. A presentation of $\mathbb{Z} \oplus \mathbb{Z}$ is given by $\langle a, b | aba^{-1}b^{-1} \rangle$.

Indeed if $\varphi : F(a, b) \to \mathbb{Z} \oplus \mathbb{Z}$ is the homomorphism defined by $\varphi(a) = (1, 0)$, $\varphi(b) = (0, 1)$ then clearly $aba^{-1}b^{-1} \in ker\,\varphi$. We set $N = \langle\langle aba^{-1}b^{-1} \rangle\rangle$. Since $aba^{-1}b^{-1} \in ker\,\varphi$, $N \subset ker\,\varphi$. We remark that in $F(a, b)/N$ we have that $ab = ba$. If

$$w = a^{k_1}b^{m_1}...a^{k_n}b^{m_n} \in ker\,\varphi$$

then $\sum k_i = \sum m_i = 0$. Therefore $w = 1$ in $F(a, b)/N$ since $ab = ba$ in this quotient group. It follows that $ker\,\varphi \subset N$ and $\langle a, b | aba^{-1}b^{-1} \rangle$ is a presentation of $\mathbb{Z} \oplus \mathbb{Z}$.

5. If G is a finite group, $G = \{g_1, ..., g_n\}$ then a presentation of G is: $\langle G | R \rangle$ where R is the set of the n^2 equations of the form $g_i g_j = g_k$ given by the multiplication table of G.

6. The presentation $\langle a, b | a^{-1}ba = b^2, \, b^{-1}ab = a^2 \rangle$ is a presentation of the trivial group. Indeed

$$a^{-1}ba = b^2 \implies (b^{-1}a^{-1}b)a = b \implies a^{-1} = b \implies a = 1 = b$$

Remark 3.2. Let $G = \langle S | R \rangle$. Then a word w on S represents the identity in G if and only if w lies in the normal closure of R in $F(S)$. Equivalently if w can be written in $F(S)$ as a product of conjugates of elements of R :

$$w = \prod_{i=1}^{n} x_i r_i^{\pm 1} x_i^{-1}, \;\; r_i \in R, \, x_i \in F(S)$$

We note that if w represents the identity in G we could prove that it is the case by listing all expressions of this form. Eventually we will find one such expression that is equal to w in S. Of course this presupposes that we know that $w = 1$ in G, otherwise this process will never terminate.

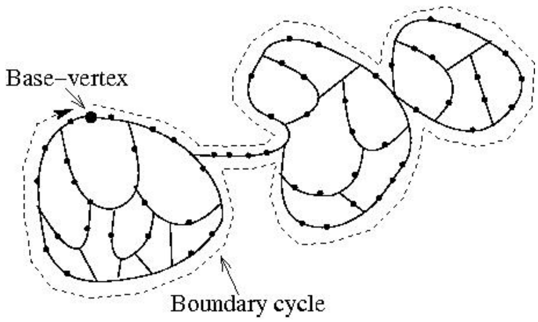
Proposition 3.1. *Let $G = \langle S | R \rangle$ and let H be a group. If $\varphi : S \to H$ is a function then φ can be extended to a homomorphism $\bar{\varphi} : G \to H$ if and only if $\varphi(r) = 1$ for every $r \in R$, where if r is the word $a_1^{\pm 1}...a_n^{\pm 1}$, we define $\varphi(r) = \varphi(a_1)^{\pm 1}...\varphi(a_n)^{\pm 1}$.*

Proof. It is obvious that $\varphi(r) = 1$ for every $r \in R$ is a necessary condition for φ to extend to a homomorphism.

Clearly φ extends to $\varphi : F(S) \to H$. Assume now that $\varphi(r) = 1$ for every $r \in R$. If $N = \langle\langle R \rangle\rangle$ then clearly $N \subset ker\,\varphi$. So the map $\bar{\varphi}(aN) = \varphi(a)$ is a well defined homomorphism from $G = F(S)/N$ to H that extends φ.

□

Let G be a group given by generators and relations: $G = \langle X|R\rangle$. A <u>*van Kampen diagram*</u> for G is a thing like this:

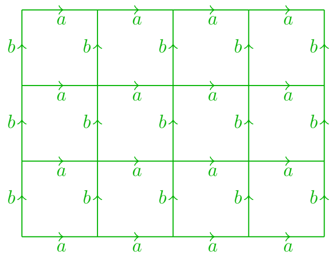


Each edge of the diagram is oriented, and labelled by an element of X. Each 2-cell reads a word $r \in R$ on its boundary. I presented in class the <u>*van Kampen lemma*</u>, along with a (rather sketchy) proof:

Lemma (van Kampen lemma)**.** *A reduced word $w \in F_X$ represents the trivial element in $G = \langle X|R\rangle$ if and only if there exists a Van Kampen diagram that reads the word w along its boundary.*

Proof. See https://en.wikipedia.org/wiki/Van_Kampen_diagram. □

Here is an example of usage of Van Kampen diagrams to show that a relation holds. *Claim:* The relation $a^n b^m = b^m a^n$ holds in the free abelian group $\langle a, b|ab = ba\rangle$.
Proof: Here's the Van Kampen diagram that proves it:



Given a presentation $G = \langle X|R\rangle$, the associated <u>*Dehn function*</u> is given by

$$D : \mathbb{N} \to \mathbb{N}$$
$$D(n) := \max_{\substack{w \in F_X, |w|=n \\ w=e \text{ in } G}} \; \min_{\substack{K:\text{ van Kampen} \\ \text{diagram, } \partial K = w}} |K|$$

It measures how hard it is to show that words are trival. For example, the Dehn function of $\mathbb{Z}^2 = \langle a, b|aba^{-1}b^{-1}\rangle$ is given by $D(n) = (n/4)^2 + \mathcal{O}(1)$.

One can use this proposition to show that a group given by a presentation is non trivial by finding a non trivial homomorphism to another group.

Before the next example we recall the definition of the semidirect product:

Let A, B be groups and let $\varphi : B \to Aut(A)$ be a homomorphism. Then we define the semidirect product of A and B to be the group $G = A \rtimes_\varphi B$ with elements the elements of the Cartesian product $A \times B$ and operation defined by

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1\varphi(b_1)(a_2), b_1 b_2) \ .$$

Example 3.1. If $G = \langle a, t | tat^{-1} = a^2 \rangle$ then $< t > \cong < a > \cong \mathbb{Z}$.

Proof. Consider the subgroup of $\mathbb{Q}$:

$$\mathbb{Z}[\tfrac{1}{2}] = \{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N}\}$$

We define an isomorphism $\varphi : \mathbb{Z}[\frac{1}{2}] \to \mathbb{Z}[\frac{1}{2}]$, by $\varphi(x) = 2x$. We form now the semidirect product $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$ where $\mathbb{Z}$ acts on $\mathbb{Z}[\frac{1}{2}]$ via φ. The elements of this semidirect product can be written as pairs $(\frac{m}{2^n}, k)$. We define now

$$\psi : G \to \mathbb{Z}[\tfrac{1}{2}] \rtimes \mathbb{Z}, \quad \text{by} \ \ \psi(a) = (1, 0), \ \ \psi(t) = (0, 1).$$

Since

$$\psi(tat^{-1}) = \psi(a^2) = (2, 0) \, ,$$

ψ is a homomorphism. Since a, t map to infinite order elements we have that
$< t > \cong < a > \cong \mathbb{Z}$.

□

Exercise 7. Prove that the group $G = \langle a, t | tat^{-1} = a^2 \rangle$ defied above is isomorphic to $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$. The easy part is to construct a map $\psi : G \to \mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$, and to show that it is surjective. The hard part is to prove injectivity.

Proceed as follows: Let $\bar{a}$ and $\bar{t}$ denote the images of a and t in $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$. First argue that there exists an action of $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$ on $\mathbb{R}^2$, given on the generators by $\bar{a} \cdot (x, y) = (x + 2^y, y)$ and $\bar{t} \cdot (x, y) = (x, y - 1)$.

Given a word $w = x_1 x_2 x_3 \dots x_n \in F_{\{\bar{a}, \bar{t}\}}$ that represents the trivial element in $\mathbb{Z}[\frac{1}{2}] \rtimes \mathbb{Z}$, consider the polygonal curve in $\mathbb{R}^2$ whose vertices are the points p, $x_n p$, $x_{n-1} x_n p$, $x_{n-2} x_{n-1} x_n p, \dots$ (p is a point in $\mathbb{R}^2$).

Now one needs to find a procedure that will simplify the curve (equivalently, that will simplify the word w) using the relation $tat^{-1} = a^2$. For this, define a measure of complexity for such curves, and show that it is possible to apply the relation $tat^{-1} = a^2$ at some place, so as to decrease the complexity. Eventually, the complexity will be zero, and the word will be trivial.

Here's a solution from Peter Neumann:

Let $G := \langle a, t \mid tat^{-1} = a^2 \rangle$ and let H be the semidirect product of the additive group A of $\mathbb{Z}[\frac{1}{2}]$ by the infinite cyclic group $\langle s \rangle$ with s acting as the doubling (or halving) automorphism. Writing A multiplicatively we see that $A \cong \langle a_0, a_1, a_2, \ldots \mid a_{i+1}^2 = a_i \rangle$, and so

$$\begin{aligned} H &\cong \langle a_0, a_1, a_2, \ldots, s \mid a_{i+1}^2 = a_i,\ s^{-1}a_i s = a_{i+1} \rangle \\ &= \langle a_0, a_1, a_2, \ldots, s \mid a_{i+1}^2 = a_i,\ s^{-i}a_0 s^i = a_i \rangle \\ &= \langle a_0, s \mid (s^{-1}a_0 s)^2 = a_0 \rangle, \end{aligned}$$

where the last equality comes from using Tietze transformations to eliminate the surplus generators $a_1,\ a_2,\ \ldots$ and the surplus relations $a_{i+1}^2 = a_i$. Thus $H \cong G$.

Exercise 8. Show that a finite index subgroup of a finitely generated group is finitely generated.

3.1 Dehn's problems

Dehn posed in 1911 the following fundamental algorithmic problems:

1. **Word problem.** Given a finite presentation $G = \langle S|R \rangle$ is there an algorithm to decide whether any word w on S is equal to 1 in G?

2. **Conjugacy problem.** Given a finite presentation $G = \langle S|R \rangle$ is there an algorithm to decide whether any words w, v on S represent conjugate elements of G?

3. **Isomorphism problem.** Is there an algorithm to decide whether any two groups G_1, G_2 given by finite presentations $G_1 = \langle S_1|R_1 \rangle$, $G_2 = \langle S_2|R_2 \rangle$ are isomorphic?

All these problems were shown to be unsolvable in general by Novikov (1955) and independently by Boone (1959). Adyan (1957) and Rabin (1958) showed that there is no algorithm to decide whether a given presentation is a presentation of the trivial group.

Here are examples of algorithms that solve the word problem for certain classes of groups:

- free groups (the algorithm is: reduce the word; check whether you get the trivial word)
- cyclic groups (the algorithm is: count the total number (with signs) of occurrences of

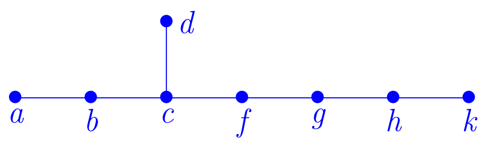
the generator; check divisibility by n.)
• free abelian groups (the algorithm is: count the total number (with signs) of occurrences of each generator; check that you get zero for each generator.)
• finite groups (the algorithm is: given a word w, multiply it out using the multiplication table of G; check whether you get e.)
• the infinite dihedral group $D_\infty = \langle a, b | a^2, b^2 \rangle$ (the algorithm is the greedy algorithm: reduce the word while eliminating any occurrence of $a^{\pm 2}$ or $b^{\pm 2}$; check whether you get the trivial word at the end.)
• Any group that admits a faithful representation $G \to GL(n\mathbb{Q})$ (the algorithm is: multiply it out the matrices; check whether you get the identity matrix.)
• Any group whose Dehn function is known, or even just an upper bound for the Dehn function (the algorithm is: given a word w, make a complete list of all van Kampen diagrams of size at most $D(|w|)$; check whether any of them satisfies $\partial K = w$)

This last class of examples has big implications for the Dehn functions of groups with unsolvable word problem. If $G = \langle X|R \rangle$ has unsolvable word problem, then its Dehn function must grow faster than *any computable function*! Actually, a word has unsolvable word problem if and only if its Dehn function grows faster than any computable function.

Exercise 9. Consider the following group, given by generators and relations:

$$G := \langle a, b, c, d, f, g, h, k | a^2 = b, b^2 = ac, c^2 = bdf, d^2 = c, f^2 = cg, g^2 = fh, h^2 = gk, k^2 = h \rangle$$

The way to remember this presentation is to draw the following graph:



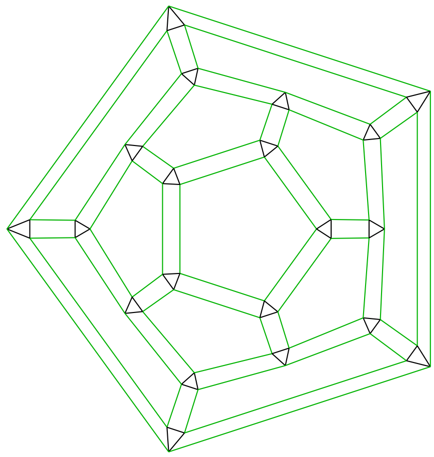
Each relation is of the form "the square of the generator is the product of its neighbours".

Prove that the elements a, d and k generate G. Write down a presentation of G that involves only those three generators.

Prove that the element c is central in G. Let $\bar{G}$ be the quotient of G by the central subgroup generated by c. Write down a presentation of $\bar{G}$.

Prove that the elements a and k generate $\bar{G}$. Write down a presentation of $\bar{G}$ that involves only those two generators. Construct a homomorphism from $\bar{G}$ to the group of symmetries of a regular dodecahedron.

Consider the following picture:

$K \ =$ 

which we are going to interpret as a van Kampen diagram for $\bar{G}$.

Use this picture to prove that the group $\bar{G}$ is isomorphic to the group of symmetries of a regular dodecahedron.

Hint: Show that the group of symmetries of a regular dodecahedron acts simply transitively on the set of vertices of K, and show that any word in $\bar{G}$ can be interpreted as a path in K.

Finally, prove that $c^2 = e$ in G.

Hint: Compute k^5 in two ways. The first way is direct, and uses one of the relations. The second way is indirect: it relies on the above van Kampen diagram K, and on the fact that c is central.

Exercises 6–9 are due on Tuesday Feb 2nd.

3.2 Tietze transformations

Different presentations of the same group are related via Tietze transformations. There are two types of Tietze transformations:

(T1) If $\langle S|R\rangle$ is a presentation and $r \in \langle\langle R\rangle\rangle \subset F(S)$ then T1 is the replacement of $\langle S|R\rangle$ by $\langle S|R \cup \{r\}\rangle$. Clearly these two presentations define isomorphic groups, an isomorphism ϕ is defined on the generators by $\phi(s) = s$ for all $s \in S$.

We denote also by T1 the inverse transformation.

(T2) If $\langle S|R\rangle$ is a presentation, $a \notin S$ and $w \in F(S)$ then T2 is the replacement of $\langle S|R\rangle$ by $\langle S \cup \{a\}|R \cup \{a^{-1}w\}\rangle$. Clearly these two presentation define isomorphic groups. A homomorphism ϕ is defined on the generators by $\phi(s) = s$ for all $s \in S$. One verifies easily that the inverse of ϕ is given by $\psi(s) = s$ for all $s \in S$ and $\psi(a) = w$.

We denote also by T2 the inverse transformation.

Theorem 3.1. *Two finite presentations $\langle S_1|R_1\rangle$, $\langle S_2|R_2\rangle$ define isomorphic groups if and only if they are related by a finite sequence of Tietze transformations.*

Proof. It is clear that if two presentations are related by a finite sequence of Tietze transformations they define isomorphic groups. Conversely suppose that $G_1 = \langle S_1|R_1\rangle \cong \langle S_2|R_2\rangle = G_2$. We may assume that $S_1 \cap S_2 = \emptyset$. Indeed if this is not the case using moves T1, T2 we can replace S_1 by a set of letters with the same cardinality, disjoint from S_2. We consider now isomomorphisms

$$\varphi : G_1 \to G_2, \ \ \psi = \varphi^{-1} : G_2 \to G_1$$

For each $s \in S_1, t \in S_2$ consider words w_s, v_t such that $\varphi(s) = w_s, \ \psi(t) = v_t$. Let

$$U_1 = \{s^{-1}w_s : s \in S_1\}, \ \ U_2 = \{t^{-1}v_t : t \in S_2\}$$

We consider the presentation:

$$\langle S_1 \cup S_2|R_1 \cup R_2 \cup U_1 \cup U_2\rangle$$

We claim that there is a finite sequence of Tietze transformations from $\langle S_1|R_1\rangle$ to this presentation. Indeed using $T2$ we may introduce one by one the generators of S_2 and the relations U_2. So we obtain the presentation

$$\langle S_1 \cup S_2|R_1 \cup U_2\rangle$$

The Tietze transformations give as an isomorphism

$$\rho : \langle S_1 \cup S_2|R_1 \cup U_2\rangle \to \langle S_1|R_1\rangle$$

where $\rho(s) = s$, $\rho(t) = v_t$ for $s \in S_1$, $t \in S_2$. We remark that $\varphi \circ \rho$ is a homomorphism from $\langle S_1 \cup S_2|R_1 \cup U_2\rangle$ to $\langle S_2|R_2\rangle$ and $\varphi \circ \rho(t) = t$ for all $t \in S_2$. It follows that for any $r \in R_2$, $\varphi \circ \rho(r) = r = 1$, hence $R_2 \subseteq \langle\langle R_1 \cup U_2\rangle\rangle$. So using $T1$ we obtain the presentation

$$\langle S_1 \cup S_2|R_1 \cup R_2 \cup U_2\rangle$$

We remark now that $\varphi \circ \rho$ is still defined on this presentation and $\varphi \circ \rho(s) = w_s$ for all $s \in S_1$, while $\varphi \circ \rho(w_s) = w_s$. It follows that $s^{-1}w_s$ is mapped to 1 by $\varphi \circ \rho$, hence the relators U_1 also follow from $R_1 \cup R_2 \cup U_2$. So applying T1 we obtain

$$\langle S_1 \cup S_2 | R_1 \cup R_2 \cup U_1 \cup U_2 \rangle$$

Similarly we see that there is a finite sequence of Tietze transformations from $\langle S_2 | R_2 \rangle$ to this presentation. □

Exercise 10. Let G be a group and let X and Y be two subsets of G such that generate it: $G = \langle X \rangle = \langle Y \rangle$. Show that if X is finite then there is a finite subset $Y' \subset Y$ such that $G = \langle Y' \rangle$. Show that if X is infinite and $|X| < |Y|$, then there exists a subset $Y' \subset Y$ of same cardinality as X, such that $G = \langle Y' \rangle$.

So, in a sense, finite generation does not depend on the generating set we pick. The next proposition shows that something similar holds for finite presentability.

Proposition 3.2. *Let $G \cong \langle S|R \rangle \cong \langle X|Q \rangle$ where S, X, R are finite. Then there is a finite subset Q' of Q such that $G \cong \langle X|Q' \rangle$*

Proof. Let $\varphi : F(S)/\langle\langle R \rangle\rangle \to F(X)/\langle\langle Q \rangle\rangle$ be an isomorphism. Let

$$S = \{s_1, ..., s_n\},\ R = \{r_1, ..., r_k\},\ X = \{x_1, ..., x_m\}$$

Then the r_i's are words in the s_j's, $r_i = r_i(s_1, ..., s_n)$. Let $\varphi(s_i) = s_i'$, $i = 1, ..., n$. If we see the s_i' as elements of $F(X)$, since φ is onto we have that the generators of G can be written in terms of the s_i', so there are words $w_j(s_1', ..., s_n')$, $j = 1, ..., m$ and $u_1, ..., u_m \in \langle\langle Q \rangle\rangle$ such that

$$x_j = w_j(s_1', ..., s_n')u_j,\ j = 1, ..., m$$

where the equality is in $F(X)$. Since φ is a homomorphism we have also that

$$r_i(s_1', ..., s_n') = v_i \in \langle\langle Q \rangle\rangle,\ i = 1, ..., k$$

Let Q' be a finite subset of Q such that all u_j, v_i, $j = 1, ..., m$, $i = 1, ..., k$ can be written as products of conjugates of elements of Q'. We claim that $\langle\langle Q' \rangle\rangle = \langle\langle Q \rangle\rangle$. Indeed the map

$$\psi : F(S)/\langle\langle R \rangle\rangle \to F(X)/\langle\langle Q' \rangle\rangle$$

given by $\psi(s_i) = s_i'$ is an onto homomorphism and $\varphi = \pi \circ \psi$ where π is the natural quotient map

$$\pi : F(X)/\langle\langle Q' \rangle\rangle \to F(X)/\langle\langle Q \rangle\rangle$$

However φ is 1-1 so π is also 1-1. It follows that $\langle\langle Q' \rangle\rangle = \langle\langle Q \rangle\rangle$. □

Proposition 3.3. *If the word problem is solvable for the finite presentation $\langle S|R \rangle$ of a group G then it is solvable for any other finite presentation $\langle X|Q \rangle$ of G. The same is true for the conjugacy problem.*

One can do much better than the proof presented below (in gray):

Proof. Let $\varphi : F(X)/\langle\langle Q \rangle\rangle \to F(S)/\langle\langle R \rangle\rangle$ be an isomorphism, and let $\tilde{\varphi} : F(X) \to F(S)$ be a homomorphism that induces φ upon taking quotients. Assuming the word problem (or conjugacy problem) for $\langle S|R \rangle$ is solvable by some algorithm A, then it's very easy to write down an algorithm A' that solves the word problem (or conjugacy problem) for $\langle X|Q \rangle$. The algorithm A' takes a word $w \in F(X)$ (or a pair of words in the case of the conjugacy problem), feeds it to $\tilde{\varphi}$, and then applies algorithm A.

Proof. To solve the word problem, given a word w on X we run 'in parallel' two procedures:

1) We list all elements in $\langle\langle Q \rangle\rangle$.

2) We list all homomorphisms $\varphi : F(X)/\langle\langle Q \rangle\rangle \to F(S)/\langle\langle R \rangle\rangle$. To find φ we enumerate $|X|$-tuples of words in $F(S)$ and we check for each such choice whether the relations Q are satisfied. We note that this is possible to do since the word problem is solvable in $\langle S|R \rangle$. Given a homomorphism φ we check whether $\varphi(w) \neq 1$ (which is possible to do since the word problem is solvable in $\langle S|R \rangle$).

Clearly one of the procedures 1,2 will terminate. We note that if the conjugacy problem is solvable for a group then the word problem is also solvable (why?). To solve the conjugacy problem, given two words w, v on X we argue similarly:

1a) We list all elements of the form $gvg^{-1}w^{-1}$.

1b) We list all elements in $\langle\langle Q \rangle\rangle$ and check whether some element is equal to $gvg^{-1}w^{-1}$ in $F(X)$.

2. We list all homomorphisms $\varphi : F(X)/\langle\langle Q \rangle\rangle \to F(S)/\langle\langle R \rangle\rangle$ and, given a homomorphism f, we check whether $f(w), f(v)$ are not conjugate in $\langle S|R \rangle$. Clearly if $f(w), f(v)$ are not conjugate in $\langle S|R \rangle$ they are not conjugate in $\langle X|Q \rangle$. □

We remark that this proposition shows that the solvability of the word and the conjugacy problem is a property of the group and not of the presentation.

3.3 Residually finite groups, simple groups

Definition 3.2. A group G is called *residually finite* if for every $1 \neq g \in G$ there is a homomorphism φ from G to a finite group F such that $\varphi(g) \neq 1$.

Exercise 11. Show that if $H < G$ is a finite index subgroup, then the subgroup $\bigcap_{g \in G} gHg^{-1}$ also has finite index in G. *Hint:* Consider the various stabilizers of the action of G on G/H.

Prove that a group G is residually finite if and only if the intersection of all its finite index subgroups is trivial.

Exercise 12. Show that if G has a finite index subgroup which is residually finite, then G itself is residually finite.

Exercise 13. Let G be a finitely generated group. Show that G has finitely many subgroups of index n.
Hint: Establish a bijection between subgroups of index n and transitive actions of G on pointed sets of cardinality n.

Remark 3.3. If a group G is residually finite then clearly any subgroup of G is also residually finite.

Proposition 3.4. *Let G be a residually finite group and let $g_1, ..., g_n$ be distinct elements of G. Then there is a homomorphism $\varphi : G \to F$ where F is finite, such that $\varphi(g_i) \neq \varphi(g_j)$ for any $1 \leq i < j \leq n$.*

Proof. If $h_1, ..., h_k$ are non trivial elements of G there are homomorphisms $\varphi_i : G \to F_i$, where F_i are finite, such that $\varphi_i(h_i) \neq 1$ for every i. It follows that

$$\varphi = (\varphi_1, ..., \varphi_k) : G \to F_1 \times ... \times F_k$$

is a homomorphism to a finite group such that $\varphi(h_i) \neq 1$ for every i. Now we apply this observation to the set of non-trivial elements $g_i g_j^{-1}$ $(1 \leq i < j \leq n)$ and we obtain a homomorphism $\varphi : G \to F$ (F finite), such that $\varphi(g_i g_j^{-1}) \neq 1$, hence $\varphi(g_i) \neq \varphi(g_j)$ for any $1 \leq i < j \leq n$. □

Intuitively residually finite groups are groups that can be 'approximated' by finite groups.

Matrix groups furnish examples of residually finite groups. To whow this we will need two easy lemmas. We leave the proofs to the reader.

Lemma 3.1. *Let A, B be commutative rings with 1 and let $f : A \to B$ be a ring homomorphism. Then the map $\bar{f} : SL_n(A) \to SL_n(B)$ given by $\bar{f}((a_{ij})) = (f(a_{ij}))$ is a group homorphism.*

Lemma 3.2. *Let A be a subring of $\mathbb{Q}$. Assume that there is a prime p such that for any $a/b \in A$, p does not divide b. Then the map $\phi : A \to \mathbb{Z}_p$, $\phi(a/b) = ab^{-1}$ is a ring homomorphism.*

Proposition 3.5. *$GL_n(\mathbb{Z})$ is a residually finite group.*

Proof. Indeed by lemma 3.1 if p is a prime we have a homomorphism

$$\varphi_p : GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}_p)$$

Clearly for any $g \neq 1$, $\varphi_p(g) \neq 1$ for some p. □

Proposition 3.6. *Any finitely generated subgroup G of $SL_n(\mathbb{Q})$ (or $GL_n(\mathbb{Q})$) is a residually finite group.*

Proof. Let $G =< g_1, ..., g_n >$. Let $p_1, ..., p_k$ be the primes that appear in the numerators or denominators of the entries of the matrices $g_1, ..., g_n$. If p is any other prime then by lemmas 3.1, 3.2 we have a homomorphism:

$$\varphi_p : G \to SL_n(\mathbb{Z}_p)$$

Clearly for any $g \in G$, $g \neq 1$, $\varphi_p(g) \neq 1$ for some prime p.

Clearly the same holds for subroups of $GL_n(\mathbb{Q})$ as we may see $GL_n(\mathbb{Q})$ as a subgroup of $SL_{n+1}(\mathbb{Q})$.

□

In fact by a similar argument one can show that the same proposition holds for any finitely generated subgroup of $GL_n(\mathbb{C})$. This uses the fact from ring theory that if R is a finitely generated ring and $\mathfrak{m}$ is a maximal ideal of R, then $R/\mathfrak{m}$ is a finite field. If R is furthermore a domain (i.e. doesn't have zero-divisors), then we also have $\bigcap_{m\in\mathbb{N}} \mathfrak{m}^m = \{0\}$.

The homomorphisms $GL_n(R) \to GL_n(R/\mathfrak{m}^m)$ are enough to faithfully detect any non-trivial element of $GL_n(R)$.

Exercise 14. Prove that the group $(\mathbb{Q}, +)$ is not residually finite.

Theorem 3.2. *Let G be a residually finite group admitting a finite presentation $\langle S|R\rangle$. Then G has a solvable word problem.*

Proof. Given a word $w \in F(S)$ we enumerate in parallel homomorphisms $f : G \to S_n$ (where S_n are the groups of permutations of $\{1, ..., n\}$) and the elements of $\langle\langle R\rangle\rangle$. Eventually either for some f, $f(w) \neq 1$, hence $w \neq 1$ in G, or we will have that $w \in \langle\langle R\rangle\rangle$ and so $w = 1$ in G. □

Theorem 3.3. *The free group F_n is residually finite.*

Proof. Since F_n is a subgroup of F_2 it is enough to show that F_2 is residually finite. One way to show this is to prove that F_2 is isomorphic to a subgroup of $GL_2(\mathbb{Z})$ (exercise). We give here a different proof. Let $w \in F_2 =< a, b >$ be a reduced word of length k. Let B be the set of reduced words of length less or equal to k. We consider the group of permutations of B, $Symm(B)$. We define now two permutations α, β of $Symm(B)$: If $|v| \leq k-1$ we define $\alpha(v) = av$ and we extend α to the words of length k in any way. Similarly if $|v| \leq k-1$ we define $\beta(v) = bv$ and we extend β in the words of length k in any way. We define now a homomorphism

$$\varphi : F_2 \to Symm(B), \ \varphi(a) = \alpha, \varphi(b) = \beta$$

Clearly $\varphi(w)(e) = w$ so $\varphi(w) \neq 1$. □

Definition 3.3. We say that a group G is *Hopf* if every epimorphism $\varphi : G \to G$ is 1-1.

Theorem 3.4. *If a finitely generated group G is residually finite then G is Hopf.*

Proof. Assume that G is residually finite but not Hopf. Let $f : G \to G$ be an onto homomorphism and let $1 \neq g \in ker\, f$. Let F be a finite group and let $\varphi : G \to F$ be a homomorphism such that $\varphi(g) \neq 1$.

Since f is onto there is a sequence $g_0 = g, g_1, ..., g_n, ...$ such that $f(g_n) = g_{n-1}$ for any $n \geq 1$. This implies that the homomorphisms

$$\varphi \circ f^{(n)} : G \to F$$

are all distinct since for any $n \geq 1$

$$\varphi \circ f^{(n)}(g_n) \neq 1, \ \varphi \circ f^{(n)}(g_k) = 1 \text{ for } k < n$$

This is a contradiction since G is finitely generated and so there are only finitely many homomorphisms from G to F. □

Corollary 3.1. *If A is a generating set of n elements of the free group of rank n, F_n, then A is a free basis of F_n.*

Proof. Let X be a free basis of F_n and let $\varphi : X \to A$ be a 1-1 function. Then φ extends to a homomorphism $\varphi : F_n \to F_n$. Since A is a generating set φ is onto. However F_n is residually finite and hence Hopf. It follows that φ is an isomorphism and A a free basis of F_n. □

Definition 3.4. The group G is called *simple* if the only normal subgroups of G are $\{1\}$ and G.

Theorem 3.5. *Let $G = \langle S|R\rangle$ be a finitely presented simple group. Then G has a solvable word problem.*

Proof. Let w be a word in S. We remark that if $w \neq 1$ in G then $\langle\langle w\rangle\rangle = G$, so $\langle\langle w \cup R\rangle\rangle = F(S)$.

We enumerate in parallel the elements of $\langle\langle w \cup R\rangle\rangle$ and of $\langle\langle R\rangle\rangle$ in $F(S)$. If $w = 1$ then eventually w will appear in the list of $\langle\langle R\rangle\rangle$, while if $w \neq 1$ the set S will eventually appear in the list of $\langle\langle w \cup R\rangle\rangle$. □

Exercise 15. (Ping-pong lemma)
Let G be a group acting on a set S and let $a, b \in G$ be two elements. Prove that if there are non empty disjoint subsets A, B of S such that $a^n B \subseteq A$, and $b^n A \subseteq B$ for all $n \in \mathbb{Z} \setminus \{0\}$ then $\{a, b\}$ generate a free subgroup of G.
Hint: if w is a reduced word that starts and ends with an $a^{\pm 1}$ then show that we have $wB \subseteq A$. Otherwise replace w by a conjugate and use the same argument.

Formulate and prove a version of the ping-pong lemma that works with *three* elements $a, b, c \in G$ instead of two.

Exercise 16. Show that the matrices $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$ generate a free subgroup of $SL(2, \mathbb{Z})$. *Hint:* Apply the above ping pong lemma to some suitable subsets $A, B \subset \mathbb{R}^2$.

Exercise 17. Show that every finitely presented group has a finite presentation in which every relation is a word of length at most 3.

Exercise 18. Show that if G has a solvable word problem and H is a finitely generated subgroup of G then H also has a solvable word problem.

Exercise 19. An infinite finitely generated group is called just infinite if all its quotients are finite groups. Show that every infinite finitely generated group has a quotient that is just infinite.
Hint: Write $G = \{g_1, g_2, g_3, g_4, \ldots\}$. Define G_i inductively by $G_i := G_{i-1}/\langle\langle g_i \rangle\rangle$ if the latter is infinite, and $G_i := G_{i-1}$ otherwise. Argue by contradiction that the "limit" of the G_i's is an infinite group. Finally, show that this group is just infinite.

Exercises 10–19 are due on Tuesday Feb 9nd.

Exercise 20. We say that a subgroup H of G is *separable* if it is equal to the intersection of all the finite index subgroups of G containing it.
i) Show that G is residually finite if and only if $\{e\}$ is a separable subgroup of G.
ii) Let G be residually finite and let $r : G \to G$ be a retract (a retract is am endomorphism that satisfies $r^2 = r$). Show that $r(G)$ is a separable subgroup.

Chapter 4

Group actions on Trees

4.1 Group actions on sets

We recall the definition of a group action on a set:

Definition 4.1. Let G be a group and let X be a set. An *action* of G on X is a map

$$\rho : G \times X \to X$$

so that the following hold:

1. $\rho(1, x) = x$ for all $x \in X$.
2. $\rho(g_1 g_2, x) = \rho(g_1, \rho(g_2, x))$ for all $g_1, g_2 \in G, x \in X$.

We often write simply $g(x)$ or gx instead of $\rho(g, x)$. Note that by property 2, $g^{-1}(gx) = x$. It follows that the map

$$x \mapsto gx$$

is 1-1 and onto map from X to X.

In fact we have an equivalent definition of a group action as a homomorphism:

$$\varphi : G \to Symm(X)$$

Indeed if $\rho : G \times X \to X$ is an action define $\varphi : G \to Symm(X)$ by $\varphi(g)(x) = gx$. Property 2 of the definition implies that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. Conversely given a homomorphism φ we define $\rho : G \times X \to X$ by $\rho(g, x) = \varphi(g)(x)$.

We often denote an action by $G \curvearrowright X$.

4.2 Graphs

Definition 4.2. A *graph* Γ consists of a set of vertices $V = V(\Gamma)$, a set of edges $E = E(\Gamma)$, a map:

$$E \to V \times V, \;\; e \mapsto (o(e), t(e))$$

and a map $E \to E, \;\; e \mapsto \bar{e}$ such that the following hold: for any $e \in E$, $\bar{\bar{e}} = e$, $\bar{e} \neq e$ and $o(\bar{e}) = t(e), \;\; t(\bar{e}) = o(e)$.

The pair of edges $\{e, \bar{e}\}$ is called *geometric edge*. Often when we define graphs we just give the vertices and the geometric edges of the graph. A choice of edges $E^+ \subset E(\Gamma)$ such that for any $e \in E(\Gamma)$ either $e \in E^+$ or $\bar{e} \in E^+$ is called an *orientation* of Γ.

A morphism between two graphs is a map that preserves the graph structure. More formally we have:

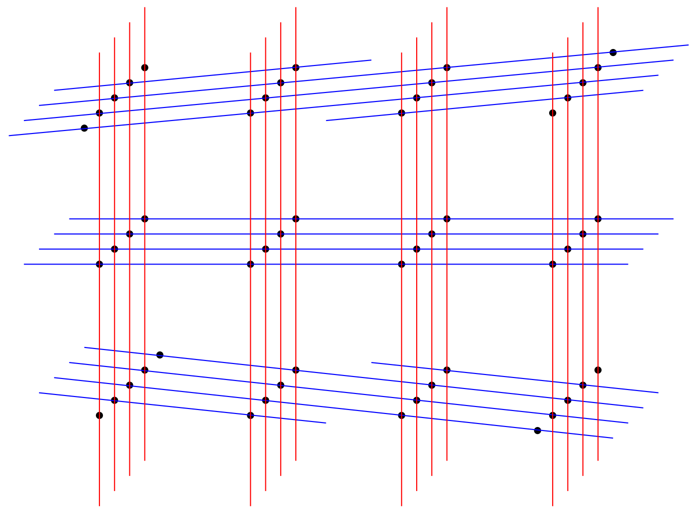
Definition 4.3. A *morphism* f from a graph $\Gamma = (V(\Gamma), E(\Gamma))$ to graph $\Delta = (V(\Delta), E(\Delta))$ is given by maps $f_V : V(\Gamma) \to V(\Delta), \;\; f_E : E(\Gamma) \to E(\Delta)$ such that $o(f(e)) = f(o(e)), \;\; t(f(e)) = f(t(e)), \;\; f(\bar{e}) = \overline{f(e)}$. An automorphism of Γ is a morphism $\Gamma \to \Gamma$ that is 1-1 and onto on the sets of edges and vertices. We denote by $Aut(\Gamma)$ the group of automorphisms of Γ.

Definition 4.4. Let $G =< S >$ be a group generated by S. We define the *Cayley graph* of G, $\Gamma = \Gamma(S, G)$, to be the graph with vertices $V(\Gamma) = \{g : g \in G\}$ and oriented edges $E^+(\Gamma) = \{(g, gs) : g \in G, \; s \in S\}$. We define $o(g, gs) = g$, $t(g, gs) = gs$.

More generally if $S \subset G$, where S is not necessarily a generating set we define the graph $\Gamma(S, G)$ as before to be the graph with vertices $\{g : g \in G\}$ and edges $\{(g, gs) : g \in G, \; s \in S\}$.

Remark 4.1. The Cayley graph of G is a connected graph. Corversely if if $\Gamma(S, G)$ is connected for some $S \subset G$, then S is a generating set of G.

Exercise 21. Find the group G whose Cayley graph this is a piece of:



Describe G either by means of a presentation, or by any other means you like.
Hint: Show that this group admits a homomorphism to $\mathbb{Z}^2$ with kernel $\mathbb{Z}$.

Definition 4.5. A *path* in a graph Γ is a sequence of edges $p = (e_1, ..., e_n)$ such that $o(e_i) = t(e_{i-1})$ for all $i > 1$. The vertices $x = o(e_1)$, $y = t(e_n)$ are the *origin* and the *end point* of the path respectively. We often say that p joins x, y. We define similarly infinite paths. We say that a path is *reduced* if $e_i \neq \bar{e}_{i-1}$ for all $i > 1$. We say that a path $(e_1, ..., e_n)$ is a *circuit* if it is reduced, the vertices $t(e_i)$ $(i = 1, ..., n)$ are all distinct and $t(e_n) = o(e_1)$. We say that a graph is *connected* if any two vertices can be joined by a path. A *tree* is a connected graph with no circuits.

Remark 4.2. A graph Γ is a tree if and only if for any two vertices of Γ there is a unique reduced path joining them (exercise).

One may realize graphs as 1-dimensional CW-complexes: we start with a set of points (vertices) and glue edges to them; so if $e = [0, 1]$ is an edge we glue 0 to $o(e)$ and 1 to $t(e)$. The edges $e, \bar{e}$ correspond geometrically to the same edge, and $e, \bar{e}$ are thought of as the two possible orientations of this edge. We can equip a connected graph with a metric by identifying each edge with an interval of length 1 and defining the distance of two points to be the length of the shortest path joining them.

Definition 4.6. An *action* of a group G on a graph Γ is a homomorphism $\rho : G \to Aut(\Gamma)$.

If $\rho : G \to Aut(\Gamma)$ is an action, $g \in G$ and $v \in V(\Gamma)$ then $\rho(g)(v) \in V(\Gamma)$. Usually we simplify the notation and we write gv rather than $\rho(g)(v)$. If G acts on Γ we write also $G \curvearrowright \Gamma$. If there is some $v \in V(\Gamma)$ such that $gv = v$ for all $g \in G$ then we say that G fixes a vertex of Γ.

Remark 4.3. A group $G =< S >$ acts on its Cayley graph $\Gamma(S, G)$ as follows: If $g \in G$ and (v, vs) an edge of $\Gamma(S, G)$ we define $g \cdot (v, vs) = (gv, gvs)$. We remark that this action is transitive on the set of vertices of $\Gamma(S, G)$.

4.3 Actions of free groups on Trees

Theorem 4.1. *Let S be a subset of a group G, and let $X = \Gamma(S, G)$. The following are equivalent:*
i) X is a tree.
ii) G is free with basis S.

Proof. ii) $\implies$ i).

Assume that G is free with basis S. Every element of G can be represented by a reduced word in S, $s_1 ... s_n$. There is a path from 1 to $s_1 ... s_n$:

$$p = ((1, s_1), (s_1, s_1 s_2), ..., (s_1 s_2 ... s_{n-1}, s_1 s_2 ... s_{n-1} s_n))$$

so X is connected. In general a reduced path starting at 1 corresponds to a reduced word in S, w. Since reduced words represent non trivial elements in G we have that $w \neq 1$ in G, so there are no circuits staring at 1. However since the action of G is transitive on vertices we deduce that X has no circuits, hence it is a tree.

i) $\implies$ ii)

Since X is connected there is a reduced path from 1 to any $g \in G$. Therefore any $g \in G$ can be written as a word in S. It follows that S generates G. Let $\varphi : F(S) \to G$ be the onto homomorphism defined by $\varphi(s) = s$ for all $s \in S$. Then if $s_1 ... s_n \in ker\, \varphi$ ($s_1 ... s_n$ reduced word) we have that the path

$$p = ((1, s_1), (s_1, s_1 s_2), ..., (s_1 s_2 ... s_{n-1}, s_1 s_2 ... s_{n-1} s_n))$$

is a reduced path in X from 1 to 1, which is impossible. We conclude that φ is 1-1, so $G \cong F(S)$.

□

Definition 4.7. Let G be a group acting on a graph X. We say that G acts on X *without inversions* if for every $g \in G$, $e \in E(X)$ we have that $ge \neq \bar{e}$. We say that G

acts *freely* on X if G acts on X without inversions and for any $1 \neq g \in G$, $v \in V(X)$, $gv \neq v$.

Remark 4.4. A group $G =< S >$ acts without inversions on the Cayley graph $\Gamma(S, G)$.

Note that if G acts on a graph Γ then it acts without inversions on the barycentric subdivision of Γ (i.e. the graph obtained by subdividing each edge of Γ in two edges).

Definition 4.8. Let G be a group acting without inversions on a graph X. We define the *quotient graph* of the action X/G as follows: If $v \in V(X)$, $e \in E(X)$ we set

$$[v] = \{gv : g \in G\}, \ [e] = \{ge : g \in G\}$$

The vertices and edges of the quotient graph are given by

$$V(X/G) = \{[v] : v \in V(X)\}, \ E(X/G) = \{[e] : e \in E(X)\}$$

and $o([e]) = [o(e)], \ t([e]) = [t(e)], \ \overline{[e]} = [\bar{e}]$.

We remark that since the action is without inversions $[\bar{e}] \neq [e]$. There is an obvious graph morphism

$$p : X \to X/G, \text{ given by } p(v) = [v], \ p(e) = [e], \ v \in V(X), e \in E(X)$$

Theorem 4.2. *If a group G acts freely on a tree T then G is free.*

I gave a topological proof of this theorem, using the technology of covering spaces.

Proof: Since G acts freely on Γ, the quotient graph Γ/G makes sense. Since Γ is contractible it is in particular simply connected. It follows that the quotient map

$$p : \Gamma \to \Gamma/G$$

exhibits Γ as the universal cover of Γ/G. The group G acts on Γ by deck transformations (i.e. maps that commute with the map p) and acts simply transitively on the fibers of p. It follows that G is isomorphic to the fundamental group of the graph Γ/G. To finish the argument, we use the fact that any graph is homotopy equivalent to a wedge of circles, and that the fundamental group of a a wedge of circles is a free group. □

Lemma Every graph is homotopy equivalent to a wedge of circles.

Proof: Let Γ be a graph. Pick a maximal tree $T \subset \Gamma$. Then Γ/T is a wedge of circles, and the map $\Gamma \to \Gamma/T$ is a homotopy equivalence. □

Exercise 22. Let Γ be a graph and let $T \subset \Gamma$ be a maximal subtree. Prove that the quotient map $p : \Gamma \to \Gamma/T$ is a homotopy equivalence. (To show this, by definition, you need to construct a homotopy inverse $q : \Gamma/T \to \Gamma$, and argue that $p \circ q$ and $q \circ p$ are homotopic to the respective identity maps.)

Exercise 23. Let H is a subgroup of the free group F_n of index $r := |F_n : H|$. Show that H is a free group of rank $r(n-1)+1$.
Hint: By the theory of covering spaces, there is a bijective correspondence between (pointed) covers of a topological space Γ, and subgroups of its fundamental group $\pi_1(\Gamma)$. Compute the Euler characteristic (defined as $\#\{\text{vertices}\} - \#\{\text{edges}\}$) of the finite cover of $\bigvee_{i=1}^{n} S^1$ associated to H, and use the fact that the Euler characteristic is a homotopy invariant (a fact which is easily shown to hold for graphs — see the previous exercise for an idea of proof).

Proof.

Lemma 4.1. *There is a tree $X \subset T$ such that X contains exactly one vertex from each orbit of the action.*

Proof. Let X be a maximal subtree of T such that X contains at most one vertex from each orbit. Clearly such a tree exists by Zorn's lemma. Suppose that X does not intersect all orbits of vertices. Let v be a vertex of minimal distance from X such that X does not meet its orbit. If $d(v, X) = 1$ then we can add v to X contradicting its maximality. Otherwise if p is a reduced path from v to X and v' is the first vertex of p then $gv' \in X$ for some $g \in G$. But then $d(gv, X) = 1$ so we can add gv to X, a contradiction. We conclude that X contains exactly one vertex from each orbit. □

Let X be as in the lemma. We choose an orientation of the edges of T, $E^+ \subset E(T)$ such that E^+ is invariant under the action (that is $e \in E^+ \Rightarrow ge \in E^+$, for all $g \in G$). This is possible since the action is without inversions.

Consider the set

$$S = \{g \in G : \text{ there is an edge } e \in E^+ \text{ with } o(e) \in X,\ t(e) \in g(X)\}$$

We will show that G is a free group with basis S.

Clearly if $g_1 \neq g_2$ then $g_1X \cap g_2X = \emptyset$. Let T' be the tree that we obtain from T by contracting each translate gX to a point. Clearly G acts on T'. We will show that $T' \simeq \Gamma(S, G)$. We remark that $V(T') = \{gX : g \in G\}$, $E(T') = \{e \in T,\ e \notin GX\}$. The orientation of T induces an orientation of the edges of T' which we denote still by

E^+. We define now $\varphi : T' \to \Gamma(S, G)$ as follows: $\varphi(gX) = g$. If $e \in E^+$ is an edge joining g_1X to g_2X then $s = g_1^{-1}g_2 \in S$ since $g_1^{-1}e$ joins X to $g_1^{-1}g_2X$. So we define $\varphi(e) = (g_1, g_1 s) = (g_1, g_2)$. It is clear that φ is 1-1 and onto on the set of vertices $V(T')$. It is also onto on edges: if (g, gs) is an edge of $\Gamma(S, G)$ then there is an oriented edge $e \in T'$ joining X to sX and $\varphi(ge) = (g, gs)$. We note that if

$$\varphi(e_1) = \varphi(e_2) = (g, gs)$$

then e_1, e_2 are both oriented edges joining gX to gsX. But T' is a tree so $e_1 = e_2$ and φ is 1-1.

It follows that $\Gamma(S, G)$ is a tree, hence G is free (theorem 4.1).

□

Corollary 4.1. *Subgroups of free groups are free.*

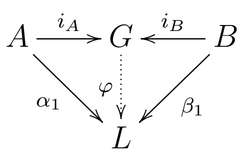
Proof. Let $F(S)$ be a free group with basis S. Then $F(S)$ acts freely on its Cayley graph $\Gamma(S, G)$ which is a tree. So any subgroup H of $F(S)$ acts freely on $\Gamma(S, G)$ hence by the previous theorem H is free. □

4.4 Amalgams

The construction of amalgams allows us to 'combine' some given groups and construct new groups. Let A, B be two groups which have two isomorphic subgroups, that is there are embeddings $\alpha : H \to A$, $\beta : H \to B$. Intuitively the amalgam of A, B over H is a group that contains copies of A, B which intersect along H and no other relations are imposed. To simplify notation we pose $\alpha(h) = h$, $\beta(h) = \bar{h}$ for all $h \in H$.

One way to define amalgams is via their universal property:

Definition 4.9. We say that a group G is the *amalgamated product* of A, B over H and we write $G = A \ast_H B$ if there are homomorphisms $i_A : A \to G$, $i_B : B \to G$ which agree on H such that for every group L and homomorphisms $\alpha_1 : A \to L$, $\beta_1 : B \to L$ which satisfy $\alpha_1(h) = \beta_1(\bar{h})$, $\forall h \in H$, there is a unique homomorphism $\varphi : G \to L$ such that $\alpha_1 = \varphi \circ i_A$ and $\beta_1 = \varphi \circ i_B$.



The amalgam of A, B over H depends of course on the maps α, β, it is however customary to suppress this on the notation. We note that it is not clear by the definition whether i_A, i_B are injective.

Remark 4.5. Assuming that an amalgam of A, B over H exists it is easy to see that this amalgam is unique using the universal property.

Indeed let G_1, G_2 be two such amalgams and let i_A, i_B, j_A, j_B be the inclusions of A, B in G_1, G_2 respectively. The homomorphisms j_A, j_B induce a homomorphism $j : G_1 \to G_2$ such that $j \circ i_A = j_A$, $j \circ i_B = j_B$. Similarly i_A, i_B induce a homomorphism $i : G_2 \to G_1$. The compositions of these maps induce homomorphisms $G_1 \to G_1$, $G_2 \to G_2$ which are both equal to the identity since they are induced by i_A, i_B and j_A, j_B respectively. So $G_1 \cong G_2$.

We show now that the amalgam of A, B over H exists:

Let $\langle S_1 | R_1 \rangle$, $\langle S_2 | R_2 \rangle$ be presentations of A, B respectively. Without loss of generality we assume that $S_1 \cap S_2 = \emptyset$. Then the amalgam of A, B over H is given by

$$A \underset{H}{*} B = \langle S_1 \cup S_2 | R_1 \cup R_2 \cup \{h = \bar{h} \, : \, h \in H\} \rangle$$

Exercise 24. Show that if the groups A and B are residually finite then their free product $A * B$ is also residually finite.

Exercise 25. The fundamental group of a surface group of genus 2 has a presentation:

$$G = \langle a, b, c, d \mid [a, b] = [c, d] \rangle$$

where we denote by $[a, b] := aba^{-1}b^{-1}$ the commutator of a and b. Show that G is an amalgamated free product of two copies of F_2 over an infinite cyclic subgroup.

Exercises 20–25 are due on Tuesday Feb 23th.

Indeed it is easy to see that this group satisfies the universal property of the definition.

When $H = \{1\}$ then the amalgam does not depend on the maps α, β and it is called *free product* of A, B; we denote this by $A * B$. We remark that $F_2 = \mathbb{Z} * \mathbb{Z}$. We would like to describe the elements of $A \underset{H}{*} B$ by 'words'. To simplify notation we identify H with its image in A, B. If $a \in A$ (or $b \in B$) we will denote the corresponding element of G by a (b) rather than $i_A(a)$ ($i_B(b)$). It is important to distinguish whether we see a as an element of A or of G since, a priori, it is possible that $a_1 = a_2$ in G while $a_1 \neq a_2$ in A (and similarly for B).

Let A_1, B_1 be sets of right coset representatives of H in A, B respectively, such that $1 \in A_1, 1 \in B_1$. So we have the 1-1 and onto maps:

$$H \times A_1 \to A, (h, a) \mapsto ha, \; H \times B_1 \to B, (h, b) \mapsto hb$$

A *reduced word* of the amalgam $A \underset{H}{*} B$ is a word of the form $(h, s_1, ..., s_n)$ where $h \in H$, $s_i \in A_1 \cup B_1$, $s_i \neq 1$ for every i and the s_i's alternate from A_1 to B_1. That is for all i, $s_i \in A_1 \implies s_{i+1} \in B_1$, $s_i \in B_1 \implies s_{i+1} \in A_1$. If $(h, s_1, ..., s_n)$ is a reduced word we associate to this the group element $hs_1...s_n \in A \underset{H}{*} B$. We say that the *length* of the reduced word $(h, s_1, ..., s_n)$ is n.

Theorem 4.3. *(Normal forms) Each $g \in G = A \underset{H}{*} B$ is represented by a unique reduced word.*

Proof. Any element $g \in G$ can be written as a product of the form

$$g = a_1 b_1 ... a_n b_n, \; a_i \in A, b_i \in B$$

By successive reductions we arrive at a reduced word, so we can represent g by a reduced word. We show now that this word is unique.

Let X be the set of all reduced words. We define an action of G on X. We recall that an action is a homomorphism $G \to Symm(X)$. By the universal property of the amalgam it is enough to define homomorphisms (actions) $A \to Symm(X)$, $B \to Symm(X)$ which agree on H. We define the action of A. If $a \in H$ and $(h, s_1, ..., s_n)$ is a reduced word we define

$$a \cdot (h, s_1, ..., s_n) = (ah, s_1, ..., s_n)$$

If $a \in A \setminus H$ and $(h, s_1, ..., s_n)$ a reduced word then there are two cases.
1st case: $s_1 \in B$. Then $ah = h_1 s$ for some $h_1 \in H$, $s \in A_1$ and we define

$$a \cdot (h, s_1, ..., s_n) = (h_1, s, s_1, ..., s_n)$$

2nd case: $s_1 \in A$. Then $ahs_1 = h_1 s$ for some $h_1 \in H$, $s \in A_1$. If $s \neq 1$ we define

$$a \cdot (h, s_1, ..., s_n) = (h_1, s, s_2, ..., s_n)$$

while if $s = 1$ we define

$$a \cdot (h, s_1, ..., s_n) = (h_1, s_2, ..., s_n)$$

One sees easily that if $a_1, a_2 \in A$ then

$$(a_1a_2)\cdot(h, s_1, ..., s_n) = a_1\cdot(a_2\cdot(h, s_1, ..., s_n))$$

so we have indeed an action. We define the action of B similarly. So we have an action of G on X. Now if $g = hs_1...s_n$ where $(h, s_1, ..., s_n)$ is a reduced word then

$$g\cdot(1) = (h, s_1, ..., s_n)$$

It follows that the reduced word representing g is unique. □

Corollary 4.2. *The homomorphisms $i_A : A \to A \underset{H}{*} B$, $i_B : B \to A \underset{H}{*} B$ are injective. So we can see A, B as subgroups of $A \underset{H}{*} B$.*

From now on we may identify elements of $A \underset{H}{*} B$ with reduced words.

Corollary 4.3. *Let $A \underset{H}{*} B$ be an amalgamated product. If $(g_1, ..., g_n)$ is such that $g_i \in A \cup B$, $g_i \notin H$ for any $i > 1$ and the g_i's alternate between A and B then $g_1g_2...g_n \neq 1$ in $A \underset{H}{*} B$.*

Proof. Starting from g_n we replace successively the g_i's by elements of the form hs_i where s_i lies in $A_1 \cup B_1 \setminus 1$ (right coset representatives of H). Eventually we arrive at a reduced word representing $g_1g_2...g_n$ which has length n if $g_1 \notin H$, and $n - 1$ if $g_1 \in H$. It follows that $g_1g_2...g_n \neq 1$. □

Exercise 26. Show that if $A \neq H \neq B$ then the center of $A \underset{H}{*} B$ is contained in H.

If $hs_1...s_n$ is a reduced word (element) in $A \underset{H}{*} B$ then we say that n is the length of this word. We say that a reduced element $hs_1...s_n$ $(n > 1)$ is *cyclically reduced* if s_1s_n is reduced.

Proposition 4.1. *1. Every element of $A \underset{H}{*} B$ is conjugate either to a cyclically reduced element or to an element of A or B.*

2. Every cyclically reduced element has infinite order.

Proof. 1. If $g = hs_1...s_n$ is not cyclically reduced then g is conjugate to an element of length $n - 1$. We repeat till we arrive either at a reduced word or an element of A or B.

2. If g is cyclically reduced of length n then g^k has length kn so $g^k \neq 1$. □

Proposition Given a finite group G acting by isometries on a metric tree T, there always exists a point $p \in T$ which is fixed under the action of G.

Proof: Pick a point $x \in T$ and let $X := Gx$ be its orbit. Let $T' := Conv(X)$ be the convex hull of that orbit. T' is a finite sub-graph of T, and hence a tree. This tree is finite and therefore has leaves (=univalent vertices). Each leaf of T' is an element of X. By G-symmetry, each element of X is therefore a leaf of T'.

Now we consider the following dynamical process. We let each point of X flow inwards at constant speed. This produces a 1-parameter family of shrinking sub-trees of T. At any give time instant, the set X maps to the set of leaves of that sub-tree. The process terminates when all the leaves crash together. That's the desired G-fixed point. . □

Exercise 4.1. (Corollary of the above proposition) If K is a finite subgroup of $A \underset{H}{*} B$ then K is contained in a conjugate of either A or B.

Example 4.1. (Higman) Let

$$A = \langle a, s | sas^{-1} = a^2 \rangle$$

$$B = \langle b, t | tbt^{-1} = b^2 \rangle$$

Then $< a > \cong < b > \cong \mathbb{Z}$ so we may form the amalgam

$$G = A \underset{<a>=<b>}{*} B = \langle a, s, t | sas^{-1} = a^2,\, tat^{-1} = a^2 \rangle$$

The group G is not Hopf.

Proof. We define $\varphi : G \to G$ by

$$\varphi(a) = a^2,\, \varphi(s) = s,\, \varphi(t) = t$$

It is easy to see that the relations are satisfied so φ is a homomorphism. Moreover $\varphi(t^{-1}at) = t^{-1}a^2t = a$ so φ is onto. On the other hand $\varphi(s^{-1}ast^{-1}a^{-1}t) = s^{-1}a^2st^{-1}a^{-2}t = aa^{-1} = 1$. As $s^{-1}as \in A- < a >$, $t^{-1}a^{-1}t \in B- < b >$ (check this! see example 3.1) the element $(s^{-1}as)(t^{-1}a^{-1}t)$ has length 2 in the amalgam $A \underset{<a>=<b>}{*} B$ so $ker\, \varphi \neq 1$.

□

4.5 Actions of amalgams on Trees

Definition 4.10. Let G be a group acting without inversions on a tree T. A subtree $S \subset T$ is called a *fundamental domain* of the action if the standard projection $p : S \to T/G$ is an isomorphism.

Theorem 4.4. *Let $G = A \underset{H}{*} B$ be an amalgamated product. Then G acts on a tree T with fundamental domain an edge $e = [P, Q]$ so that $stab(P) = A$, $stab(Q) = B$, $stab(e) = H$.*

Proof. We define the vertices of T to be

$$V(T) = G/A \sqcup G/B = \{gA : g \in G\} \sqcup \{gB : g \in G\}$$

and the edges

$$E(T) = G/H \sqcup \overline{G/H}$$

We define $o(gH) = gA$, $t(gH) = gB$. The action of G is the obvious one: If $g' \in G$ then

$$g' \cdot gA = (g'g)A, \quad g' \cdot gB = (g'g)B, \quad g' \cdot gH = (g'g)H$$

Clearly G acts transitively on the set of geometric edges of T and there are two orbits of vertices. T is connected since if $g = hs_1...s_n$, (reduced word of length n) then there is an edge joining gA to $hs_1...s_{n-1}B$ if $s_n \in A$. Otherwise there is an edge joining gB to $hs_1...s_{n-1}A$. Since gA, gB are joined by an edge we see by induction on the length of g that every vertex gA or gB can be joined by a path to $1 \cdot A$, so T is connected.

We note that if p a path starting and ending at $1 \cdot A$ then necessarily the length of p is even. Suppose now that p is a reduced path of length $2n$ starting at $1 \cdot A$. We claim that the vertices of p are of the form

$$1 \cdot A, a_1B, a_1b_1A, ..., a_1b_1...a_nb_nA$$

where $a_i \in A - H$ for $i > 1$ and $b_i \in B - H$ for all i. Indeed this is easily proven inductively as if e.g. $a_1b_1...a_kb_kA, gB$ are successive vertices then $gb = a_1b_1...a_kb_ka$ for some $a \in A, b \in B$. However $gbB = gB$ so we may denote the vertex gB by $a_1b_1...a_kb_kaB$ (in other words $a_{k+1} = a$). Note also that if $a \in H$ then $gB = a_1b_1...a_kB$ so the path is not reduced. It follows that the length of $a_1b_1...a_nb_n$ is at least $2n - 1$ so $1A \neq a_1b_1...a_nb_nA$, ie there are no reduced paths starting and ending at A. Similarly there are no reduced paths starting and ending at B. As every vertex of T lies either in the orbit of A or of B we conclude that T has no circuits.

Therefore T is a tree. □

Corollary 4.4. *Let F be a subgroup of $A \underset{H}{*} B$ which intersects trivially any conjugate of A or B. Then F is free.*

Proof. Let T be the tree constructed in the theorem 4.4. The stabilizers of vertices of T are conjugates of A, B. Since F intersects trivially the conjugates of A, B, F acts freely on T. By theorem 4.2 F is a free group. □

Proposition 4.2. *Let $G = A * B$. Then the kernel of the natural map $\varphi : A * B \to A \times B$ is free.*

Proof. If $R = ker\,\varphi$ then R intersects trivially all conjugates of A, B since these map isomorphically to their image. By corollary 4.4 R is free. □

Corollary 4.5. *If A, B are finite groups then $A * B$ has a finite index subgroup which is free.*

Theorem 4.4 has a converse:

Theorem 4.5. *Assume that G acts on a tree T with fundamental domain an edge $e = [P, Q]$. If $stab(P) = A$, $stab(Q) = B$, $stab(e) = H$ then $G = A \underset{H}{*} B$.*

Proof. The inclusions $A \to G$, $B \to G$ induce a homomorphism

$$\varphi : A \underset{H}{*} B \to G$$

We consider the subgroup $G' =< A, B >$. We remark that $G'e$ is connected. If for some $g_1 \in G$, $g_2 \in G'$ we have that $g_1 P = g_2 P$ then $g_2^{-1} g_1 \in A$ so $g_1 \in G'$. The same holds if $g_1 Q = g_2 Q$. So $(G - G')e \cap G'e = \emptyset$. On the other hand $T = Ge = (G - G')e \cup G'(e)$ and T is connected. It follows that $G - G' = \emptyset$ and $G = G'$. Therefore φ is onto. We show now that φ is 1-1. Let $g = hs_1...s_n$ (reduced word in $A \underset{H}{*} B$) be an element of $ker\,\varphi$. Clearly $n > 1$.

We distinguish now two cases. If $s_n \in A$ then we see by induction on n that $d(gQ, Q) = n$ if n is even and $d(gQ, Q) = n + 1$ if n is odd. Similarly if $s_n \in B$ we see inductively that $d(gP, P) = n$ if n is even and $d(gP, P) = n + 1$ if n is odd. It follows that $g \neq 1$ in G so φ is 1-1.

□

4.6 HNN extensions

Definition 4.11. Let G be a group, A a subgroup of G and $\theta : A \to G$ a monomorphism. The *HNN-extension* of G over A with respect to θ is the group

$$G \underset{A}{*} = \langle G* < t > |tat^{-1} = \theta(a), \forall a \in A\rangle = G* < t > / \langle\langle tat^{-1}\theta(a)^{-1}, a \in A\rangle\rangle$$

The letter t is called stable letter of the HNN-extension.

We remark that if $\langle S|R\rangle$ is a presentation of G then a presentation of $G \underset{A}{*}$ is given by

$$\langle S \cup \{t\}|R \cup \{tat^{-1} = \theta(a), \forall a \in A\}\rangle$$

Let A_1, A_2 be sets of right coset representatives of $A, \theta(A)$ in G so that $1 \in A_1, 1 \in A_2$. A *reduced word* of the HNN extension $G \underset{A}{*}$ is a word of the form

$$(g_0, t^{\epsilon_1}, g_1, t^{\epsilon_2}, ..., t^{\epsilon_n}, g_n)$$

where $\epsilon_i = \pm 1$, $g_0 \in G$, $g_i \in A_1$ if $\epsilon_i = 1$, $g_i \in A_2$ if $\epsilon_i = -1$ and $g_i \neq 1$ if $\epsilon_{i+1} = -\epsilon_i$.

If $(g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n)$ is a reduced word we associate to this the group element $g_0 t^{\epsilon_1} ... t^{\epsilon_n} g_n \in G \underset{A}{*}$.

Theorem 4.6. *(Normal forms) Each $g \in G \underset{A}{*}$ is represented by a unique reduced word.*

Proof. It is easy to see by successive reductions that any $g \in G \underset{A}{*}$ can be represented by some reduced word. We show now that this representation is unique. We use a similar argument as for amalgamated products. Let X be the set of all reduced words. We define an action of $G \underset{A}{*}$ on X. To do this it is enough to define actions of G and $< t >$ and show that the relations are satisfied. Let $g \in G$ and $(g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n)$ a reduced word. We define

$$g \cdot (g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) = (gg_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n)$$

Clearly this defines an action of G on X. We define now the action of t.

$$t \cdot (g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) = \begin{cases} (\theta(a), t, g_0', t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 = ag_0',\ 1 \neq g_0' \in A_1 \\ (\theta(g_0), t, 1, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 \in A, \epsilon_1 = 1 \\ (\theta(g_0)g_1, t^{\epsilon_2}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 \in A, \epsilon_1 = -1 \end{cases}$$

So t defines a 1-1 map $X \to X$. We show that this map is onto. If $(g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) \in X$ then

$$(g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) = \begin{cases} t \cdot (1, t^{-1}, g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 \notin \theta(A) \\ t \cdot (ag_1, t^{\epsilon_2}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 = \theta(a),\ a \in A, \epsilon_1 = 1 \\ t \cdot (a, t^{-1}, 1, t^{\epsilon_1}g_1, t^{\epsilon_2}, ..., t^{\epsilon_n}, g_n) & \text{if } g_0 = \theta(a),\ a \in A, \epsilon_1 = -1 \end{cases}$$

So t gives an element of $Symm(X)$. In other words we have defined homomorphisms $G \to Symm(X)$, $< t > \to Symm(X)$. It follows that there is an extension of these homomorphisms to $G * < t > \to Symm(X)$. We verify that tat^{-1} and $\theta(a)$ $(a \in A)$ act in the same way. So we have an action of $G \underset{A}{*}$ on X. If $g_0 t^{\epsilon_1} ... t^{\epsilon_n} g_n \in G \underset{A}{*}$ is an element corresponding to a reduced word then

$$g_0 t^{\epsilon_1} ... t^{\epsilon_n} g_n \cdot (1) = (g_0, t^{\epsilon_1}, ..., t^{\epsilon_n}, g_n)$$

So each element is represented by a unique reduced word. □

Corollary 4.6. *The group G embeds in $G \underset{A}{*}$.*

Corollary 4.7. *Let $G \underset{A}{*}$ be an HNN extension. Let $(g_0, t^{\epsilon_1}, g_1, t^{\epsilon_2}, ..., t^{\epsilon_n}, g_n)$ be such that $g_i \in G$ for all i, $\epsilon_i = \pm 1$, $g_i \notin A$ if $\epsilon_i = 1$ and $\epsilon_{i+1} = -1$, $g_i \notin \theta(A)$ if $\epsilon_i = -1$ and $\epsilon_{i+1} = 1$, then $g_0 t^{\epsilon_1} g_1 ... t^{\epsilon_n} g_n \neq 1$ in $G \underset{A}{*}$.*

Proof. Starting from g_n we replace successively the g_i's by elements of the form hs_i where s_i lies in $A_1 \cup A_2$ (right coset representatives of $A, \theta(A)$) so that eventually we arrive at a reduced word representing $g_0 t^{\epsilon_1} g_1 ... t^{\epsilon_n} g_n$ which has length n, so $g_0 t^{\epsilon_1} g_1 ... t^{\epsilon_n} g_n \neq 1$. □

Definition 4.12. If a group G is an amalgam $G = A \underset{H}{*} B$ (with $A \neq H \neq B$) or an HNN-extension $G = A \underset{H}{*}$ then we say that G *splits* over H.

Example 4.2. (Higman, Neumann and Neumann) Any countable group embeds in a group with 2 generators.

Proof. Let $C = \{c_0 = e, c_1, c_2, ...\}$ be a countable group. We remark that the set of elements $S = \{a^n b a^{-n} : n \in \mathbb{N}\}$ forms a basis for free subgroup of the free group of rank 2, $F = F(a, b)$. Consider the group

$$H = F * C$$

The subgroups

$$A = \langle a^n b a^{-n} : n \in \mathbb{N} \rangle, \; B = \langle c_n b^n a b^{-n} : n \in \mathbb{N} \rangle$$

are both free of infinite rank by the normal form theorem for free products (theorem 4.3). Let $\phi : A \to B$ be the isomorphism given by $\phi(a^n b a^{-n}) = c_n b^n a b^{-n}$. Consider the HNN extension

$$G = H \underset{A}{*} = \langle H * < t > | t a^n b a^{-n} t^{-1} = c_n b^n a b^{-n}, \forall n \in \mathbb{N} \rangle$$

Clearly C embeds in G (normal form theorem for HNN extensions). Morover

$$ta^nba^{-n}t^{-1} = c_nb^nab^{-n} \implies c_n = ta^nba^{-n}t^{-1}b^na^{-1}b^{-n}$$

so G is generated by t, a, b, and in fact since $tbt^{-1} = a$, G is generated by a, t. $\square$

Chapter 5

Graphs of Groups

5.1 Fundamental groups of graphs of groups

Definition 5.1. A *graph of groups* (G,Y) consists of a connected graph Y and a map G such that

1. G assigns a group G_v to every vertex $v \in V(Y)$ and a group G_e to every edge $e \in E(Y)$, so that $G_e = G_{\bar{e}}$.
2. For each edge group G_e there is a monomorphism $\alpha_e : G_e \to G_{t(e)}$.

Graphs of groups occur naturally in the context of group actions on trees. If a group G acts on a tree T without inversions then we can form the quotient graph $Y = T/G$. We note that there is a projection $p : T \to T/G$.

To each vertex $v \in Y$ (or edge $e \in Y$) we associate a group G_v (G_e) where G_v is the stabilizer of a vertex in $p^{-1}(v)$ (edge in $p^{-1}(e)$). Note that all stabilizers of vertices in $p^{-1}(v)$ are isomorphic and the same holds for edges. If the vertex $v' \in p^{-1}(v)$ is an endpoint of the edge $e' \in p^{-1}(e)$ in T we have a monomorphism (inclusion) $stab(e') \to stab(v')$ and this is how we obtain the monomorphism $G_e \to G_v$. We will associate graphs of groups to actions more formally later, here we mention this as a source of examples and in order to put this definition in context.

Definition 5.2. The *path group* of the graph of groups (G,Y) is the group

$$F(G,Y) = \langle \mathop{*}_{v\in V(Y)} G_v \mathop{*}_{e\in E(Y)} \langle e\rangle | \bar{e} = e^{-1},\, e\alpha_e(g)e^{-1} = \alpha_{\bar{e}}(g),\ \forall e \in E(Y),\, g \in G_e \rangle$$

If $G_v = \langle S_v | R_v \rangle$ then a presentation of $F(G,Y)$ is given by

$$\langle \underset{v\in V(Y)}{\cup} S_v \cup \{e \in E(Y)\} | \underset{v\in V(Y)}{\cup} R_v, \bar{e} = e^{-1}, \, e\alpha_e(g)e^{-1} = \alpha_{\bar{e}}(g), \; \forall e \in E(Y), \, v \in V(Y), \, g \in G_e \rangle$$

Remarks.

1. If $G_v = \{1\}$ for all $v \in V(Y)$ then $F(G,Y) = F(E^+(Y))$ (the free group with basis the geometric edges of Y).

2. If $G_e = \{1\}$ for all $e \in E(Y)$ then $F(G,Y) = \underset{v\in V(Y)}{*} G_v * F(E^+(Y))$.

3. There is an epimorphism $F(G,Y) \to F(E^+(Y))$ defined by sending all $g \in G_v$ (for all v) to 1.

Definition 5.3. A *path* c in the graph of groups (G,Y) is a sequence

$$c = (g_0, e_1, g_1, e_2, ..., g_{n-1}, e_n, g_n)$$

such that $t(e_i) = o(e_{i+1})$ and $g_i \in G_{o(e_{i+1})} = G_{t(e_i)}$ for all i. If

$$v_0 = o(e_1), v_1 = o(e_2) = t(e_1), ..., v_n = t(e_n)$$

we say that c is a path from v_0 to v_n and $(v_0, ..., v_n)$ is the sequence of vertices of the path c. We define $|c|$ to be the element of the path group: $|c| = g_0 e_1 g_1 .... e_n g_n$.

If $a_0, a_1 \in V(Y)$ we define

$$\pi[a_0, a_1] = \{|c| : c \text{ path from } a_0 \text{ to } a_1\}$$

If $a_0, a_1, a_2 \in V(Y)$ and $\gamma \in \pi[a_0, a_1]$, $\delta \in \pi[a_1, a_2]$ then $\gamma \cdot \delta \in \pi[a_0, a_2]$.

Proposition 5.1. *Let (G,Y) be a graph of groups. The set $\pi[a_0, a_0]$ ($a_0 \in V(Y)$) is a subgroup of $F(G,Y)$. We call this fundamental group of the graph of groups (G,Y) with base point a_0 and we denote it by $\pi_1(G,Y,a_0)$.*

Given a graph of groups one can define a topological space as follows (the topological space is not unique, but its fundamental group is independent of the choices). Pick for every vertex group G_v a space X_v whose fundamental group is G_v. Then pick, for every edge group G_e a space Y_e whose fundamental group is G_e. For every edge $v \overset{e}{-} w$ of the graph, pick continuous maps $f_{e,v} : Y_e \to X_v$ and $f_{e,w} : Y_e \to X_w$ that induce at the level of π_1 the homomorphisms $G_e \to G_v$ and $G_e \to G_w$ given by the graph of groups. Then we build a space as follows:

First take the disjoint union of all the X_v's. Then glue on top of that a copy of

$Y_e \times [0,1]$ for every edge e. The attaching maps $Y_e \times \partial[0,1] \to \coprod_v X_v$ are given by $f_{e,v} \sqcup f_{e,w}$. The the fundamental group of the graph of groups is the fundamental group (in the sense of topology) of that space we constructed.

Special cases: When the graph consists of two vertices and a single edge, then the fundamental group of the graph of groups is just an amalgamated free product. When the graph consists of a single vertex and a single loop, then the fundamental group of the graph of groups is an HNN extension. In that way, we see that both amalgamated free products and HNN extensions are special cases of the notion of a fundamental group of a graph of groups.

Recall that we say that a subgroup H of G is *separable* if it is equal to the intersection of all the finite index subgroups of G containing it.

Exercise 27. Show that every finitely generated subgroup of F_n (the free group of rank n) is separable.
Hint: Use the correspondence between covers of $\bigvee_{i=1}^n S^1$ and subgroups of F_n.
(Which covers correspond to finitely generated subgroups? Which covers correspond to finite index subgroups?)

Exercise 28. Show that if $G = A *_C B$ and $[A : C] \geq 3$ and $[B : C] \geq 2$ then G has a free subgroup of rank 2.

Exercise 29. i) Let G be a finitely generated group such that $G = A *_C B$ where $[A : C] = [B : C] = 2$, and A and B are finite. Show that G has a finite index subgroup isomorphic to $\mathbb{Z}$.
ii) Show that if $G = A*_A$ and A is finite, then G has a finite index subgroup isomorphic to $\mathbb{Z}$.

Exercise 30. Let G be a finitely presented group. Show that the HNN-extension $G*_A$ is finitely presented if and only if A is finitely generated.
Hint: If A is not finitely generated, write it as an increasing union $A = \bigcup A_n$ and consider the groups $G*_{A_n}$. Show using normal forms (Thm 4.6) that the natural homomorphisms $G*_{A_n} \to G*_{A_{n+1}}$ are not isomorphisms.

Exercise 31. Let G be a group acting on a tree T. Show that if $g \in G$ fixes no point of T (either a vertex of a midpoint of an edge), then there is a line $L \subset T$ such that g acts on L by translations.

Exercise 32. Let $G := \mathbb{Z}^2 * \mathbb{Z}^2$. Describe a space whose fundamental group is G. Show that G can be written non-trivially as the fundamental group of a graph of groups, where the graph has two vertices and three edges.

Exercises 26–32 are due on Tuesday March 1st.

Proof. It is enough to show that every element of $\pi[a_0, a_0]$ has an inverse in $\pi[a_0, a_0]$. If $c = (g_0, e_1, g_1, e_2, ..., g_{n-1}, e_n, g_n)$ is a path from a_0 to a_0 then

$$|c|^{-1} = g_n^{-1}\bar{e}_n....\bar{e}_1 g_0^{-1} \in \pi[a_0, a_0]$$

□

Definition 5.4. Let (G, Y) be a graph of groups and let T be a maximal tree of Y. We define the *fundamental group* of (G, Y) with respect to T, $\pi_1(G, Y, T)$ to be the quotient group

$$\pi_1(G, Y, T) = F(G, Y)/\langle\langle\{e, e \in T\}\rangle\rangle$$

We have the obvious quotient map $q : F(G, Y) \to \pi_1(G, Y, T)$.

Proposition 5.2. *The restriction of q to $\pi_1(G, Y, a_0)$ is an isomorphism, so*

$$\pi_1(G, Y, a_0) \cong \pi_1(G, Y, T)$$

Proof. We would like to define a homomorphism $f : \pi_1(G, Y, T) \to \pi_1(G, Y, a_0)$. Let $a \in V(Y)$ and $(e_1, ..., e_n)$ a geodesic path on T from a_0 to a. We set $g_a = e_1...e_n \in F(G, Y)$. If $a = a_0$ we set $g_a = 1$.

If e is an edge with $o(e) = a$, $t(e) = b$ we define

$$f(e) = g_a e g_b^{-1} \in \pi_1(G, Y, a_0)$$

Clearly if $e \in T$ then $f(e) = 1$ so this makes sense.

If $g \in G_a$ we define

$$f(g) = g_a g g_a^{-1} \in \pi_1(G, Y, a_0).$$

If e is an edge and $o(e) = P$, $t(e) = Q$ then

$$f(e\alpha_e(g)e^{-1}) = (g_P e g_Q^{-1})(g_Q \alpha_e(g) g_Q^{-1})(g_Q e g_P^{-1}) = g_P e \alpha_e(g) e^{-1} g_P^{-1} = g_P \alpha_{\bar{e}}(g) g_P^{-1}$$

and

$$f(\alpha_{\bar{e}}(g)) = g_P \alpha_{\bar{e}}(g) g_P^{-1}$$

so the relations are satisfied for all $e \in E(Y)$. It follows that f is a homomorphism.

Also $q \circ f(g) = g$ for all $g \in G_v$, $v \in V(T)$ and $q \circ f(e) = e$ for all $e \notin T$. So $q \circ f = id$.

We calculate now $f \circ q$. Let $(g_0, e_1, ..., e_n, g_n)$ be a path such that $g_0, g_n \in G_{a_0}$. If $e_i = [P_{i-1}, P_i]$ then $q(g_i) = g_i$ and $f(g_i) = g_{P_i} g_i g_{P_i}^{-1}$. Also $q(e_i) = e_i$ and $f(e_i) = g_{P_{i-1}} e_i g_{P_i}^{-1}$. We remark also that $g_{P_0} = g_{P_n} = g_{a_0} = 1$.

So

$$f \circ q(g_0 e_1 ... e_n g_n) = g_0 (e_1 g_{P_1}^{-1}) g_{P_1} ... g_{P_{n-1}}^{-1} (g_{P_{n-1}} e_n g_n) = g_0 e_1 ... e_n g_n$$

so $f \circ q = id$. □

Corollary 5.1. *The fundamental group of the graph of groups $\pi_1(G, Y, a_0)$ does not depend on the basepoint a_0.*

Exercise 33. This exercise consists of two parts which should be carried our separately. Once Part 1 is done, you may no longer look at your course notes. So be sure that you really understand the proof before you declare yourself ready to switch to Part 2.

Part 1:
Read and understand the statement and the proof of Theorem 4.6. (about normal forms for HNN extensions).

Part 2:
Write down a complete proof of this theorem in your own words.

Exercise 34. Read ahead, and try to understand the notion of quasi-isometry.

Exercises 33–34 are due on Tuesday March 8th.

5.2 Reduced words

Definition 5.5. Let (G, Y) be a graph of groups and let $c = (g_0, e_1, g_1, e_2, ..., g_{n-1}, e_n, g_n)$ be a path. We say that c is *reduced* if:

1) $g_0 \neq 1$ if $n = 0$.

2) For every i if $e_{i+1} = \bar{e}_i$ then $g_i \notin \alpha_{e_i}(G_{e_i})$.

If c is a reduced path we say that $g_0 e_1 .... e_n g_n$ is a reduced word. We denote by $|c|$ the element of $F(G, Y)$ represented by the word $g_0 e_1 .... e_n g_n$.

Theorem 5.1. *If c is a reduced path then $|c| \neq 1$ in $F(G,Y)$. In particular for any vertex $v \in V(Y)$ the homomorphism $G_v \to F(G,Y)$ is injective.*

Proof. We prove first the theorem for finite graphs by induction on the number of edges. If Y is a single vertex there is nothing to prove. Otherwise we distinguish two cases:

Case 1: $Y = Y' \cup \{e\}$ where Y' is a connected graph and $v = t(e) \notin Y'$. In this case

$$F(G,Y) = (F(G,Y') * G_v) \underset{\alpha_e(G_e)}{*}$$

and a reduced word on $F(G,Y)$ corresponds to a reduced word in the HNN extension which is non trivial by corollary 4.7.

Case 2: $Y = Y' \cup \{e\}$ where Y' is a connected graph and $o(e), t(e) \in Y'$. In this case

$$F(G,Y) = F(G,Y') \underset{\alpha_e(G_e)}{*}$$

and a reduced word on $F(G,Y)$ corresponds to a word in the HNN extension which is non trivial by corollary 4.7.

This proves the theorem in case Y is finite. If Y is infinite and a reduced word w is equal to 1 in $F(G,Y)$ then it is equal to a product of finitely many conjugates of relators of $F(G,Y)$. However these relators involve only group elements and edge generators lying in a finite subgraph Y_1. By taking Y_1 big enough we may assume that the conjugating elements also lie in Y_1. It follows that $w = 1$ in $F(G,Y_1)$ which is a contradiction since w is a reduced word and Y_1 is finite.

□

Corollary 5.2. *For any vertex $v \in V(Y)$ the homomorphism $G_v \to \pi_1(G,Y,T)$ is injective.*

Proof. The homomorphism $G_v \to \pi_1(G,Y,v)$ is injective since $\pi_1(G,Y,v)$ is a subgroup of $F(G,Y)$ and if $1 \neq g \in G_v$ g is a reduced word in $F(G,Y)$ hence $g \neq 1$. However $\pi_1(G,Y,v) \cong \pi_1(G,Y,T)$ and $g \in G_v$ maps to itself in $\pi_1(G,Y,T)$ so $g \neq 1$ in $\pi_1(G,Y,T)$.

□

Remark 5.1. If Y consists of a single edge $e = [u,v]$ with $u \neq v$ then one sees from the presentation that $\pi_1(G,Y,T) = G_u \underset{G_e}{*} G_v$. If the endpoints of e are equal ($u = v$) then $\pi_1(G,Y,T) = G_v \underset{\alpha_e(G_e)}{*}$ where the homomorphism of the HNN extension $\theta : \alpha_e(G_e) \to G_v$ is given by $\theta(g) = \alpha_{\bar{e}} \circ \alpha_e^{-1}$ and the stable letter is e.

In general if $Y = Y' \cup e$ and $t(v) \notin Y'$ then

$$\pi_1(G,Y,T) = \pi_1(G,Y',T') \underset{G_e}{*} G_v$$

while if $t(v) \in Y'$ then

$$\pi_1(G, Y, T) = \pi_1(G, Y', T) \underset{\alpha_e(G_e)}{*}$$

As we did for amalgams and HNN-extensions we can find a set of words that is in one to one correspondence with the elements of the fundamental group of the graph of groups.

Let (G, Y) be a graph of groups. For each edge $e \in E(Y)$ we pick a set S_e of left coset representatives of $\alpha_{\bar{e}}(G_e)$ in $G_{o(e)}$. We require that $1 \in S_e$.

Definition 5.6. We say that the path $(s_1, e_1, ..., s_n, e_n, g)$ is *S-reduced* if $s_i \in S_{e_i}$ for all i and $s_i \neq 1$ if $e_{i-1} = \bar{e}_i$.

Lemma 5.1. *Let $a, b \in V(Y)$. Then every element of $\pi[a, b]$ is represented by a unique S-reduced path.*

Proof. Existence. For every element $\gamma \in \pi[a, b]$ there is a reduced path $c = (g_1, e_1, g_2, e_2, ..., g_n, e_n, g)$ such that $\gamma = |c|$. We can write $g_1 = s_1 h_1,\ s_1 \in S_{e_1},\ h_1 \in \alpha_{\bar{e}_1}(G_{e_1})$. So

$$g_1 e_1 = s_1 h_1 e_1 = s_1 e_1 \bar{e}_1 h_1 e_1 = s_1 e_1 \alpha_{e_1}(h_1)$$

So we replace c by $(s_1, e_1, \alpha_{e_1}(h_1) g_2, e_2, ..., e_n, g_n)$ and we continue similarly replacing $\alpha_{e_1}(h_1) g_2$ and so on till we arrive at an S-reduced path c' such that $|c'| = \gamma$.

Uniqueness. Let

$$c = (s_1, e_1, ..., s_n, e_n, g),\ \ c' = (t_1, y_1, ..., t_k, y_k, h)$$

be S-reduced paths such that $|c| = |c'|$. Then

$$s_1 e_1 .... s_n e_n g = t_1 y_1 .... t_k y_k h \Rightarrow h^{-1} y_k^{-1} ... y_1^{-1} t_1^{-1} s_1 e_1 .... s_n e_n g = 1$$

Obviously this word is not reduced so $y_1 = e_1$ and $t_1^{-1} s_1 \in \alpha_{\bar{e}_1}(G_{e_1})$. Since t_1, s_1 are left coset representatives of $\alpha_{\bar{e}_1}(G_{e_1})$ we have $t_1 = s_1$. So $y_1^{-1} t_1^{-1} s_1 e_1 = 1$. Continuing in the same way we see that all corresponding elements are equal so $c = c'$.

□

5.3 Graphs of groups and actions on Trees

Let (G, Y) be a graph of groups. We will show in this section that the fundamental group of this graph of groups acts on a tree T so that the quotient graph of this action is isomorphic to Y.

The construction of T resembles the construction of the universal cover in topology. The universal cover $\tilde{X}$ of a space X is defined using the paths of X modulo an equivalence relation (homotopy). Here we do something similar: we consider paths in the graph of groups. The group elements on the paths account for the branching of the tree. A trivial case which illustrates this point is the case of a $\mathbb{Z}_2$ action on a tree with 2 edges fixing the vertex in the middle and permuting the 2 edges. The quotient space is just a single edge, so topologically it is the universal cover of itself. However we can recover the original 2-edge tree using the $\mathbb{Z}_2$ stabilizer of the middle vertex.

Let $a_0 \in Y$. We consider the set of paths in (G, Y):

$$\pi[a_0, a] = \{|c| : c \text{ path from } a_0 \text{ to } a\}$$

We define an equivalence relation in $\pi[a_0, a]$: $|c_1| \sim |c_2|$ if $|c_1| = |c_2|g$ for some $g \in G_a$. We define then

$$V(T) = \bigcup_{a \in V(Y)} \pi[a_0, a]/\sim$$

We remark that an element of $\pi[a_0, a]/\sim$ corresponds to a unique S-reduced path of the form: $(s_1, e_1, ..., s_n, e_n)$ where $t(e_n) = a$ and $o(e_1) = a_0$. Indeed note that

$$|(s_1, e_1, ..., s_n, e_n)| \sim |(s_1, e_1, ..., s_n, e_n, g)| \ \ (g \in G_a)$$

So we may identify the vertices of T with S-reduced paths of the form $(s_1, e_1, ..., s_n, e_n)$. An edge of T now is given by a pair of S-reduced paths that differ by an edge of Y:

$$\{(s_1, e_1, ..., s_n, e_n), \ (s_1, e_1, ..., s_n, e_n, s_{n+1}, e_{n+1})\}$$

Clearly T is connected since (1) can be joined to any other vertex by a path. Moreover, it follows from lemma 5.1 that if $v \in V(T)$ there is a unique S-reduced path joining $(1), v$. Therefore T is a tree.

We define now the action of $H = \pi_1(G, Y, a_0) = \pi[a_0, a_0]$ on T. If $g \in \pi[a_0, a_0]$ and $v \in \pi[a_0, a]$ then $gv \in \pi[a_0, a]$. So we define $g \cdot [v] = [gv]$ (where we denote by $[v]$ the equivalence class of v in $\pi[a_0, a]/\sim$). This defines an action of H on $V(T)$ since $(g_1 g_2) \cdot [v] = g_1 \cdot (g_2 \cdot [v])$. We note that adjacent vertices go to adjacent vertices under this action so we have an action on T. We remark that if $v_1, v_2 \in \pi[a_0, a]$ then $v_2 v_1^{-1} \in \pi[a_0, a_0]$ and $(v_2 v_1^{-1}) \cdot [v_1] = [v_2]$. It follows that we can identify the vertices of the quotient graph T/H with the vertices of Y. We show now that the edges of the quotient graph T/H correspond to the edges of Y too. Let $e_1 = ([v], [vs_1e]), e_2 = ([v], [vs_2e])$ be two edges of T with $o(e_1) = o(e_2) = [v]$, $s_1, s_2 \in G_{o(e_1)}$. If $g = v(s_2 s_1^{-1})v^{-1}$ we have that $g \in \pi[a_0, a_0]$ and $g \cdot e_1 = e_2$. So both edges lie in the same orbit and this orbit corresponds to the edge $e \in E(Y)$.

We can see further that stabilizers of vertices and edges of T are conjugates of vertex and edge groups of (G, Y). Precisely:

Proposition 5.3. *1. If $[v] \in V(T)$ and $v \in \pi[a_0, b]$ then $stab([v]) = vG_bv^{-1}$.*

2. If $\delta \in E(T)$, $\delta = [[v], [vge]]$ where $e = [a, b]$, $g \in G_a$ then $stab(\delta) = (vg)(\alpha_{\bar{e}}(G_e)(vg)^{-1}$.

Proof. 1. Clearly $vG_bv^{-1} \subset stab([v])$. Assume now that $g \in stab([v])$. Then by the definition of $V(T)$ $gv = vg_b$, $g_b \in G_b$. So $g \in vG_bv^{-1}$. We conclude that $stab([v]) = vG_bv^{-1}$.

2. $stab(\delta) = stab([v]) \cap stab([vge])$. So

$$stab(\delta) = vG_av^{-1} \cap (vge)G_b(vge)^{-1} = v(G_a \cap geG_be^{-1}g^{-1})v^{-1} =$$

$$= (vg)(G_a \cap eG_be^{-1})(vg)^{-1}$$

since $g \in G_a$. We remark that $eG_be^{-1} \cap G_a = \alpha_{\bar{e}}(G_e)$. This is because if $g_b \in G_b$, either eg_be^{-1} is a reduced word and so does not lie in G_a or $g_b \in \alpha_e(G_e)$ and then $eg_be^{-1} \in G_a$. We conclude that

$$stab(\delta) = (vg)(\alpha_{\bar{e}}(G_e)(vg)^{-1}$$

□

We denote the tree T by $(\widetilde{G, Y, a_0})$ and we say that it is the *universal covering tree* of the graph of groups (G, Y).

5.4 Quotient graphs of groups

We showed in the previous section that if $\pi_1(G, Y, a_0)$ is the fundamental group of a graph of groups then $\pi_1(G, Y, a_0)$ acts on a tree T with quotient graph Y. The converse is also true: If a group Γ acts on a tree T with quotient Y, then there is a graph of groups (G, Y) so that $\pi_1(G, Y, a_0) = \Gamma$.

We explain now how to associate a graph of groups (G, Y) to an action $\Gamma \curvearrowright T$ (where T is a tree). We define $Y = T/\Gamma$. We have the projection map $p : T \to Y$. Let $X \subset S \subset T$ be subtrees of T such that $p(X)$ is a maximal tree of Y, $p(S) = Y$ and the map p restricted to S is 1-1 on the set of edges. We introduce some convenient notation: if v, e are respectively a vertex and an edge of Y we write v^X for the vertex of X for which $p(v^X) = v$ and e^S for the edge of S for which $p(e^S) = e$. We define now a graph of groups with Y as underlying graph. If $v \in V(Y)$ we set $G_v = stab(v^X)$. If $e \in E(Y)$

we set $G_e = stab(e^S)$. It remains to define monomorphisms $\alpha_e : G_e \to G_{t(e)}$. For every $x \in V(S)$ we pick $g_x \in \Gamma$ such that $g_x x \in X$. If $x \in X$ we take $g_x = 1$. If $x = t(e^S)$ we define:

$$\alpha_e : G_e \to G_{t(e)}, \text{ by } \alpha_e(g) = g_x g g_x^{-1}$$

In this way we define a graph of groups (G, Y). We define a homomorphism $\varphi : F(G, Y) \to \Gamma$ as follows: $\varphi|_{G_a} = id$ for all $a \in V(Y)$. If $e \in E(Y)$ and $y = o(e^S)$, $x = t(e^S)$ then we define $\varphi(e) = g_y g_x^{-1}$. We verify that the relations are satisfied:

$$\varphi(e\alpha_e(g)e^{-1}) = (g_y g_x^{-1})(g_x g g_x^{-1})(g_y g_x^{-1})^{-1} = g_y g g_y^{-1}$$

and

$$\varphi(\alpha_{\bar{e}}(g)) = g_y g g_y^{-1}$$

So φ is indeed a homomorphism. We note that if $e \in p(X)$ then $\varphi(e) = 1$ so we have in fact a homomorphism

$$\varphi : \pi_1(G, Y, p(X)) = \pi_1(G, Y, a_0) \to \Gamma$$

We have the following:

Theorem 5.2. *The map $\varphi := \pi_1(G, Y, a_0) \to \Gamma$ is an isomorphism. If $\tilde{T}$ is the universal covering tree of (G, Y) then there is a graph morphism $\psi : \tilde{T} \to T$ such that ψ is 1-1 and onto and $\psi(gv) = \varphi(g)\psi(v)$ for all $v \in V(\tilde{T})$, $g \in \pi_1(G, Y, a_0)$.*

We omit the proof of this theorem. What this theorem essentially says is that we can recover the group and the action on the tree by the quotient graph of groups.

We can now understand subgroups of fundamental groups of graphs of groups.

Theorem 5.3. *Let $\Gamma = \pi_1(G, Y, a_0)$ where (G, Y) is a graph of groups. If B is a subgroup of Γ then there is a graph of groups (H, Z) such that $B = \pi_1(H, Z, b_0)$ and for every $v \in V(Z)$, $e \in E(Z)$, $H_v \leq gG_a g^{-1}$, $H_e \leq \gamma G_y \gamma^{-1}$ for some $a \in V(Y)$, $y \in E(Y)$ and $g, \gamma \in \Gamma$.*

Proof. Γ acts on a tree T with quotient graph of groups (G, Y). Since $B \leq \Gamma$, B acts also on T and the vertex and edge stabilizers of B are contained in the vertex and edge stabilizers of Γ. If $Z = T/B$ it is clear that the quotient graph of groups (H, Z) that we obtain from the action of B satisfy the assertions of the theorem. $\square$

Corollary 5.3. *(Kurosh's theorem) Let $G = G_1 * ... * G_n$. If $H \leq G$ then $H = (\underset{i \in I}{*} H_i) * F$ where F is a free group and the H_i's are subgroups of conjugates of the G_j's.*

Proof. G is the fundamental group of a graph of groups with underlying graph a tree with n vertices labeled by $G_1, ..., G_n$ and trivial edge groups. We apply now the previous theorem. □

We mention two important theorems on the structure of finitely presented groups.

We say that a group G is *indecomposable* if it can not be written as a non-trivial free product $G = A * B$.

Theorem 5.4. *(Grushko) Let G be a finitely generated group. There are finitely many indecomposable groups $G_1, ..., G_k$ and $n \geq 0$ such that*

$$G = G_1 * ... * G_k * \mathbb{F}_n$$

Moreover if we have another decomposition of G as

$$G = H_1 * ... * H_m * \mathbb{F}_r$$

where H_i are indecomposable then $m = k$, $r = n$, and after reordering H_i is conjugate to G_i for all i.

Theorem 5.5. *(Dunwoody) Let Γ be a finitely presented group. Then Γ can be written as $\Gamma = \pi_1(G, Y, a_0)$ where (G, Y) is a finite graph of groups such that all edge groups are finite and all vertex groups do not split over finite groups.*

Dunwoody has shown that this last theorem does not generalize to all finitely generated groups.

Chapter 6

Groups as geometric objects

Although geometric methods were used in group theory since its inception it was Gromov in 1984 that set the foundations of modern group theory. His insight was that one can derive many algebraic properties of infinite groups from their 'geometry'. In fact looking at the geometry turned out to be very revealing of the group structure, more so than pure algebraic manipulations. The first section of this chapter will explain what we mean by 'geometry' in this context. Riemannian geometry, even though it inspires many arguments that follow, is useless for studying finitely generated groups. Finitely generated groups are discrete objects with no interesting 'local' geometry. Their true geometry becomes apparent only from 'infinitely far away'. Gromov's insight transformed the field, as by bringing geometry into play, other tools such as analysis, dynamics etc. became available for studying groups.

One of the most convincing demonstrations of the geometric point of view is the theory of hyperbolic groups. This is a class of groups which is generic (in a precise statistical sense 'most' groups are hyperbolic) and which can be studied by geometric methods. The theory of hyperbolic groups unifies the small cancellation theory which has algebraic origin and the deep theory of negatively curved manifolds. We will show in the following sections that the word and conjugacy problem are solvable for hyperbolic groups and we will give an introduction to the geometric tools used to study them.

6.1 Quasi-isometries

We consider in the sequel connected graphs as metric spaces. So if Γ is a connected graph we identify each edge of Γ with the unit interval and the distance of any two points is defined to be the length of the shortest path joining them.

Definition 6.1. If v is a vertex of a graph Γ we define the *degree* of v to be the number of edges incident with v. So $deg(v) = card\,\{e \in E(\Gamma) : o(e) = v\}$. We say that a graph Γ is *locally finite* if every vertex is incident to finitely many edges. A graph is called *regular* if all vertices have the same degree. A subgraph L of Γ is a *bi-infinite geodesic* if it is isometric to $\mathbb{R}$ (where we consider L to be equipped with the metric induced by Γ).

We remark that if Γ is the Cayley graph of a finitely generated group then Γ is a regular locally finite graph.

We recall the definition of the Cayley graph of a group:

Definition 6.2. Let G be a group generated by a finite set S. The Cayley graph of G, $\Gamma = \Gamma(S, G)$, is the graph with vertex set

$$V = \{g : g \in G\}$$

and edge set

$$E = \{(g, gs), g \in G, s \in S\}$$

We can see G as a subset of Γ, so the metric of Γ induces a metric d_S on G, called the *word metric* of G. We remark that

$$d_S(g, e) = \min\{n : g = s_1^{\pm 1} ... s_n^{\pm 1}, s_1, ..., s_n \in S\}$$

In this way we can associate to a finitely generated group G a metric space or view G itself as a metric space. There is a problem however, the graph we defined depends on the generating set S. In general given a group G there is no natural way to pick a generating set S and different generating sets give different graphs (and word metrics) for G!

Example 6.1. Consider the Cayley graphs of $\mathbb{Z}$ equipped with 2 different generating sets: $S_1 = \{1\}$, $S_2 = \{2, 3\}$.

One sees from this example that Cayley graphs for the same group can look completely different. One may remark however that when viewed from ‘far away’ these graphs look similar. Although the ‘local geometry’ of Cayley graphs changes when we change generating sets the ‘large scale’ geometry is preserved.

We make this remark precise by introducing quasi-isometries.

Definition 6.3. A (usually non-continuous) map between metric spaces $f : X \to Y$ is called a *quasi-isometry* if there exist $K \geq 1, A > 0$ such that

- for all $x_1, x_2 \in X$

$$\frac{1}{K} d(x_1, x_2) - A \leq d(f(x_1), f(x_2)) \leq K d(x_1, x_2) + A, \quad \textit{and}$$

- for all $y \in Y$ there is some $x \in X$ such that $d(y, f(x)) \leq A$.

When there is a quasi-isometry $f : X \to Y$ we say that X, Y are quasi-isometric and we write $X \sim Y$.

Example 6.2. 1. $\mathbb{R}$ and $\mathbb{Z}$ are quasi-isometric.

2. Any metric space of finite diameter is quasi-isometric to a point.

Exercises 6.1. 1. Show that $\sim$ is an equivalence relation.

2. Let S_1, S_2 be finite generating sets of a group G. Show that $\Gamma(S_1, G) \sim \Gamma(S_2, G)$.

3. Let T_3, T_4 be the regular trees of degrees, respectively, 3,4. Show that T_3, T_4 are quasi-isometric.

We remark that if a group G is not finitely generated we can not associate a 'geometry' to the group in this way. Indeed if we take as generating set the set of all elements of G the Cayley graph is a bounded metric space, so it is quasi-isometric to a point.

Given $\epsilon, \delta > 0$ a subset N of a metric space X is called an (ϵ, δ)-*net* (or simply a net) if for every $x \in X$ there is some $n \in N$ such that $d(x, n) \leq \epsilon$ and for every $n_1, n_2 \in N$, $d(n_1, n_2) \geq \delta$.

A set N that satisfies only the second condition (i.e. for every $n_1, n_2 \in N$, $d(n_1, n_2) \geq \delta$) is called δ-separated.

Exercises 6.2. 1. Show that any metric space X has a $(1, 1)$-net.

2. Show that if $N \subset X$ is a net then $X \sim N$.

3. Show that $X \sim Y$ if and only if there are nets $N_1 \subset X, N_2 \subset Y$ and a bilipschitz map $f : N_1 \to N_2$.

4. Give an example of a metric space which is not quasi-isometric to any graph.

5. Let G be a finitely generated group. Show that $H < G$ is a net in G if and only if H is a finite index subgroup of G.

It turns out that if a finitely generated group acts 'nicely' on a 'nice' metric space then the space is quasi-isometric to the group.

We make this precise below.

Definition 6.4. Let $p : [0,1] \to X$ be a path in a metric space (X,d). We define the *length* of p to be the supremum of

$$\sum_{i=0}^{n} d(p(t_i), p(t_{i+1}))$$

over all partitions $0 = t_0 < t_1 < ... < t_n = 1$ ($n \in \mathbb{N}$) of $[0,1]$. We say that X is a *geodesic metric space* if for any $a, b \in X$ there is a path p joining a, b such that $length(p) = d(a,b)$. Such a path p is called *geodesic*.

It will be convenient to parametrize paths with respect to arc-length. We recall that a path $p : [0,l] \to X$ is said to be parametrized by arc-length if

$$|t - s| = length(p([t,s])), \ \forall t, s \in [a,b]$$

If X is a geodesic metric space and $a, b \in X$ we denote by $[a,b]$ a geodesic path joining them.

Examples. 1. Connected graphs with the metric defined earlier are geodesic metric spaces.

2. $\mathbb{R}^n$ with the Euclidean distance and, more generally, complete Riemannian manifolds are geodesic metric spaces (Hopf-Rinow).

3. $\mathbb{R}^2 - \{(0,0)\}$ is not a geodesic metric space.

Definition 6.5. We say that a metric space X is *proper* if every closed ball in X is compact.

Example 6.3. A graph with a vertex of infinite degree is not a proper metric space.

Definition 6.6. Assume that a group G acts on a metric space X by isometries. We say that the action is *co-compact* if there is a compact $K \subset X$ such that

$$\bigcup_{g \in G} \{gK\} = X$$

We say that G acts *properly discontinuously* on X if for every compact $K \subset X$ the set $\{g \in G : gK \cap K \neq \emptyset\}$ is finite.

Theorem 6.1. *(Milnor-Svarč lemma) Let X be a proper geodesic metric space. If G acts by isometries, properly discontinuously and co-compactly on X then:*

1) G is finitely generated.

2) If S is a finite generating set of G the map

$$f : \Gamma(S,G) \to X, \ \ g \mapsto gx_0$$

is a quasi-isometry (for any fixed $x_0 \in X$).

Proof. Let $R > 0$ be such that the G-translates of $B = B(x_0, R)$ cover X, i.e.

$$\bigcup_{g \in G} \{gB\} = X$$

The set

$$S = \{s \in G : d(sx_0, x_0) \leq 2R + 1\}$$

is finite since the action of G is properly discontinuous. We claim that S is a generating set of G. Indeed let $g \in G$. Consider a geodesic path $[x_0, gx_0]$. If

$$k - 1 < d(x_0, gx_0) \leq k, \ (k \in \mathbb{N})$$

consider $x_1, ..., x_k = gx_0$ such that $d(x_i, x_{i+1}) \leq 1$ for all $i = 0, ..., k-1$. Pick $g_i \in G$, $i = 1, ..., k-1$ such that $d(g_i x_0, x_i) \leq R$. Then $d(g_i x_0, g_{i+1} x_0) \leq 2R + 1$ so $g_i^{-1} g_{i+1} \in S$. We pick $g_0 = e, g_k = g$. We have then

$$g = g_k = (eg_1)(g_1^{-1} g_2)...(g_{k-2}^{-1} g_{k-1})(g_{k-1}^{-1} g_k)$$

So g can be written as a product of elements in S.

Let's denote now by d_S the distance in $\Gamma(S, G)$. The previous calculation shows that

$$d(gx_0, x_0) \geq d_S(g, e) - 1$$

Assume that $d_S(g, e) = n$, so $g = s_1 ... s_n$ where $s_i \in S \cup S^{-1}$ for all i. Then

$$d(gx_0, x_0) = d(s_1...s_n x_0, x_0) \leq d(s_1...s_n x_0, s_1...s_{n-1} x_0) + ... + d(s_1 x_0, x_0) \leq (2R+1)n$$

So

$$d(gx_0, x_0) \leq (2R+1) d_S(g, e)$$

It follows that the map $g \to gx_0$ is a quasi-isometry between $\Gamma(S, G)$ and Gx_0.

Since S is finite the set $S' = \{g \in S : gx_0 \neq x_0\}$ is finite. Let

$$r = \min\{d(gx_0, x_0) : g \in S'\}$$

We remark that $N = \{gx_0 : g \in G\}$ is an (R, r)-net of X, so the identity map $i : N \to X$, $i(gx_0) = gx_0$ is a quasi-isometry, so $f = f \circ i$ is a quasi-isometry from G to X. ☐

This is what we've done so far.

Corollary 6.1. *1. Let $G =< S >$ be a finitely generated group and let H be a finite index subgroup of G. Then H is quasi-isometric to G.*

2. Let G be a finitely generated group and let N be a finite normal subgroup of G. Then G/N is quasi-isometric to G.

Proof. 1. H acts freely and co-compactly on $\Gamma(S, G)$.

2. G acts properly discontinuously and co-compactly on the Cayley graph of G/N. □

In geometric group theory we 'identify' groups which differ by a 'finite amount' as in the corollary above.

We give now some examples of algebraic properties that are preserved by quasi-isometries.

Exercise 6.1. Let $G =< S|R >$ be a finitely presented group and let H be a finitely generated group quasi-isometric to G. Then H is finitely presented.

Definition 6.7. If $G =< S >$ is a finitely generated group we define the growth function of G to be

$$vol_{S,G}(r) = |B(r)|$$

where $B(r)$ is the ball of radius r in (G, d_S) centered at e.

We define an equivalence relation on functions $f : \mathbb{R}^+ \to \mathbb{R}^+$. We say that $f \prec g$ if there are $A, B, C > 0$ such that for all $r \in \mathbb{R}^+$ we have $f(r) \le Ag(Br) + C$. We note that $\prec$ is a partial order.

We say that $f \sim g$ if $f \prec g$ and $g \prec f$. $\sim$ is clearly an equivalence relation.

Exercise 6.2. Show that if $G_1 =< S >, G_2 =< S' >$ are finitely generated quasi-isometric groups then $vol_{S,G_1} \sim vol_{S',G_2}$. Deduce that the growth function of a group does not depend (up to equivalence) on the generating set that we pick.

Usually one considers this function up to equivalence, and denotes it by $vol_G(r)$.

Theorem 6.2. *(Gromov) A finitely generated group G has a nilpotent subgroup of finite index if and only if $vol_G(r) \prec r^n$ for some $n \in \mathbb{N}$.*

It follows from this theorem that if G is quasi-isometric to a finitely generated nilpotent group then G has a nilpotent subgroup of finite index.

Definition 6.8. (ends) Let Γ be a locally finite graph. If $K \subset \Gamma$ is compact we define $c(K)$ to be the number of unbounded connected components of $\Gamma - K$. We define then the *number of ends* of Γ to be

$$e(\Gamma) = \sup\{c(K) : K \subset \Gamma, \ \textit{compact}\}$$

We remark that we obtain an equivalent definition if, instead of compact sets K, we consider finite sets of vertices of Γ. Clearly finite graphs have 0 ends.

For a finitely generated group G we define the number of ends, $e(G)$, of G to be the number of ends of the Cayley graph of G.

Exercise 6.3. Show that two quasi-isometric locally finite graphs have the same number of ends. Deduce that the number of ends of a finitely generated group is well defined (ie it does not depend on the Cayley graph that we pick).

Exercise 6.4. Show that a finitely generated group has 0,1,2 or ∞ ends.

For example $\mathbb{Z}^2$ has 1 end, $\mathbb{Z}$ has 2 ends while $\mathbb{F}_2$ has ∞ ends.

It turns out that the number of ends of the Cayley graph of a group tells us whether the group splits over a finite group:

Theorem 6.3. *(Stallings) A finitely generated group G splits over a finite group if and only if G has more than 1 end.*

It is easy to see (exercise) that if a f.g. group G splits over a finite group then $e(G) > 1$. So the interesting direction of the theorem is: if $e(G) > 1$ then G splits over a finite group.

Stallings theorem combined with Dunwoody's accessibility theorem implies that if a finitely generated group is quasi-isometric to a free group then it has a finite index subgroup which is free.

We treat now the easier case of groups quasi-isometric to $\mathbb{Z}$.

Proposition 6.1. *Let G be a finitely generated 2-ended group. Then G has a finite index subgroup isomorphic to $\mathbb{Z}$.*

Proof. Let Γ be the Cayley graph of G. We consider a compact connected set K such that $\Gamma - K$ has 2 unbounded connected components C, D.

We claim that there is some $a \in G$ such that aC is properly contained in C. Indeed pick g such that gK is contained in C. Then at least one unbounded component of $\Gamma - gK$ does not contain K. If this is gC, then, since gC is connected, gC is properly contained in C and we are done. Otherwise gD is contained in C. Pick now h such that hK is contained in gD. If hD is properly contained in gD then $g^{-1}hD$ is properly contained in D. Set $a = g^{-1}h$ and rename D to C. Otherwise hC is properly contained in gD, hence it is properly contained in C.

We remark that $aC \subset C$ and $aC \neq C$. So $a^2C \subset aC \subset C$. Inductively we have $a^nC \subset C$, $a^nC \neq C$. It follows that a is an element of infinite order.

We note now that $K \cap aK = \emptyset$. Since $d(e, a^n) \to \infty$ for any vertex $v \in \Gamma$, there is some $n \in \mathbb{Z}$ such that v is either contained in a^nK or v is contained in a bounded component of $\Gamma - (a^{n-1}K \cup a^nK)$.

It follows that

$$\{a^n : n \in \mathbb{Z}\}$$

is a net in Γ. So $< a >$ is a finite index subgroup of G. $\square$

Corollary 6.2. *Let G be a finitely generated group quasi-isometric to $\mathbb{Z}$. Then G has a finite index subgroup isomorphic to $\mathbb{Z}$.*

6.2 Hyperbolic Spaces

If X is a geodesic metric space, a geodesic triangle $[x, y, z]$ in X is a union of three geodesic paths $[x, y] \cup [y, z] \cup [x, z]$ where $x, y, z \in X$.

Definition 6.9. Let $\delta \geq 0$. We say that a geodesic triangle in a geodesic metric space is *δ-slim* if each side is contained in the δ-neighborhood of the two other sides. We say that a geodesic metric space X is *hyperbolic* if there is some $\delta \geq 0$ so that all geodesic triangles in X are δ-slim.

Examples. 1. Trees are hyperbolic spaces (in fact 0-hyperbolic).

2. Finite graphs are hyperbolic spaces.

3. $\mathbb{R}^2$ with the usual Euclidean metric is not hyperbolic.

4. It turns out that $\mathbb{H}^2$, the hyperbolic plane, is hyperbolic.

There are several equivalent formulations of hyperbolicity. We give one more now and we will discuss some other reformulations later in the course.

If $\Delta = [x, y, z]$ is a triangle then there is a metric tree (a 'tripod') T_Δ with 3-endpoints x', y', z' such that there is an onto map $f_\Delta : \Delta \to T_\Delta$ which restricts to an isometry from each side $[x, y], [y, z], [x, z]$ to the corresponding segments $[x', y'], [y', z'], [x', z']$. We denote by c_Δ the point $[x', y'] \cap [y', z'] \cap [x', z']$ of T_Δ.

Definition 6.10. Let $\delta \geq 0$. We say that a geodesic triangle $\Delta = [x, y, z]$ in a geodesic metric space is *δ-thin* if for every $t \in T_\Delta = [x', y', z']$, $diam(f_\Delta^{-1}(t)) \leq \delta$.

Theorem 6.4. *Let X be a geodesic metric space. The following are equivalent:*

1. *There is a $\delta \geq 0$ such that all geodesic triangles in X are δ-slim.*
2. *There is a $\delta' \geq 0$ such that all geodesic triangles in X are δ'-thin.*

Proof. Clearly 2 implies 1. Indeed one can simply take $\delta = \delta'$.

We show now that 1 implies 2. We will show that we may take $\delta' = 4\delta$.

Let $\Delta = [x, y, z]$ be a geodesic triangle and let $f_\Delta : \Delta \to T_\Delta$ the map defined above to a tripod. Let $f^{-1}(c_\Delta) = \{c_x, c_y, c_z\}$ where

$$c_x \in [y, z],\ c_y \in [x, z],\ c_z \in [x, y]$$

Let $a \in [x, c_z]$ and let a' in $[x, c_y]$ such that $d(x, a') = d(x, a)$. By symmetry it is enough to show that $d(a, a') \leq 4\delta$.

We have that

$$d(a, a_1) \leq \delta$$

for some

$$a_1 \in [x, z] \cup [y, z]$$

We distinguish two cases:

Case 1. $a_1 \in [x, z]$. Then

$$d(x, a') + \delta \geq d(x, a) + d(a, a_1) \geq d(x, a_1) \geq d(x, a) - d(a, a_1) \geq d(x, a') - \delta$$

by the triangle inequality. It follows that

$$d(a, a') \leq \delta + d(a_1, a') \leq 2\delta$$

Case 2. $a_1 \in [y, z]$. We claim that $d(a, c_x) \leq 2\delta$ in this case. Indeed if $a_1 \in [c_x, y]$ by the triangle inequality

$$d(a, y) \leq d(y, a_1) + \delta \implies d(y, a_1) \geq d(y, c_x) - \delta \implies d(a_1, c_x) \leq \delta$$

so $d(a, c_x) \leq 2\delta$.

If $a_1 \in [c_x, z]$ then again by the triangle inequality:

$$d(x, z) \leq d(x, a) + \delta + d(a_1, z) \implies d(x, z) \leq d(x, c_z) + \delta + d(a_1, z)$$

Since $d(x, z) = d(z, c_y) + d(x, c_z)$ and $d(z, c_y) = d(z, c_x)$ we obtain:

$$d(z, c_x) \leq d(a_1, z) + \delta$$

so $d(a_1, c_x) \leq \delta$ and $d(a, c_x) \leq 2\delta$. By symmetry, either, as in case 1, $d(a', a) \leq 2\delta$ or $d(a', c_x) \leq 2\delta$. It follows that

$$d(a, a') \leq 4\delta$$

□

Definition 6.11. Let X be a geodesic metric space. We say that X is δ-hyperbolic if all geodesic triangles in X are δ-thin.

Lemma 6.1. *Let X be a δ-hyperbolic geodesic metric space. Let $x_0, x_1, ..., x_n \in X$ and let $p \in [x_0, x_n]$. Then*

$$d(p, [x_0, x_1] \cup [x_1, x_2] ... \cup [x_{n-1}, x_n]) \leq (log_2(n) + 1)\delta$$

Proof. Let's say that $2^{k-1} < n \leq 2^k$ for $k \in \mathbb{N}$. It suffices to prove that

$$d(p, [x_0, x_1] \cup [x_1, x_2] ... \cup [x_{n-1}, x_n]) \leq k\delta.$$

We argue by induction on k. This is clearly true if $k = 1$ (ie. $n = 2$). For $k > 1$, pick $m = 2^{k-1}$. Then there is some $p_1 \in [x_0, x_m] \cup [x_m, x_n]$ with $d(p, p_1) \leq \delta$. By the inductive hypothesis

$$d(p_1, [x_0, x_1] \cup [x_1, x_2] ... \cup [x_{n-1}, x_n]) \leq (k - 1)\delta$$

and the result follows.

□

6.3 Quasi-geodesics

Definition 6.12. A path $\alpha : I \to X$ in a geodesic metric space X is a (λ, μ)-*quasi-geodesic*, where $\lambda \geq 1, \mu \geq 0$, if for all $t, s \in I$,

$$length\,(\alpha([t, s])) \leq \lambda d(\alpha(t), \alpha(s)) + \mu$$

Proposition 6.2. *Let X be a δ-hyperbolic metric space. There exist constants $L = L(\lambda, \mu), M = M(\lambda, \mu)$ such that if $x, y \in X$, $\alpha : I \to X$ is a (λ, μ)-quasi-geodesic with endpoints x, y and $\gamma = [x, y]$ then*

$$\gamma \subset N_L(\alpha),\ \alpha \subset N_M(\gamma)$$

Proof. We show first the existence of L. Let $a \in \gamma$ such that $d(a, \alpha) = D$ is maximum. Let $a_1 \neq a_2 \in \gamma$ with

$$d(a, a_1) = d(a, a_2) = D$$

and let $\alpha(t), \alpha(s)$ points in α realizing $d(a_1, \alpha), d(a_2, \alpha)$, respectively. We consider the path

$$\beta = [a_1, \alpha(t)] \cup \alpha([t, s]) \cup [a_2, \alpha(s)]$$

Clearly $d(a, \beta) \geq D/2$.

We pick points $x_1 = \alpha(t), x_2, ..., x_{n-1} = \alpha(s)$ such that $d(x_i, x_{i+1}) = 1$ for $i = 1, ..., n-3$ and $d(x_{n-2}, x_{n-1}) \leq 1$. By lemma 6.1

$$d(a, [a_1, \alpha(t)] \cup [x_1, x_2] \cup ... \cup [x_{n-2}, x_{n-1}] \cup [a_2, \alpha(s)]) \leq (log_2(n) + 1)\delta$$

and

$$(log_2(n) + 1)\delta \geq \frac{D}{2} - 1 \Rightarrow (2n)^\delta \geq 2^{\frac{D}{2}-1}$$

Since $n - 2 \leq length\,(\alpha([t, s]))$ and $length\,(\alpha([t, s])) \leq 4D\lambda + \mu$ we obtain:

$$(8D\lambda + 2\mu + 4)^\delta \geq 2^{\frac{D}{2}-1}$$

which gives a bound L for D that depends only on λ, μ (and δ).

We show now the existence of M. Let $x = \alpha(s)$. By a continuity argument there is some $y \in \gamma$ such that y is at distance less than L from $\alpha(s_1)$ and $\alpha(s_2)$ with $s_1 \leq s \leq s_2$. It follows that

$$length(\alpha([s_1, s_2]) \leq 2L\lambda + \mu,$$

therefore

$$d(x, \gamma) \leq 2L(\lambda + 1) + \mu$$

so we may take $M = 2L(\lambda + 1) + \mu$.

□

Corollary 6.3. *Let X be a δ-hyperbolic metric space and let Y be a geodesic metric space quasi-isometric to X. Then Y is hyperbolic.*

Proof. Let Δ be a geodesic triangle in Y. If $f : Y \to X$ is a quasi-isometry $f(\Delta)$ is contained in a finite neighborhood of a (λ, μ) quasi-geodesic triangle Δ' in X, where λ, μ depend only on f. By proposition 6.2 Δ' is ϵ-thin for some $\epsilon = \epsilon(\lambda, \mu, \delta) \geq 0$. But then Δ is also δ'-thin for some δ' that depends only on δ and f. □

6.4 Hyperbolic Groups

Definition 6.13. Let $G = \langle S \rangle$ where S is finite. We say that G is *hyperbolic* if the Cayley graph $\Gamma = \Gamma(S, G)$ is a hyperbolic metric space.

Remark 6.1. By corollary 6.3 if $G = \langle S_1 \rangle = \langle S_2 \rangle$ with S_1, S_2 finite then $\Gamma(S_1, G)$ is hyperbolic if and only if $\Gamma(S_2, G)$ is hyperbolic, so the definition above does not depend on the generating set S.

We note that if a group G is not finitely generated then for $S = G$, $\Gamma(S, G)$ is bounded, hence hyperbolic. So one can not extend in any reasonable way the definition of hyperbolicity to groups that are not finitely generated.

Examples. 1. Finitely generated free (or virtually free) groups are hyperbolic.

2. Groups acting discretely and co-compactly on $\mathbb{H}^n$ are hyperbolic.

3. $\mathbb{Z}^2$ is *not* hyperbolic.

4. A finite presentation $\langle S|R\rangle$ is said to satisfy condition $C'(\frac{1}{7})$ if for any two cyclic permutations r_1, r_2 of words in $R \cup R^{-1}$ any common initial subword w of r_1, r_2 has length $|w| \leq \frac{1}{7}\min\{|r_1|, |r_2|\}$. It can be shown that $C'(\frac{1}{7})$-groups are hyperbolic. As an example the group

$$G = \langle a, b, c, d|abcdbadc\rangle$$

satisfies the $C'(\frac{1}{7})$ condition, so it is hyperbolic.

5. A theorem of Gromov-Olshanskii shows that 'statistically most groups are hyperbolic': Given $p, q \in \mathbb{N}$ consider all presentations of the form

$$\langle a_1, ..., a_p|r_1, ..., r_q\rangle$$

where the r_i's are cyclically reduced words of the a_j's. Let's denote by $N(t, \lambda t)$ (where $\lambda > 1$) all presentations of this type such that for all i,

$$t \leq |r_i| \leq \lambda t$$

We denote N_h the presentations of hyperbolic groups among those. Then

$$\lim_{t\to\infty} \frac{N_h}{N(t, \lambda t)} = 1$$

Definition 6.14. A *Dehn presentation* of a group G is a finite presentation $\langle S|R\rangle$ such that every reduced word $w \in F(S)$ which is equal to the identity in G contains more than half of a word in R.

Remark 6.2. If $\langle S|R\rangle$ is a Dehn presentation then the word problem for $\langle S|R\rangle$ is solvable. Indeed if w is a word we check if it contains more than half of a relation in R. If not then $w \neq 1$. Otherwise $w = w_1uw_2$ for some $uv \in R$ with $|v| < |u|$. Then $w = w_1v^{-1}w_2$ so we replace w by $w_1v^{-1}w_2$ and we repeat. Since the length decreases this procedure terminates in finitely many steps.

Theorem 6.5. *Let $G = \langle S\rangle$ be a hyperbolic group. Then G has a Dehn presentation. In particular G is finitely presented and the word problem for G is solvable.*

Proof. Assume that triangles in $\Gamma = \Gamma(S, G)$ are δ-thin for $\delta \in \mathbb{N}$. We set

$$R = \{w \in F(S) : |w| \le 10\delta,\ w \underset{G}{=} 1\}$$

We claim that $\langle S|R\rangle$ is a Dehn presentation for G. We will show that if $w \in F(S)$ is word such that $w \underset{G}{=} 1$ then w contains more than half of a word in R. We remark that this is trivially true if $|w| \le 10\delta$. We see w as a closed path of length $n = |w|$ in the Cayley graph Γ, $w : [0, n] \to \Gamma$, $w(0) = w(n) = e$. If w contains a subword u of length $\le 5\delta$ which is not geodesic then there is v with $|v| < |u|$ such that $uv \in R$, so w contains more than half of a relator and we are done. Otherwise let $t \in \{0, 1, 2, ..., n\}$ be such that $d(w(t), e)$ is maximum. We consider the triangles:

$$[e, w(t), w(t - 5\delta)], [e, w(t), w(t + 5\delta)]$$

Since these two triangles are δ-thin and $d(w(t), e) > 5\delta$ we have that

$$d(w(t - 2\delta), w(t + 2\delta)) \le 2\delta$$

so the subword of length 4δ, $[w(t - 2\delta), w(t + 2\delta)]$ is not geodesic. It follows that w contains more than half of a word in R.

□

Proposition 6.3. *Let G be a hyperbolic group. Then G has finitely many conjugacy classes of elements of finite order.*

Proof. Let $\langle S|R\rangle$ be a Dehn presentation of G. Let g be an element of finite order and let w be an element of the conjugacy class of g of minimal length. Then $w^n = 1$ so the word w^n contains more than half of a relation $r \in R$. We claim that

$$|w| \le \frac{|r|}{2} + 2$$

Suppose not. We remark that w is cyclically reduced. We have then that $r = r_1 r_2$, with $|r_1| > |r_2|, |r_1| \le \frac{|r|}{2} + 2$ and $w = utv$, $r_1 = vu$ for some words r_1, r_2, v, t, u where all the previous expressions are reduced. Then $u^{-1}wu = tvu = tr_1$ is in the conjugacy class of g. We have that $tr_1 = tr_2^{-1}$ and

$$|tr_2^{-1}| \le |t| + |r_2| < |t| + |r_1| = |w|$$

which is a contradiction since w is an element of the conjugacy class of g of minimal length. We remark now that there are finitely many words w of length less than

$$\max\{\frac{|r|}{2} + 2 \,:\, r \in R\}$$

so there are finitely many conjugacy classes of elements of finite order. □

We turn now our attention to the conjugacy problem. We recall that if $g \in G = \langle S \rangle$ we denote by $|g|$ the length of a shortest word on S representing g.

Lemma 6.2. *Let $G = \langle S|R \rangle$ be δ-hyperbolic (so triangles in $\Gamma(S,R)$ are δ-thin). If $g_1 \in G$ is conjugate to g_2 then there is some $x \in G$ such that $g_2 = xg_1x^{-1}$ and*

$$|x| \leq (2|S|)^{2\delta+|g_1|} + |g_1| + |g_2|$$

Proof. Let x be a word of minimal length such that $g_1 = xg_2x^{-1}$. Let's say that $x = x_1...x_n$ with $x_i \in S \cup S^{-1}$. We have then

$$|(x_1...x_i)^{-1}g_1(x_1...x_i)| \leq 2\delta + |g_1|$$

for all i with $|g_1| \leq i \leq n - |g_2|$. If

$$|x| \geq (2|S|)^{2\delta+|g_1|} + |g_1| + |g_2| + 1$$

then there are $i < j$ such that

$$(x_1...x_i)^{-1}g_1(x_1...x_i) = (x_1...x_j)^{-1}g_1(x_1...x_j)$$

so

$$(x_1...x_ix_{j+1}...x_n)^{-1}g_1(x_1...x_ix_{j+1}...x_n) = g_2$$

which contradicts the minimality of x.

□

Corollary 6.4. *The conjugacy problem is solvable for hyperbolic groups.*

Proof. Indeed given $g_1, g_2 \in G$ it suffices to check whether $g_2 = xg_1x^{-1}$ for all x with

$$|x| \leq (2|S|)^{2\delta+|g_1|} + |g_1| + |g_2|$$

□

Lemma 6.3. *Let $G = \langle S \rangle$ be δ-hyperbolic for some $\delta \in \mathbb{N}$, $\delta \geq 1$. Assume that for some $g \in G$ with $|g| > 4\delta$ we have that $|g^2| \leq 2|g| - 2\delta$. Then there is some $h \in G$ conjugate to g with $|h| < |g|$.*

Proof. Consider the triangle $[1, g, g^2]$ in $\Gamma(S, G)$. By δ-thinness of this triangle we have that there are $u, s, v \in G$ such that $g = usv$ (where usv is a geodesic word), $|u| = |v| = \delta$ and $|vu| \leq \delta$. If we set $t = vu$ we have that

$$g = usv = ustu^{-1}$$

and $|st| < |g|$.

□

Lemma 6.4. *Let $G = \langle S \rangle$ be δ-hyperbolic for some $\delta \in \mathbb{N}$, $\delta \geq 1$. Assume that for some $g \in G, x \in \Gamma(S, G)$ with $d(x, gx) > 100\delta$ we have that $d(x, g^2x) > 2d(x, gx) - 8\delta$. Then*

$$d(x, g^n x) \geq nd(x, gx) - 16n\delta$$

for all $n \in \mathbb{N}$.

Proof. It suffices to show that for all n

$$d(x, g^n x) \geq d(x, g^{n-1}x) + d(x, gx) - 16\delta$$

Clearly this holds for $n = 1, 2$. We argue by induction. Assume that it is true for all $k \leq n$. We consider the triangles $[x, g^n x, g^{n+1}x]$, $[x, g^{n-1}x, g^n x]$. Assume that

$$d(x, g^{n+1}x) < d(x, g^n x) + d(x, gx) - 16\delta$$

By δ-thinness of $[x, g^n x, g^{n+1}x]$ there are vertices u_1, u_2 on the geodesics $[g^n x, g^{n+1}x], [x, g^n x]$ respectively, such that

$$d(u_1, g^n x) = d(u_2, g^n x) = 5\delta,\ d(u_1, u_2) \leq \delta$$

Similarly by δ-thinness of $[x, g^{n-1}x, g^n x]$ there is a vertex $u_3 \in [g^{n-1}x, g^n x]$ such that $d(u_3, g^n x) = 5\delta$ and $d(u_2, u_3) \leq \delta$. We have then

$$d(x, g^2x) = d(g^{n-1}x, g^{n+1}x) \leq d(g^{n-1}x, u_3) + d(u_1, u_3) + d(u_1, g^{n+1}x) = 2d(x, gx) - 8\delta$$

which is a contradiction.

□

Proposition 6.4. *Let $G = \langle S \rangle$ be δ-hyperbolic for some $\delta \in \mathbb{N}$, $\delta \geq 1$. Assume that g is an element of infinite order. Then there are constants $c > 0, d \geq 0$ such that*

$$d(1, g^n) \geq cn - d$$

for all $n \in \mathbb{N}$.

Proof. It is clear that we may replace g by a power. Further it is enough to show that for some $x \in \Gamma(S, G)$ there are constants c', d' so that

$$d(x, g^n x) \geq c'n - d'$$

for all n.

In what follows we pick $n \gg k \gg 0, k, n \in \mathbb{N}$. It will be clear from the proof how k, n are chosen. We consider the geodesic $[1, g^n]$. Let m be a vertex on this geodesic at distance ≤ 1 from its midpoint. Since there are finitely many vertices in the ball $B(m, 100\delta)$ we may pick k so that

$$d(m, g^k m) \geq 100\delta$$

Now by thinness of the quadrilateral

$$[1, g^n, g^{k+n}, g^k]$$

and since $n \gg k$, we have that

$$d(g^k m, [1, g^n]) \leq 2\delta$$

In particular there is a vertex y on $[1, g^n]$ such that $d(y, g^k m) \leq 2\delta$. Then $g^k[m, y]$ is contained in the geodesic $[g^k, g^{k+n}]$ and there is some $z \in [1, g^n]$ such that $d(z, g^k y) \leq 2\delta$. It follows that

$$d(m, g^{2k} m) \geq d(m, g^k y) - 2\delta \geq 2d(m, y) - 4\delta \geq d(m, g^k m) - 8\delta$$

since $d(m, y) \geq d(m, g^k m) - 2\delta$. The assertion now follows by applying lemma 6.4 to g^k and m.

$\square$

It follows from this proposition that if α is a geodesic from 1 to g then

$$\bigcup_n g^n \alpha$$

is a quasi-geodesic.

Proposition 6.5. *Let $G = \langle S \rangle$ be δ-hyperbolic and let $g \in G$ be an element of infinite order. Let $C(g)$ be the centralizer of g. Then the quotient $C(g)/\langle g \rangle$ is finite.*

Proof. Let $L > 0$ be such that for any $n \in \mathbb{N}$ the geodesic $[1, g^n]$ is contained in the L-neighborhood of $\{1, g, ..., g^n\}$. Let $s \in C(g)$ and $m \in \mathbb{N}$ such that

$$|g^m| \geq 2|s| + 2\delta$$

We consider the quadrilateral $[1, g^m, sg^m, s]$. By δ-thinness there is some vertex $p \in [1, g^m]$ such that

$$d(p, [s, sg^m]) \leq 2\delta$$

It follows that there are g^i, g^j such that

$$d(g^i, g^j s) \leq 2L + 2\delta$$

so

$$d(g^{i-j}, s) \leq 2L + 2\delta$$

It follows that $s = g^{i-j}u$ with $|u| \leq 2L + 2\delta$. Therefore every coset $s\langle g\rangle$ has a representative which has word length $\leq 2L + 2\delta$. Hence the quotient $C(g)/\langle g\rangle$ is finite. □

Corollary 6.5. *If G is hyperbolic then G has no subgroup isomorphic to $\mathbb{Z} \times \mathbb{Z}$.*

6.5 More results and open problems

There is a number of results on hyperbolic groups that we were not able to present in this short introduction. We give a list of some results hoping that this will give a better perspective on the subject. Some of the results below can be proven by the techniques that we have already presented while others are quite deep requiring a quite different approach.

Theorem 6.6. *Let G be a hyperbolic group which is not finite or virtually $\mathbb{Z}$. Then G contains a free subgroup of rank 2.*

Theorem 6.7. *Let G be a hyperbolic group and let $g_1, ..., g_n \in G$. Then there is some $N > 0$ such that the group $\langle g_1^N, ..., g_n^N\rangle$ is free of rank at most n.*

Theorem 6.8. *(Gromov-Delzant) Let G be a hyperbolic group and let H be a fixed one-ended group. Then G contains at most finitely many conjugacy classes of subgroups isomorphic to H.*

Theorem 6.9. *(Sela-Guirardel-Dahmani) The isomorphism problem is solvable for hyperbolic groups.*

Theorem 6.10. *(Sela) Torsion free hyperbolic groups are Hopf.*

There is a number of open questions about hyperbolic groups:

1. Are hyperbolic groups resudually finite?
2. Let G be hyperbolic. Does G have a torsion free subgroup of finite index?
3. Gromov conjectures that if G is torsion free hyperbolic then G has finitely many torsion free finite extensions.