Combinatorial Group Theory

Charles F. Miller III

March 5, 2002

Abstract

These notes were prepared for use by the participants in the Workshop on Algebra, Geometry and Topology held at the Australian National University, 22 January to 9 February, 1996. They have subsequently been updated for use by students in the subject 620-421 Combinatorial Group Theory at the University of Melbourne.

Contents

Chapter 1

Free groups and presentations

In introductory courses on abstract algebra one is likely to encounter the dihedral group D_3 consisting of the rigid motions of an equilateral triangle onto itself. The group has order 6 and is conveniently described by giving two generators which correspond to rotation through 120° and flipping about a central axis. These operations have orders 3 and 2 respectively and the group D_3 is described by the *presentation*

$$D_3 =< a, b \mid a^2 = 1, b^3 = 1, a^{-1}ba = b^{-1} >$$

some equivalent version. Here the symbols a and b are called *generators* and the equations they are subjected to are called *defining relations*.

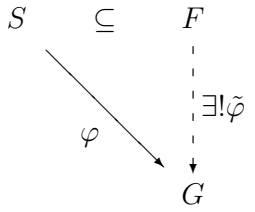
Combinatorial group theory is concerned with groups described by generators and defining relations and also with certain natural constructions for making new groups out of groups we already have in hand. Also one would like to (1) say something about their structure, their subgroups, and various properties they might enjoy and to (2) find algorithms for answering some natural questions about them and their elements. Combinatorial group theory has many connections with algebraic and geometric topology which have provided both motivation and methods for studying groups in this manner.

In order to begin our study of presentations we first need to discuss free groups. We will then introduce presentations in terms of generators and relations more formally and indicate their connection with algebraic topology via the fundamental group.

1.1 Free groups

In most algebraic contexts a *free* object is an object which has a *free basis*. The pattern for groups is typical of this sort of definition.

A subset S of a group F is said to be a *free basis* for F if, for every (set) function $\varphi : S \to G$ from the set S to a group G can be extended uniquely to a homomorphism $\tilde{\varphi} : F \to G$ so that $\tilde{\varphi}(s) = \varphi(s)$ for every $s \in S$.



A group F is said to be a *free group* if there is some subset which is a free basis for F.

Consider the infinite cyclic group C (written multiplicatively) which consists of all powers of a single element a,so

$$C = \{\ldots, a^{-2}, a^{-1}, 1 = a^0, a = a^1, a^2, a^3, \ldots\}$$

and multiplication is defined by $a^i \cdot a^j = a^{i+j}$ for $i, j \in \mathbb{Z}$. Then C is a free group with free basis the set with a single element $S = \{a\}$. For if $\varphi : S \to G$ is any function, say $\varphi(a) = g \in G$ then φ extends to a homomorphism $\tilde{\varphi} : C \to G$ by defining $\tilde{\varphi}(a^i) = g^i$. Moreover it is clear this is the only way to extend φ to a homomorphism. Notice that C also has another free basis, namely the singleton set $\{a^{-1}\}$ and that these two are the only free bases for C.

Similarly, the additive group of integers $\mathbb{Z}$ (which is of course isomorphic to C) is also a free group with either of the singleton sets $\{1\}$ or $\{-1\}$ as a free basis. As a slightly more exotic example, we note that the trivial group consisting of $\{1\}$ alone is a free group with the empty subset as free basis.

Beyond these familiar examples we have to do something to prove that free groups exist. In fact we can make a free group with any given set S as a basis in the way described below.

Theorem 1.1 *If S is any set, there is a free group F_S having S as a free basis.*

Suppose we are given a set S which we think of as just a set of symbols (S need not be countable or ordered). By a *word* on S we mean an expression of the form $a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_k^{\epsilon_k}$ where $\epsilon_i = \pm 1$ and $a_i \in S$ (not necessarily distinct symbols). That is, a word is a string of elements of S with exponents either $+1$ or -1. The intention is that a^{-1} and a^{+1} are to be mutually inverse group elements and one usually identifies a^{+1} with a.

Sometimes it is convenient to adopt a slightly different definition. Let $S^{-1} = \{a^{-1} \mid a \in S\}$ be thought of as the set of inverse symbols for the symbols of S. Then by a word on S we would mean just a string of symbols from $S \cup S^{-1}$. This rarely causes confusion and we use whichever version is convenient.

A word on S is said to be *(freely) reduced* if it does not contain a subword (consecutive substring) of the form aa^{-1} or of the form $a^{-1}a$; such substrings are called *inverse pairs* of generators. If a word w contains an inverse pair, say $w \equiv ua^{-1}av$ where u and v are subwords, then in any group containing w one must have $w = uv$ (here $\equiv$ means identical as words and $=$ means equal as group elements). If we start with any word w by successively removing inverse pairs we arrive in a finite number of steps at a freely reduced word w'. One can show that w' does not depend on the order in which the inverse pairs are removed. This is a basic but non-trivial fact which certainly requires proof (which we omit). But this fact does allow us to call w' the (free) reduction of w and we write this as $w' = \rho(w)$.

We are now ready to define the free group F_S with free basis S. The elements of F_S are the freely reduced words on S (including the empty word which we denote by 1). Multiplication in F_S is defined by $u \cdot v = \rho(uv)$, that is the product is the free reduction of one word followed by the other (concatenation). One now must check the axioms for a group. The identity is the empty word 1 and the inverse of $a_1^{\epsilon_1}a_2^{\epsilon_2}\dots a_k^{\epsilon_k}$ is $a_k^{-\epsilon_k}a_{k-1}^{-\epsilon_{k-1}}\dots a_1^{-\epsilon_1}$. The associative law follows from the fact that the reduction of a word is independent of the order in which inverse pairs are removed.

To see that F_S is in fact free, consider any function $\varphi : S \to G$ where G is a group. We define

$$\tilde{\varphi}(a_1^{\epsilon_1}a_2^{\epsilon_2}\dots a_k^{\epsilon_k}) = \varphi(a_1)^{\epsilon_1}\varphi(a_2)^{\epsilon_2}\dots\varphi(a_k)^{\epsilon_k}.$$

This map $\tilde{\varphi}$ is easily checked to be a homomorphism. Moreover, it is clear the definition is forced upon us so that it is the unique homomorphism extending the function φ.

Here is on consequence of the above.

Corollary 1.2 *Every group is a quotient group of a free group. Thus if G is a group there is a free group F and a normal subgroup N such that $G \cong F/N$.*

To see this, given a group G we think of G as a set (forgetting its group operation for the moment) and form the free group F_G as above. Then the identity function $\varphi : G \to G$ from G as a set to G as a group (remember the group operation) extends uniquely to a homomorphism $\tilde{\varphi} : F_G \to G$. The

homomorphism $\tilde{\varphi}$ is clearly surjective (since φ is a bijection), so $G \cong F_G/N$ where $N = \ker \tilde{\varphi}$.

In general, if S is a subset of a group G, the subgroup denoted by $< S >$ (called the *subgroup generated by* S) is the image of the extension $\tilde{\varphi} : F_S \to G$ of the inclusion function. That is, the subgroup $< S >$ generated by S consists of those elements of G which are equal to some product of elements in S and their inverses. In particular, if $< S >= G$, we say that S generates G.

The *rank* of a the free group F_S is the cardinality of the set S of generators. One can show this is an invariant of the free group F_S, that is if T is another free basis for F_S then S and T have the same cardinality (number of elements). If G is any group, then the *rank* of G is the cardinality of the smallest set of generators for G, that is the rank of the smallest free group F for which there is a surjection $\varphi : F \to G$. It is often difficult to determine the rank of a group (other than a free group).

Notation: Although we somewhat carefully distinguished between φ and $\tilde{\varphi}$ in the above, we often adopt the notational convention that the extending homomorphism is also denoted φ. This is common practice and usually causes no confusion. In some cases to be more precise we may resort to the original notation. We will also use notation such as $w \equiv uv$ to mean that the word w is identical to the word u followed by the word v. The equation $w = uv$ or $w =_G uv$ means that w is equal in some appropriate group G to the product of u and v. Also, if $x, y \in G$ their *commutator* is the element denoted $[x, y]$ which is by definition $[x, y] = x^{-1}y^{-1}xy$. As usual, two such elements *commute* if $xy =_G yx$ which is equivalent to $[x, y] =_G 1$.

Terminology We use the terms *surjective*,*epic* and *onto* for functions interchangeably. An *epimorphism* is a surjective homomorphism. Likewise, the terms *injective monic* and *one-one* are interchangeable, and a *monomorphism* is an injective homomorphism.

Theorem 1.3 (Characterization of freeness) *Let G be a group, and S a subset of G. Then G is free with basis S if and only if the following both hold:*

1. *S generates G; and*
2. *If w is a word on S and $w =_G 1$, then w is not freely reduced, that is w must contain an inverse pair.*

These conditions imply that every element of G is equal to a unique freely reduced word in G. For if $u =_G v$ and u and v are freely reduced, then uv^{-1} contains an inverse pair. Hence the last symbol of u is the same as the last

symbol of v. So inductively u and v must be identical. Thus different freely reduced words represent different elements of G. Hence the obvious extension of the identity on S is an isomorphism from F_S onto G.

Recall that two elements say g and h in a group G are *conjugate* if there exists some $x \in G$ such that $g = x^{-1}hx$. A word w in the free group F_S with basis S is said to be *cyclically reduced* if every cyclic permutation of w is (freely) reduced. If w is (freely) reduced, cyclically reduced is equivalent to saying the first symbol of w is not the inverse of the last symbol of w.

Exercise 1.1 *Show that two cyclically reduced words u and v in a free group F_S are conjugate if and only if one is a cyclic permutation of the other.*

1.2 Presentations by generators and relations

As in the case of D_3 above, we want to describe groups by writing down some elements which generate the group and then imposing some equations on them. Such a piece of notation might look like

$$G =< a_1, a_2, \ldots \mid u_1 = v_1, u_2 = v_2, \ldots >$$

where the a_i are symbols and the u_j and v_j are certain words in the a_i. (While we habitually use this sort of notation, it is not necessary for the set of generators to be countable or ordered.)

In any group, $u = v$ if and only if $uv^{-1} = 1$ so we can always write our presentations in the equivalent form

$$G =< a_1, a_2, \ldots \mid r_1 = 1, r_2 = 1, \ldots >$$

where $r_i = u_i v_i^{-1}$. Although we will use presentations with equations of the form $u = v$, for our theoretical discussion it is convenient to assume our defining equations are of the form $r = 1$.

To be a bit more formal for a moment, a *presentation* $P =< S \mid D >$ is a pair consisting of a set S called *generators* and a set D of words on S called *(defining) relators*. The *group presented by* P, denoted $gp(P)$ is the group F_S/N_D where F_S is the free group with free basis S and N_D is the normal closure of D in F_S, that is the smallest normal subgroup containing D. Thus if $r \in D$, then $r \in N_D$ and so $r =_{gp(P)} 1$. If $G = gp(P)$ we often abuse notation and write $G =< S \mid D >$ when it is not necessary to distinguish between a group and a description of that group.

A presentation $P =< S \mid D >$ is said to be *finitely generated* if S is a finite set and to be *finitely related* if D is a finite set of words. If both S and

D are finite, P is said to be a *finite presentation*. If $S = \{a_1, a_2, \ldots\}$ and $D = \{r_1, r_2, \ldots\}$ we use either the notation

$$P =< a_1, a_2, \ldots \mid r_1, r_2, \ldots >$$

in which case the r_i are called *relators*, or the notation

$$P =< a_1, a_2, \ldots \mid r_1 = 1, r_2 = 1, \ldots >$$

in which case the equations $r_i = 1$ are called relations. Usually we also extend the latter to allow

$$P =< a_1, a_2, \ldots \mid u_1 = v_1, u_2 = v_2, \ldots >$$

where $r_i = u_i v_i^{-1}$.

Here are a few more examples of presentations.

1. The infinite cyclic group C written multiplicatively with generator a has presentation $C =< a \mid >$ with an empty set of defining relators. More generally the free group F_S with free basis S has a presentation $F_S =< S \mid \emptyset >$.

2. The finite cyclic group C_n of order n has a presentation $C_n =< a \mid a^n = 1 >$.

3. The free abelian group of rank 2 has a presentation $< a, b \mid ab = ba >$ or equivalently $< a, b \mid aba^{-1}b^{-1} = 1 >$. In this group, which is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$, every element is equal to a unique word the form $a^i b^j$ where $i, j \in \mathbb{Z}$ and multiplication is addition of the corresponding exponents.

4. The dihedral group D_n of order $2n$ consisting of the rigid motions of the regular n-gon has presentation

$$D_n =< a, b \mid a^2 = 1, b^n = 1, a^{-1}ba = b^{-1} > .$$

5. The presentation $P =< a, b \mid ababa = 1 >$ turns out to be a presentation of the infinite cyclic group. This is not quite obvious, but we will show this below.

6. Any finite group G has a finite presentation. For generators we can take all the group elements, say $\{a_1, \ldots, a_n\}$, and for relations we take all the equations from the multiplication table (these have the form $a_i a_j = a_k$ and are n^2 in number.)

Of course when we write down some defining relations for a group there can be consequences we don't expect. For instance consider the group mentioned above with presentation $G =< a, b \mid ababa = 1 >$. Now $baaba =_G 1$ since this is just a conjugate of the given relator. Multiplying this by the inverse of the relator we obtain

$$1 =_G (baaba)(ababa)^{-1} = baabaa^{-1}b^{-1}a^{-1}b^{-1}a^{-1} = bab^{-1}a^{-1}$$

and so $ab =_G ba$. It follows that G is an abelian group which may not have been apparent at first.

Exercise 1.2 *Let $G =< a, t \mid t^{-1}at = a^2 >$. Show that every element of G is equal to a word of the form $t^n a^k t^{-m}$ where $n \geq 0$ and $m \geq 0$. Let N denote the normal closure in G of the element a. Show that N is generated by elements of the form $t^n a t^{-n}$, and that N is abelian.*

Exercise 1.3 *Let $G =< a, b \mid a^{-1}ba = b^2, b^{-1}ab = a^2 >$. Show that $a =_G 1$ and $b =_G 1$ and conclude that this is a presentation of the trivial group.*

Suppose that $G =< S \mid D >$ is a group given by a presentation. There is a sort of theoretical characterization of those words w such that $w =_G 1$, namely

Lemma 1.4 *Let $G =< S \mid D >$ be a group given by a presentation. If w is any word in the generators of G, then $w =_G 1$ if and only if as an element of the free group F_S there is an equation*

$$w =_{F_S} u_1 r_1^{\epsilon_1} u_1^{-1} u_2 r_2^{\epsilon_2} u_2^{-1} \dots u_k r_k^{\epsilon_k} u_k^{-1}$$

for some words $u_i \in F_S$, $r_i \in D$ and $\epsilon_i = \pm 1$.

To see this, one simply observes that the set of words equal to such expressions contains D and is closed under conjugation, multiplication and inversion. Hence it is N_D, the smallest normal subgroup containing D.

1.3 Dehn's fundamental problems

Suppose we are studying groups given by presentations. We would like to know about the existence and nature of algorithms which decide

- *local properties* – whether or not elements of a group have certain properties or relationships;

- *global properties* – whether or not groups as a whole possess certain properties or relationships.

Such questions are called *decision problems*. The groups in question are assumed to be given by finite presentations or in some other explicit manner.

Historically the following three fundamental decision problems formulated by Max Dehn in 1911 have played a central role:

word problem: Let G be a group given by a finite presentation. Does there exist an algorithm to determine of an arbitrary word w in the generators of G whether or not $w =_G 1$?

conjugacy problem: Let G be a group given by a finite presentation. Does there exist an algorithm to determine of an arbitrary pair of words u and v in the generators of G whether or not u and v define conjugate elements of G?

isomorphism problem: Does there exist an algorithm to determine of an arbitrary pair of finite presentations whether or not the groups they present are isomorphic?

The word and conjugacy problems are decision problems about local properties while the isomorphism problem is a decision problem about a global relationship.

Motivation for studying these questions can be found in algebraic topology. For one of the more interesting algebraic invariants of a topological space is its fundamental group. If a connected topological space T is reasonably nice, for instance if T is a finite complex, then its fundamental group $\pi_1(T)$ is finitely presented and a presentation can be found from any reasonable description of T. The word problem for $\pi_1(T)$ then corresponds to the problem of determining whether or not a closed loop in T is contractible. The conjugacy problem for $\pi_1(T)$ corresponds to the problem of determining whether or not two closed loops are freely homotopic (intuitively whether one can be deformed into the other). Since homeomorphic spaces have isomorphic fundamental groups, a solution to the isomorphism problem would give a method for discriminating between spaces (the homeomorphism problem).

1.4 Homomorphisms

One useful aspect of having a presentation for a group is that it gives us a method of checking whether a proposed map between groups is a homomorphism. Suppose that we have a group given by a presentation, say $G =< S \mid D >$, and that $\psi : S \to H$ is a function. We want to know

whether ψ can be extended to a homomorphism from G to H. Now we do know that ψ extends uniquely to a homomorphism $\tilde{\psi} : F_S \to H$. The map $\tilde{\psi}$ is of course just a formal extension of ψ to all (freely reduced) words.

Recall that $G = F_S/N_D$ where N_D is the normal closure of D. The original ψ extends to a homomorphism if and only if $N_D \subseteq \ker \tilde{\psi}$. Hence ψ extends to a homomorphism if and only if $\tilde{\psi}(r) =_H 1$ for all $r \in D$. We record this observation as

Theorem 1.5 *Let $G =< S \mid D >$ and suppose that $\psi : S \to H$ is a function. Then ψ extends to a homomorphism $\psi : G \to H$ if and only if $\tilde{\psi}(r) =_H 1$ for all $r \in D$ where $\tilde{\psi} : F_S \to H$ is the formal extension of ψ to all words.*

As an illustration, consider the group $G =< a, b \mid ababa = 1 >$ and the infinite cyclic group $C =< t \mid \ >$ with generator t. Consider the function ψ defined by $\psi(a) = t^{-2}$ and $\psi(b) = t^3$. We ask whether ψ extends to a homomorphism. We compute that

$$\tilde{\psi}(ababa) = t^{-2}t^3t^{-2}t^3t^{-2} = t^{6-6} =_C 1$$

and so we can conclude that, yes, ψ extends to a homomorphism.

Continuing this example, the function $\varphi(t) = ab$ extends uniquely to a homomorphism from $\varphi : C \to G$ since C is free with basis t (or technically $\{t\}$). Now

$$(\psi \circ \varphi)(t) = \psi(\varphi(t)) = \psi(ab) = t^{-2}t^3 = t$$

and

$$(\varphi \circ \psi)(a) = \varphi(\psi(a)) = \varphi(t^{-2}) = (ab)^{-2} = a$$
$$(\varphi \circ \psi)(b) = \varphi(\psi(a)) = \varphi(t^3) = (ab)^3 = b$$

where last equations are follow easily from the relation $ababa = 1$, for instance $(ab)^3 = abababab = b$ and $a = (ab)^{-2}ababa$. It follows that the homomorphisms are mutually inverse and hence are both isomorphism. So G is isomorphic to the infinite cyclic group as we claimed earlier.

Here is another illustration using equation notation. Consider the group with presentation $G =< a, t \mid t^{-1}at = a^2 >$. We ask whether the function ψ defined by $\psi(a) = a^2$ and $\psi(t) = t$ extends to a homomorphism from G to itself. To check this we simply compute $\tilde{\psi}$ of both sides of the defining relation and show they are equal.

$$\tilde{\psi}(t^{-1}at) = \psi(t)^{-1}\psi(a)\psi(t) = t^{-1}a^2t = (t^{-1}at)^2 = (a^2)^2 = \tilde{\psi}(a^2).$$

Hence ψ defines a homomorphism from G to itself which we again denote by ψ. Observe that this homomorphism is surjective. For its image contains t

and a^2 and hence also a since $a = ta^2t^{-1}$ is a consequence of the defining relation.

Next consider the function φ defined by $\varphi(a) = tat^{-1}$ and $\varphi(t) = t$. One can check that φ extends to a homomorphism and that ψ and φ are mutually inverse. Hence they are both automorphisms of the group G.

This group is actually one of a family of interesting groups having presentations

$$G_{m,n} =< a, t \mid t^{-1}a^m t = a^n >$$

which are known as *Baumslag-Solitar groups*. In this notation the above group is $G_{1,2}$.

Again consider a presentation of a group $G =< S \mid D >$ and let E be any set of words in F_S. Then the group presented by $< S \mid D \cup E >$ is $F_S/N_{D\cup E}$ which is a quotient group of G. The quotient homomorphism from G to $< S \mid D \cup E >$ is defined by just sending the symbols in S to themselves. Moreover if $\theta : G \to H$ is surjective, then $H \cong F_S/N_{D\cup E}$ for some suitable set of words E; simply take E to be the set of words in the kernel of θ. We record this as follows:

Lemma 1.6 *Let $G =< S \mid D >$ be a presentation of a group and let E be any set of words in F_S. Then the group presented by $< S \mid D \cup E >$ is a quotient group of G with quotient homomorphism defined by the identity map on S. Moreover, every quotient group of G is isomorphic to a quotient of this form.*

Suppose that we have a presentation

$$G =< a_1, a_2, \ldots \mid r_1 = 1, r_2 = 1, \ldots > .$$

Then we can present the *abelianization* $G/[G, G]$ of G (which is the largest abelian quotient), by simply adding all the relations $a_i a_j = a_j a_i$, thus

$$G/[G, G] \cong< a_1, a_2, \ldots \mid a_i a_j = a_j a_i (\forall i, j), r_1 = 1, r_2 = 1, \ldots > .$$

In case the given presentation is finite, one can then use the resulting presentation to compute the decomposition of $G/[G, G]$ as a direct sum of cyclic groups.

1.5 Presentations and fundamental groups

Consider a group G given by a presentation, say

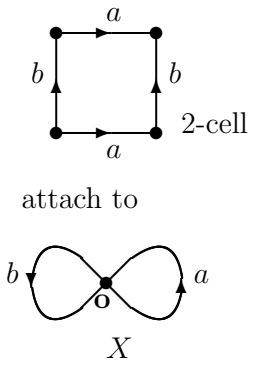
$$G =< a_1, a_2, \ldots, a_n \mid r_1 = 1, r_2 = 1, \ldots, r_m = 1 > .$$

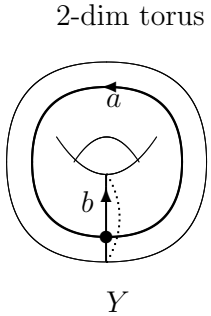
Such a presentation corresponds in a standard way to a 2-dimensional complex Y whose fundamental group is isomorphic to G, that is $G \cong \pi_1(Y, \mathbf{o})$. We review the features of this correspondence. Most of what we say can also be done for presentations with arbitrarily many generators and relations by resorting to CW-complexes. There are no substantial difficulties, just distracting topological niceties.

We start with a single 0-cell which we label as $\mathbf{o}$. For each a_i we take an oriented 1-cell, identify its ends with $\mathbf{o}$ and label its positive direction by the generator a_i. This gives us a space X consisting of a bouquet or wedge of n loops at $\mathbf{o}$. The fundamental group of this space is a free group with basis the (homotopy classes of the) closed loops labeled by the a_i. So we identify $\pi_1(X, \mathbf{o})$ with the free group $F =< a_1, a_2, \ldots, a_n \mid >$.

We now add 2-cells corresponding to the defining relations. For each r_i take a 2-cell, thought of as a disk, and subdivide and label its boundary according to r_i. So if $r_i = a_{j_1}^{\epsilon_1} \ldots a_{j_k}^{\epsilon_k}$ we subdivide the boundary of the 2-cell into k 1-cells with orientation and labeling chosen so that reading in the counter-clockwise direction the label on the boundary is just r_i. We then attach or glue each of these 2-cells to X by identifying the oriented edges in the boundary labeled by a_i with the corresponding loop in X and the 0-cells in the boundary with $\mathbf{o}$. Call the resulting space Y. So Y has a single 0-cell $\mathbf{o}$, a 1-cell for each generator a_i and a 2-cell for each relation r_i. The Seifert-vanKampen Theorem tells us that the fundamental group of Y is just G, that is $G \cong \pi_1(Y, \mathbf{o})$.

As an illustration consider the group $G = \mathbb{Z} \oplus \mathbb{Z}$ which has presentation $G =< a, b \mid aba^{-1}b^{-1} = 1 >$. In this case X consists of 2 loops at $\mathbf{o}$ labeled by a and b. There is a single 2-cell with 4 boundary edges labeled as shown. The space Y is then the 2-dimensional torus which is homeomorphic to $S^1 \times S^1$. As in general, $G \cong \pi_1(Y, \mathbf{o})$.





The universal covering space $\tilde{Y}$ of Y in this example can be identified with the Euclidean plane $\mathbb{R}^2$. With suitable identifications, the 0-skeleton of $\tilde{Y}$ consists of the lattice of points in the plane with integer coordinates and the 1-skeleton $\tilde{Y}^1$ of $\tilde{Y}$ is the grid of horizontal and vertical lines with one integer coordinate.

In the general situation, fix a 0-cell $\tilde{\mathbf{o}}$ in the universal cover $\tilde{Y}$ of Y as a base point. Any word w in the generators of G can be thought of as a closed path λ_w starting in X at $\mathbf{o}$. Now X is just the 1-skeleton of Y, so as a path in Y we can lift λ_w to a unique path $\tilde{\lambda}_w$ in the 1-skeleton $\tilde{Y}^1$ of $\tilde{Y}$ starting at $\tilde{\mathbf{o}}$. Now $\tilde{\lambda}_w$ is a closed path if and only if w belongs to the subgroup of G corresponding to $\tilde{Y}$, that is, if and only if $w =_G 1$. This means that the 1-skeleton $\tilde{Y}^1$ of $\tilde{Y}$ is just the covering space of X corresponding to the normal subgroup N_D of $F_S = \pi_1(X, \mathbf{o})$.

By a graph we mean a 1-dimensional CW-complex. The graph $\tilde{Y}^1$ we have just been considering is called the *Cayley graph* of G (with respect to the given generators) and is usually denoted $\Gamma = \Gamma_{G,S}$ where the decorative subscripts are used when necessary to show the group and generating set. (Notice that Γ does not depend on the particular defining relations used, but rather on the whole normal subgroup N_D.) The Cayley graph is of fundamental importance in the area known as geometric group theory.

1.6 Tietze transformations

There are some alterations one can make to a presentation which result in presentations of a group isomorphic to the original. These are called *Tietze transformations* and we describe them as follows:

$T1$ (add consequences) If in F_S we have a collection of words $E \subseteq N_D$ (and hence $N_D = N_{D \cup E}$), replace $< S \mid D >$ by $< S \mid D \cup E >$.

$T1^{-1}$ (remove redundancies) If in F_S we have a collection of words E such that $N_{D \cup E} = N_D$ (and hence the relators in E are redundant), replace $< S \mid D \cup E >$ by $< S \mid D >$.

$T2$ (introduce abbreviations) If T is a collection of symbols disjoint from S and $\{u_t \mid t \in T\}$ is a set of words on S, replace $< S \mid D >$ by $< S \cup T \mid D \cup \{t^{-1}u_t \mid t \in T\} >$. (The effect here is to introduce abbreviations of the form $t = u_t$ where u_t is a word on the S symbols.)

$T2^{-1}$ (remove abbreviations) If T is a collection of symbols disjoint from S and $\{u_t \mid t \in T\}$ is a set of words on S and the words in D do

not contain T symbols, replace $< S \cup T \mid D \cup \{t^{-1}u_t \mid t \in T\} >$ by $< S \mid D >$. (The effect is to remove abbreviations.)

If only one consequence is introduced (removed) or one abbreviation is introduced (removed) with a transformation, we term the move a *single step* transformation. In general we need to allow more the more general operations, but in finite situations a sequence of single step transformations suffice.

Theorem 1.7 *Suppose that the groups presented by the two presentations $< S \mid D >$ and $< T \mid E >$ are isomorphic. Then there is a sequence of Tietze transformations leading from one of these to the other. If these presentations are both finite the sequence can be taken to be a finite number of single step transformations.*

Roughly the proof proceeds as follows. Use the isomorphisms between the two groups to expand each of the given presentations to a common presentation containing both of the given presentations. Then since the inverse of a transformation is also a transformation, the result follows.

An analogous result is actually true for a large class of algebraic systems and a similar proof can be used.

1.7 Extraction principles

A group G is said to be *finitely generated* if there is some presentation for G on a finite set of generators, that is $G \cong gp(< S \mid D >)$ for some finite set S. Similarly G is said to be *finitely presented* if there is some presentation for G with a finite set of generators and a finite set of relations, that is $G \cong gp(< S \mid D >)$ where both S and D are finite.

Suppose we are given an arbitrary presentation of a group G which satisfies one of these conditions. Is it possible to somehow extract a suitably finite "subpresentation" from the one we have. The answer is provided by the following two results.

Theorem 1.8 *Suppose that G is a finitely generated group and that G is isomorphic to a group with presentation $< T \mid E >$. Then there is a finite subset $T_0 \subseteq T$ and a collection of words D_0 on T_0 such that the inclusion of T_0 into T induces an isomorphism $< T_0 \mid D_0 > \cong < T \mid E >$.*

Even if G is finitely presented in the above result it may not be possible to choose D_0 a finite subset of the given relators E. However, in case the generating set was already finite, this can be done.

Theorem 1.9 *Suppose that G is a finitely presented group and that G is isomorphic to a group with presentation $< T \mid E >$ where T is finite. Then there is a finite subset $E_0 \subseteq E$ such that in F_T the normal subgroups $N_{E_0} = N_E$ and hence $< T \mid E_0 > \cong < T \mid E >$.*

Chapter 2

Construction of new groups

We are going to discuss several methods of constructing new groups from groups we already have in hand. In each case we write down a presentation of the resulting group and give some information on expressing elements in a normal (standard) form.

2.1 Direct products

A hopefully familiar construction is the direct product. Suppose we are given two groups H and K. We can construct their *direct product* $H \times K$ as the set of ordered pairs (h, k) with $h \in H, k \in K$ with multiplication defined by $(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$. The maps defined by $h \mapsto (h, 1)$ an $k \mapsto (1, k)$ embed H and K respectively into $H \times K$. Though of as subgroups in this way H and K are called the *direct factors* of $H \times K$. Observe that $(h, 1)(1, k) = (h, k) = (1, k)(h, 1)$ so the (images of) the direct factors commute in $H \times K$.

Suppose that H and K are given by presentations, say $H =< S \mid D >$ and $K =< T \mid E >$. By changing one of the alphabets if necessary, we can assume S and T are disjoint, that is $S \cap T = \emptyset$. Then a presentation for $H \times K$ can be obtained by joining these together and adding the relations which imply that elements of H commute with elements of K, that is

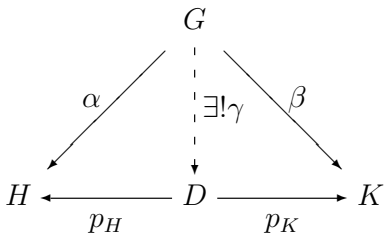
$$H \times K =< S, T \mid D, E,\ st = ts\ \forall s \in S, t \in T > .$$

Here the notation means that generators are those symbols in S and those in T, and similarly for relations. We prefer this to the more set theoretic $S \cup T$.

The inclusion maps on generators induce embeddings of H and K into $H \times K$ presented in this way. The projection of $H \times K$ onto H, for instance, is defined by adding the relations $t = 1\ \forall t \in T$, thus "killing" the factor K.

Observe that every element $w \in H \times K$ can be written by using just the commuting relations $st = ts$ in the form $w = uv$ where u is a word on S and v is a word on T. Moreover, if $w =_{H\times K} 1$ then $u =_H 1$ and $v =_K 1$. This last fact is equivalent to the following: if $w = u_1v_1 = u_2v_2$ where the u_i are words on S and the v_i are words on T, then $u_1 =_H u_2$ and $v_1 =_K v_2$.

There is a more abstract way (arrow theoretic or categorical) to define the direct product of H and K. It goes as follows. A group D is said to be the *direct product* of groups H and K if there are homomorphisms $p_H : D \to H, p_K : D \to K$ satisfying the following condition: for every group G, for every pair of homomorphisms $\alpha : G \to H, \beta : G \to K$ there is a unique homomorphism $\gamma : G \to D$ such that $\alpha = p_H \circ \gamma$ and $\beta = p_K \circ \gamma$.



One easily sees the group $H \times K$ has the properties required of D where γ is defined for any given α, β by $\gamma(g) = \alpha(g)\beta(g)$. A diagram chase using uniqueness now shows that $D \cong H \times K$.

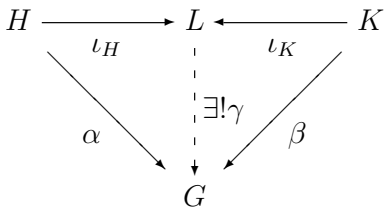
But let's recover the description just using this arrow theoretic definition. Assume that D satisfies the above definition. If we take α to be the identity map on H and β to be the trivial map, we get $p_H \circ \gamma$ is the identity map on H and so p_H is surjective and γ is injective. Hence p_H maps the subgroup $\gamma(H)$ of D isomorphically onto H. For this same choice we have $p_K \circ \gamma$ is the trivial map and so $\gamma(H) \subseteq \ker p_K$.

An analogous choice of α and β for K, shows that p_K maps a subgroup $\delta(K)$ of D isomorphically onto K and that $\delta(K) \subseteq \ker p_H$. Hence we can identify H with $\gamma(H)$ and K with $\delta(K)$ and so think of H and K as subgroups of D and p_H and p_K as retractions onto those subgroups. Now if $h \in H, k \in K$ observe that their commutator $[h, k] \in \ker p_H \cap \ker p_K$ What we expect is that $[h, k] =_D 1$ which follows if we can show this intersection is trivial.

Suppose $1 \neq x \in \ker p_H \cap \ker p_K$. Let C be the infinite cyclic group generated by a and take α and β to be the trivial maps from C to H and K respectively. Now there are two maps which when composed with the projections give α and β: one is the trivial map, the other sends a to x. So this contradicts the uniqueness requirement. Thus $\ker p_H \cap \ker p_K = \{1\}$. Hence also $[H, K] = \{1\}$ and $D = HK$ as desired.

2.2 Free products

Suppose that H and K are two groups. A group L is said to be the *free product* of H and K if there are homomorphisms $\iota_H : H \to L$ and $\iota_K : K \to L$ satisfying the following condition: for any pair of homomorphisms $\alpha : H \to G$ and $\beta : K \to G$ where G is any group, there is a unique homomorphism $\gamma : L \to G$ such that $\alpha = \gamma \circ \iota_H$ and $\beta = \gamma \circ \iota_K$.



An easy diagram chase shows that the free product of H and K is unique (up to to isomorphism) and we will denote it by $H \star K$.

It is easy to see that free products exist because we can just write down a presentation for $H \star K$. Suppose that H and K are given by presentations, say $H =< S \mid D >$ and $K =< T \mid E >$. By changing one of the alphabets if necessary, we can assume S and T are disjoint, that is $S \cap T = \emptyset$. Then a presentation for $H \star K$ can be obtained by joining these together, thus

$$H \star K =< S \cup T \mid D \cup E > .$$

The required maps ι_H and ι_K are just the homomorphisms induced by the inclusions on generators. Both of these are monomorphisms. For instance, if we define $\varphi : H \star K \to H$ by $s \mapsto s, t \mapsto 1 \ \forall s \in S, t \in T$, then φ defines a homomorphism and $\varphi \circ \iota_H$ is the identity on H. So ι_H is a monomorphism. It also follows from this argument that $H \cap K = \{1\}$.

Finally, given homomorphisms α and β as in the definition, the required γ is given by $\gamma(s) = \alpha(s)$ for $s \in S$ and $\gamma(t) = \beta(t)$ for $t \in T$. Then γ defines a homomorphism; since the definition was clearly forced on us, this is the unique such map.

In a sense the free product $H \star K$ is the "freest" group containing H and K. The subgroups H and K are called the *(free) factors* of $H \star K$. The construction can be generalized to any number of factors, say $H_j (j \in J)$, in which case we denote the free product by $\star_{j \in J} H_j$.

By an *alternating word or expression* in $H \star K$ we mean a product of the form $h_1 k_1 \cdots h_m k_m$ where each $h_i \in H$ and each $k_i \in K$; by convention, we allow the possibility that one of h_1 or k_m is not present so that all possible beginnings or ends are covered. The number of terms present is called the *length* of the word. Such an alternating expression is said to be *reduced* if

each $h_i \neq_H 1$ and each $k_i \neq_K 1$. If such an alternating word is not reduced, it is equal in $H \star K$ to a shorter alternating expression obtained by removing one of the terms and regrouping.

Theorem 2.1 (Normal Form Theorem) *Every element of $H \star K$ is equal to a unique alternating expression of the form $h_1 k_1 \cdots h_m k_m$ with $h_i \neq_H 1$ and $k_i \neq_K 1$ when present. Here uniqueness means that if two such expressions are equal in $H \star K$, say*

$$h_1 k_1 \cdots h_m k_m =_{H \star K} h'_1 k'_1 \cdots h'_n k'_n$$

then $n = m$ and each $h_i =_H h'_i$ and each $k_i =_K k'_i$.

That any element is equal to an alternating expression is clear from the presentation. The uniqueness assertion is a non-trivial result and requires proof. The following is an alternate version which is often useful.

Theorem 2.2 (Characterization of free products) *G is the free product of its subgroups H and K if and only if the following two conditions hold:*

1. *H and K generate G, that is every element of G is equal to an some alternating expression $h_1 k_1 \cdots h_m k_m$; and*

2. *if $w \equiv h_1 k_1 \cdots h_m k_m$ is an alternating expression and if $w =_G 1$ then for some i either $h_i =_H 1$ or $k_i =_K 1$.*

As an example, consider the group $G = H \star K$ where $H =< a \mid a^2 = 1 >$ and $K =< b \mid b^3 = 1 >$. Then G has the presentation $G =< a, b \mid a^2 = 1, b^3 = 1 >$. Several questions arise. Is G infinite ? What are the possible orders of the elements of G ? Clearly G has elements of finite order 2 and 3 (and 1 if you consider the identity element).

Consider the element ab. Could its order be finite ? A power of ab has the form $(ab)^n = abab \cdots ab$ which is an alternating word. By the normal form results, if $(ab)^n =_G 1$ then either $a =_H 1$ or $b =_K 1$ and neither is the case. Hence ab has infinite order in G. In fact this argument easily generalizes to show that if H and K are non-trivial groups then $H \star K$ contains an element of infinite order.

An alternating word $h_1 k_1 \cdots h_m k_m$ is said to be *cyclically reduced* if it is reduced and either has length 1 or even length. It follows that a cyclically reduced w alternating word has first and last term from different factors and every cyclic permutation (as an alternating word) is reduced. Also if a cyclically reduced word w has length at least 2, the w has infinite order in $H \star K$, for the same reasons that ab had infinite order in our example.

But by cyclically permuting and reducing as often as possible one arrives at a cyclically reduced word. Hence any alternating word is conjugate to a cyclically reduced word in $H \star K$ Hence an element of finite order must be conjugate to an element of length 1, that is an element of H or K.

We record this observation as follows.

Lemma 2.3 *In the free product $H \star K$, every element of finite order is conjugate to an element of H or of K. If both H and K are non-trivial, then $H \star K$ has elements of infinite order; in fact every reduced alternating word of even length a has infinite order.*

It is reassuring that no new finite orders have been introduced in our construction since we didn't add any equations to force such new orders.

One quite useful fact about free products is the following result whose proof we omit:

Theorem 2.4 (Grushko-Neumann) *The rank of the free product $H \star K$ is the sum of the ranks of H and K.*

Recall that the centre of a group G is $Z(G) = \{x \in G \mid gx = xg \ \forall g \in G\}$.

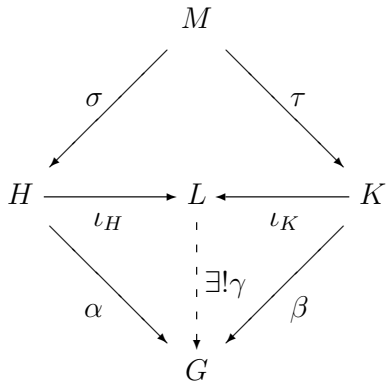
Exercise 2.1 *Show that if both H and K are non-trivial, then $H \star K$ has a trivial centre.*

2.3 Free products with amalgamation

We want to generalize the free product construction to the following: suppose H and K have isomorphic subgroups, so there are a pair of embeddings (monomorphisms) $\sigma : M \to H$ and $\tau : M \to K$. We want to form the "freest" group containing H and K in which their subgroups $\sigma(M)$ and $\tau(M)$ are identified, so hopefully $H \cap K = \sigma(M) = \tau(M)$.

The group L will be called the *free product of H and K with amalgamated subgroup M* if there are maps $\iota_H : H \to L$ and $\iota_K : K \to L$ such that $\iota_H \circ \sigma = \iota_K \circ \tau$ satisfying the following condition: for any pair of homomorphisms $\alpha : H \to G$ and $\beta : K \to G$ such that $\alpha \circ \sigma = \beta \circ \tau$ where G is any group, there is a unique homomorphism $\gamma : L \to G$ such that $\alpha = \gamma \circ \iota_H$ and

$\beta = \gamma \circ \iota_K$.



An easy diagram chase shows that the free product L of H and K with amalgamated subgroup M is unique (up to isomorphism) and we will denote it by $L = H \star_M K$.

It is also easy to see that amalgamated free products exist because we can just write down a presentation for $H \star_M K$. Suppose that H and K are given by presentations, say $H =< S \mid D >$ and $K =< T \mid E >$. Also suppose that $M =< Q \mid V >$ (only the generators of M are relevant here). By changing one of the alphabets if necessary, we can assume S and T are disjoint, that is $S \cap T = \emptyset$. Then a presentation for $H \star_M K$ can be obtained by joining these together and identifying the images of M, thus

$$H \star_M K =< S \cup T \mid D \cup E, \sigma(q) = \tau(q) \ \forall q \in Q > .$$

The required maps ι_H and ι_K are just the homomorphisms induced by the inclusions on generators. Both of these are monomorphisms, but this is not obvious. Also one can show $H \cap K = \sigma(M) = \tau(M)$, but again this is not obvious.

Finally, given homomorphisms α and β as in the definition, the required γ is given by $\gamma(s) = \alpha(s)$ for $s \in S$ and $\gamma(t) = \beta(t)$ for $t \in T$. Then γ defines a homomorphism; since the definition was clearly forced on us, this is the unique such map.

In case the group M is the trivial subgroup, $H \star_M K$ reduces to the free product $H \star K$ discussed previously. We sometimes refer to $H \star K$ as the *ordinary* free product.

There is another convenient notation for the above that is frequently used. Namely, let $A = \sigma(M) \subseteq H$ and $B = \tau(M) \subseteq K$. Then these subgroups A and B are isomorphic via the homomorphism $\varphi = \tau \circ \sigma^{-1} : A \to B$. The amalgamated free product is then often denoted $H \star_{A=B} K$ and is presented

in the following equivalent form:

$$H \star_{A=B} K =< S \cup T \mid D \cup E, a = \varphi(a)\ \forall a \in \sigma(Q) > .$$

We will use both sorts of notation.

The notion of an *alternating word or expression* is as for ordinary free products. The following gives the basic facts concerning this construction.

Theorem 2.5 (Normal Form Theorem - variant)

1. *The maps defined by inclusion of generators induce monomorphisms of H and K into $H \star_M K$; and*

2. *if $w \equiv h_1 k_1 \cdots h_m k_m$ is an alternating word and if $w = 1$ in $H \star_M K$, then for some i either $h_i \in \sigma(M)$ viewed as an element of H or $k_i \in \tau(M)$ viewed as an element of K.*

Again this is a non-trivial result which requires proof. Using this we can show $H \cap K = \sigma(M) = \tau(M)$. Clearly $H \cap K \supseteq \sigma(M) = \tau(M)$. Suppose $g \in H \cap K$. Then $g = h = k$ for suitable words h and k in the generators of H and K respectively. Hence, applying the second conclusion above to $hk^{-1} = 1$ we know either $h \in \sigma(M)$ or $k \in \tau(M)$, and in either case it follows that $g \in \sigma(M) = \tau(M)$.

To state a more traditional version of the normal form theorem, it is convenient to use the $H \star_{A=B} K$ notation introduced above. We first choose a *transversal* Y for the right cosets of A in H, that is Y contains exactly one element (called the *coset representative*) from each right coset Ah where $h \in H$ subject to the condition that the representative chosen for A itself is 1. Similarly we choose a transversal Z for the right cosets of B in K. Using these choices we can state the desired result which is easily seen to be equivalent to the previous version.

Theorem 2.6 (Normal Form Theorem) *Every element of $H \star_{A=B} K$ is equal to a unique alternating expression of the form $a h_1 k_1 \cdots h_m k_m$ with $1 \neq h_i \in Y$ and $1 \neq k_i \in Z$ when present and $a \in A$. Here Y and Z are the transversals chosen above. The uniqueness assertion means that if two such expressions are equal in $H \star K$, say*

$$a h_1 k_1 \cdots h_m k_m =_{H \star_{A=B} K} a' h'_1 k'_1 \cdots h'_n k'_n$$

then $n = m$ and each $h_i = h'_i$ and each $k_i = k'_i$ and $a = a'$.

That any element is equal to an alternating expression is clear from the presentation. The reduction to an expression of this type is not too difficult. But the uniqueness assertion is a non-trivial result and requires proof. The following is an alternate version which is often useful.

Theorem 2.7 (Characterization of amalgamated free products) *G is the free product of its subgroups H and K with amalgamated subgroup $M = H \cap K$ if and only if the following two conditions hold:*

1. *H and K generate G, that is every element of G is equal to an some alternating expression $h_1k_1 \cdots h_mk_m$; and*

2. *if $w \equiv h_1k_1 \cdots h_mk_m$ is an alternating expression and if $w =_G 1$ then for some i either $h_i \in M$ or $k_i \in M$.*

As an illustration consider the two infinite cyclic groups $H =< a \mid >$ and $K =< b \mid >$ with their respective subgroups $A =< a^2 >$ and $B =< b^3 >$ which are isomorphic via the map $a^2 \mapsto b^3$. Then their amalgamated free product is

$$G = H \star_{A=B} K =< a, b \mid a^2 = b^3 > .$$

Observe that the element a^2 lies in the centre of G since $a^2b = b^3b = bb^3 = ba^2$ so that a^2 commutes with the generators of G and hence every element.

Also observe that G is not abelian. For consider the alternating word $w \equiv a^{-1}b^{-1}ab$. If it were the case that $w =_G 1$ then either $a =_H a^{2j}$ or $b =_K b^{3j}$ for some $j \in \mathbb{Z}$ by the normal form results. But neither is the case, so we conclude $w \neq_G 1$.

Exercise 2.2 *Determine the centre of the group $G =< a, b \mid a^2 = b^3 > .$*

Exercise 2.3 *Define a suitable notion of cyclically reduced alternating words for amalgamated free products. Show that every element is conjugate to a cyclically reduced word.*

Exercise 2.4 *Show that in an amalgamated free product, any element of finite order is conjugate to an element of one of the factors.*

2.4 HNN extensions

Suppose that we are given a group G, say by a presentation $G =< S \mid D >$ and a pair of isomorphic subgroups A and B with an isomorphism $\varphi : A \to B$. We want to find a larger group containing G in which the subgroups A and

B are conjugate by an element realizing the isomorphism between them. Naturally we want to do this in the "freest" possible way.

It is easy to write down a candidate for the desired group, but not so easy to show it has the required properties and to give a normal form result. By the *HNN extension* of G with *associated subgroups* A and B via the isomorphism $\varphi : A \to B$ we mean the group G^* with presentation

$$G^* =< S, p \mid D, p^{-1}ap = \varphi(a) \ \forall a \in A > .$$

The additional generator p added here is call the *stable letter*. We note that it suffices to add only the relations $p^{-1}ap = \varphi(a)$ for a ranging over a set of generators for A. (Remark: HNN stands for Higman-Neumann-Neumann, the names of the authors who introduced this construction).

Here is the basic normal form result about this construction.

Theorem 2.8 *Let G^* be the HNN extension of G with associated subgroups A and B via the isomorphism $\varphi : A \to B$. Then*

1. *(Higman,Neumann,Neumann) The identity map on generators induces and embedding of G into G^*, and p generates an infinite cyclic subgroup of G^*.*

2. *(Britton's Lemma) Let w be any word of G^* which involves p, that is either p or p^{-1} appears as a subword. If $w =_{G^*} 1$, then w contains a subword of the form (i) $p^{-1}cp$ or (ii) pcp^{-1}, where c is a word on S, and such that, in case (i) c is equal in G to an element of A, and in case (ii), c is equal in G to an element of B.*

A subword of the form mentioned in Britton's Lemma is called a *p-pinch*, for by using the defining relations in a straight forward way the subword can be replaced by a word on S, thereby reducing the number of p symbols. For instance, suppose $w \equiv upcp^{-1}v$ where $c =_G b \in B$. Then for some $a \in A, \varphi(a) = b$, hence $p^{-1}ap = b$ or equivalently $a = pbp^{-1}$. Thus in G^* we have

$$w \equiv upcp^{-1}v = upbp^{-1}v = uav$$

and this last word has fewer p symbols. A word in G^* is said to be *p-reduced* if it contains no p-pinches. An statement equivalent to Britton's Lemma is the following: a p-reduced word w which involves p must have $w \neq_{G^*} 1$.

In order to give a unique representative for each element in G^*, we again choose two transversals. Let Y be a transversal for the right cosets of A in G, and Z a transversal for the right cosets of B in G (subject to 1 being the chosen representative for A and B). With these choices we can now state

Theorem 2.9 (Unique normal form) *Every element in G^* is equal to a unique expression of the form*

$$g_0 p^{\epsilon_1} g_1 p^{\epsilon_2} g_2 \dots p^{\epsilon_n} g_n$$

where if $\epsilon_i = -1$, then $1 \neq g_i \in Y$; and if $\epsilon_i = +1$, then $1 \neq g_i \in Z$. Here Y and Z are the transversal chosen above.

There are close connection and many parallels between HNN extensions and amalgamated free products. Usually facts about one can easily be deduced from facts about the other. For instance, we remark that the subgroups G and pGp^{-1} of G^* generate their free product with amalgamated subgroup $A = pBp^{-1}$.

As an illustration, consider the infinite cyclic group $G =< a \mid >$ and its two isomorphic subgroups $A =< a >$ and $B =< a^2 >$. Then the corresponding HNN extension has presentation $G^* =< a, p \mid p^{-1}ap = a^2 >$. Let $w \equiv a^{-1}pap^{-1}$. We claim that $w \neq_{G^*} 1$ and hence G^* is not abelian. For if $w =_{G*} 1$, then by Britton's Lemma it must contain a p-pinch. But there is only possibility, at the subword pap^{-1} with $a \in B$. But clearly $a \notin B$ since B consists of the even powers of a. So there is no such pinch and $w \neq_{G*} 1$.

Exercise 2.5 *Define a suitable notion of cyclically p-reduced words for HNN extensions. Show that every element is conjugate to a cyclically p-reduced word.*

Exercise 2.6 *Show that in an HNN extension G^*, any element of finite order is conjugate to an element of G.*

Finally, we remark that the whole discussion above for HNN extensions applies more generally to adding any number of stable letters $p_1, p_2, \dots$ conjugating pairs of isomorphic subgroups $(A_1, B_1), (A_2, B_2), \dots$ onto each other.

Chapter 3

Properties, embeddings and examples

In this chapter we will utilize some of the constructions above to build new groups with interesting properties. In a sense we are exercising the mathematical muscles the results the preceding chapters have developed.

At the outset one might ask a number of naive questions such as the following. Is every subgroup of a finitely generated group, finitely generated? How many finitely generated groups are there (up to isomorphism of course)? Is every finitely generated subgroup of a finitely presented group again finitely presented? These questions among others will be answered in the next two sections.

3.1 Countable groups embed in 2-generator groups

Let $F =< a, b \mid >$ be a free group on two generators a and b. Consider the set of elements $a^{-i}ba^i$ $(i \geq 0)$. One can show that any freely reduced word in these elements is not equal to 1 in F, because in forming such an expression and then reducing in F the central b of each term survives. Hence, by our characterization of freeness, these elements are a free basis for the subgroup they generate. (Notice that this answers one of our naive questions because it shows a subgroup of a finitely generated group need not be finitely generated.)

We use this observation to prove the following remarkable fact.

Theorem 3.1 (Higman, Neumann and Neumann) *Any countable group can be embedded in a group with two generators.*

For let C be a countable group with presentation $C =< c_1, c_2, \ldots \mid D >$ on a countable set of generators. First form the group $L = C \star F$ where $F =< a, b \mid >$ is the free group as above. Now the two subgroups

$$A =< b, c_1 a^{-1} b a, c_2 a^{-2} b a^2, c_3 a^{-3} b a^3, \ldots >$$

$$B =< a, b^{-1} a b, b^{-2} a b^2, b^{-3} a b^3, \ldots >$$

are both free with free bases the listed generators by our previous discussion. So we can form the HNN extension

$$G =< a, b, c_1, c_2, \ldots, t \mid D, t^{-1} b t = a, t^{-1} c_i a^{-i} b a^i t = b^{-i} a b^i \ (i \geq 1) >$$

in which the stable letter t conjugates the basis for A to the basis for B.

We can rewrite these added defining relations of G to put them in the equivalent form

$$c_i =_G t b^{-i} a b^i t^{-1} a^{-i} b^{-1} a^i$$

so the group G is generated by $\{t, a, b\}$. But since $b = tat^{-1}$, the group G is even generated by a and t alone. So if we substitute tat^{-1} for b in the above we get equations of the form $c_i =_G u_i(a, t)$ where the u_i are (suitably complicated) words on a and t. Now the words in D are words on the c_i alone so if we rewrite them in terms of the u_i we obtain a new set of words, say $\overline{D}$. Applying Tietze transformations to eliminate the other symbols, it follows that G can be presented as $G \cong < a, t \mid \overline{D} >$.

Now our previous results on free products imply that C is embedded in L and our results on HNN extensions imply that L is embedded in G. Hence C is embedded in G which is a two generator group. This completes the proof.

Notice that G can be presented with the same number of relations as C. Also observe that by properties of free products and HNN extensions, any element of finite order in G is conjugate to an element of C. Hence the group G has an element of finite order k if and only if C has and element of order k. So we have actually proved slightly more, namely:

Corollary 3.2 *If C is a countable group having a presentation with n generators and m defining relations, then C can be embedded in a group G having 2 generators and m defining relations. Moreover, G can be constructed so that any element of finite order in G is conjugate to an element of C.*

Using this more detailed version, we can also determine how many two generator groups there are (up to isomorphism).

Corollary 3.3 *There are continuously many non-isomorphic two generator groups.*

Observe that there are at most continuously many such groups since there are at most continuously many presentations on two generating symbols. To construct lots of non-isomorphic groups, we start with an arbitrary infinite set P of primes, say $P = \{p_1, p_2, p_3, \ldots\}$. Consider the group with presentation

$$C_P =< c_1, c_2, \ldots \mid c_1^{p_1} = 1, c_2^{p_2} = 1, \ldots, c_i^{p_i} = 1, \ldots >$$

and let G_P be the group constructed for C_P in the previous corollary. Observe that C_P is just the free product of the infinitely many cyclic groups of order $p_i \in P$. Hence C_P and thus G_P contain an element of finite order k if and only if $k \in P$. So if Q is a different set of primes then G_P and G_Q are not isomorphic. Since there are continuously many ways to choose such a set of primes, there are continuously many such non-isomorphic G_P. This completes the proof.

Suppose that $G =< S \mid D >$ is a group and that u and v are two words which have the same order as elements. Then we can form the HNN-extension $G^* =< S, t \mid D, t^{-1}ut = v >$ in which they are conjugate. More generally, if we have a set of such pairs u_i and v_i which have the same order, we can form the HNN extension

$$G^* =< S, t_1, t_2, \ldots \mid D, t_1^{-1}u_1t_1 = v_1, t_2^{-1}u_2t_2 = v_2, \ldots >$$

in which these pairs become conjugate. This observation may be helpful for the following exercise.

Exercise 3.1 (Higman,Neumann and Neumann) *Show that any countable group can be embedded in a countable group in which any two elements of the same order are conjugate. Also show that there is a countable torsion free group in which any two non-trivial elements are conjugate.*

3.2 Non-finite presentability of subgroups

We are going to give an example of a finitely presented group G having a finitely generated subgroup L which is not finitely presented. But to do this we need a method of showing that a group is not finitely presented. The following gives appropriate criteria for HNN extensions and amalgamated free products.

Theorem 3.4 (G. Baumslag)

1. *If $G = H \star_M K$ is an amalgamated free product where H and K are finitely presented groups, and if M is not finitely generated, then G is not finitely presented.*

2. *Let $G =< S \mid D >$ be a finitely presented group with isomorphic subgroups via the isomorphism $\psi : A \to B$. If A is not finitely generated, then the corresponding HNN extension*

$$G^* =< S, t \mid D, t^{-1}at = \psi(a) \ (a \in A) >$$

is not finitely presented.

We prove the second assertion. The proof of the first is similar using facts about amalgamated free products. We can assume that $G =< S \mid D >$ is a finite presentation so that the given presentation of G^* is finite except for the $t^{-1}at = \psi(a)$ relations. Assume on the contrary that G^* is finitely presented. Then, by the extraction theorem, some finite subset $\{D, t^{-1}a_1t = \psi(a_1), \ldots, t^{-1}a_nt = \psi(a_n)\}$ of the given relations suffice.

Let $A_0 =< a_1, \ldots, a_n >$ be the subgroup of A generated by the a_i that appear in these relations. Form the HNN extension of G with associated subgroups A_0 and $\psi(A_0)$ which can be presented as,

$$H =< S, t \mid D, t^{-1}a_1t = \psi(a_1), \ldots, t^{-1}a_nt = \psi(a_n) > .$$

Since A was not finitely generated we know there is some $x \in A \setminus A_0$. Then by Britton's Lemma applied to H we know $t^{-1}xt\psi(x)^{-1} \neq_H 1$. But above we saw $t^{-1}xt\psi(x)^{-1} = 1$ is a consequence of the given relations, which is a contradiction. Hence G^* is not finitely presented.

We are now going to construct an example of a finitely presented group (namely $F \times F$ where F is free of rank 2) which has a finitely generated subgroup L which is not finitely presented. We are going to use the following fact.

Exercise 3.2 *Let $F =< a, b \mid >$ be the free group on a and b and consider the subgroup $K =< a^ib^{-i} \ (i \in \mathbb{Z}) >$. Show that the listed elements are a free basis for K. Also show that K is normal and is in fact the kernel of the quotient map from F onto the group $< a, b \mid a = b >$.*

Let F and K be as in the previous exercise. Form the HNN extension corresponding to the identity isomorphism on K which has presentation

$$L =< a, b, t \mid t^{-1}a^ib^{-i}t = a^ib^{-i} \ (i \in \mathbb{Z}) > .$$

Since the associated subgroup K is not finitely generated, by the previous theorem L is not finitely presented.

Observe the K is a normal subgroup of L. If we let $\varphi : L \to G$ where $G =< a, b, t \mid a = b >$ be the map induced by the identity on generators,

then $K = \ker\varphi$. Observe that G is just a free group on two generators and φ is surjective. It is convenient to change notation slightly and write $G =< s, t \mid >$ where we rename the image of a and b by the letter s.

Let $\psi : L \to F$ be the map which is the identity on F and sends the stable letter t to $1 \in F$. Clearly $\ker\psi \cap F = \{1\}$ so that $\ker\varphi \cap \ker\psi = \{1\}$. Hence the map $\gamma : L \to F \times G$ defined by $\gamma(x) = (\psi(x), \varphi(x))$ is a monomorphism and so L embeds in $F \times G$. In terms of the given generators we have $\gamma(a) = (a, s)$, $\gamma(b) = (b, s)$ and $\gamma(t) = (1, t)$. We summarize this as follows.

Theorem 3.5 *Let $F =< a, b \mid >$ and $G =< s, t \mid >$ be two free groups. Their direct product $D = F \times G$ is finitely presented, for instance by*

$$D \cong < a, b, s, t \mid as = sa, bs = sb, at = ta, bt = tb >$$

but the subgroup L of D generated by the three elements $\{(a, s), (b, s), (1, t)\}$ is not finitely presented.

Later we will discuss a remarkable theorem of Graham Higman which actually characterizes those finitely generated groups which are subgroups of finitely presented groups.

3.3 Hopfian and residually finite groups

A group G is said to be *hopfian* if $G/N \cong G$ implies $N = \{1\}$, that is, every epimorphism $\alpha : G \to G$ is an automorphism.

Being hopfian has aspects of a finiteness property. Clearly any finite group is hopfian since a function from a finite set onto itself is a bijection. A free group F_S with an infinite basis $S = \{a_1, a_2, \ldots\}$ is not hopfian since $\alpha(a_1) = 1, \alpha(a_{i+1}) = a_i$ $(i \geq 1)$ defines a homomorphism $\alpha : F_S \to F_S$ which is surjective but not injective.

We will eventually see that all finitely generated free groups are hopfian and all finitely generated abelian groups are hopfian. It is also known that all finitely generated groups of matrices are hopfian. So one might ask whether all finitely presented groups are hopfian since they satisfy one sort of finiteness condition. The answer is no as the following simple example shows.

Theorem 3.6 (Baumslag-Solitar) *The group with presentation*

$$G =< a, t \mid t^{-1}a^2t = a^3 >$$

is non-hopfian

To prove this we define $\psi(t) = t$ and $\psi(a) = a^2$. To see that ψ defines a homomorphism we observe that $\psi(t^{-1}a^2t) = t^{-1}a^4t =_G a^6 = \psi(a^3)$. Also since $a =_G t^{-1}a^2ta^{-2}$ the homomorphism ψ is surjective and hence an epimorphism.

Now $[t^{-1}at, a] \equiv t^{-1}a^{-1}ta^{-1}t^{-1}ata \neq_G 1$ by Britton's Lemma since there are no t-pinches possible. But

$$\psi([t^{-1}at, a]) = [t^{-1}a^2t, a^2] =_G [a^3, a^2] = 1$$

so that $[t^{-1}at, a]$ is a non-trivial element in the kernel of ψ. Hence ψ is not an isomorphism as desired.

Exercise 3.3 (G. Higman) *Show that the group with presentation*

$$H =< a, p, q \mid p^{-1}ap = a^2, q^{-1}aq = a^2 >$$

is non-hopfian.

There is a large class of finitely generated groups which turn out to be hopfian, namely, the *residually finite* groups. Before proving this result, we briefly discuss residual properties in general.

Let $\mathcal{P}$ be a property of groups which is abstract in the sense that it depends only on the isomorphism type of the group and not on the way it is presented or defined. For example "being finite" is such a property. A group G is said to be *residually-$\mathcal{P}$* if for every $1 \neq g \in G$ there is a surjective homomorphism $\psi : G \to H$ where $H \in \mathcal{P}$ with $\psi(g) \neq_H 1$. Equivalently, if for every $1 \neq g \in G$ there is a normal subgroup N_g of G such that $g \notin N_g$ and $G/N_g \in \mathcal{P}$. Thus the fact that $g \neq_G 1$ is witnessed in some quotient group of G which enjoys the property.

For example the infinite cyclic group $C =< a \mid >$ is residually finite. To see this observe that if a^n $(n \neq 0)$ is any nontrivial element, then $a^n \notin < a^{2n} >$ and $C/ < a^{2n} >$ is finite. Also any finite group is residually finite.

Exercise 3.4 *Show that the direct product of two residually-$\mathcal{P}$ groups is residually-$\mathcal{P}$*

A property $\mathcal{P}$ is said to be *hereditary* if every subgroup H of a group $G \in \mathcal{P}$ also has property $\mathcal{P}$. Examples of hereditary properties are "being finite", "being abelian", "being nilpotent" "being solvable" and so on.

Exercise 3.5 *Show that residually abelian is the same as abelian. Show that residually-(residually-$\mathcal{P}$) is the same as residually-$\mathcal{P}$.*

Exercise 3.6 *Show that if $\mathcal{P}$ is a hereditary property, then G is residually-$\mathcal{P}$ if and only if G is isomorphic to a subgroup of an (unrestricted) direct product of groups with property $\mathcal{P}$.*

We want to investigate residual finiteness, but to do so we need a few facts about subgroups of finite index in groups. We pose these as exercises.

Exercise 3.7 *Let G be a group and let H and K be two subgroups of finite index in G. Show that $H \cap K$ has finite index in G.*

Exercise 3.8 *Let G be a group and H a subgroup of finite index in G. Show that H contains a subgroup N which is normal in G and $[G : N] < \infty$.*

Exercise 3.9 *Show that if G is a finitely generated group and $1 \leq k \in \mathbb{N}$, then there are at most finitely many subgroups of G of index k.*

Exercise 3.10 *Show that G is residually finite if and only if the intersection of all of the subgroups of finite index in G is the trivial subgroup $\{1\}$.*

The following useful result provides more examples of residually finite groups.

Theorem 3.7 *If H and K are residually finite, then their free product $H \star K$ is residually finite.*

We first observe that it suffices to consider the case in which both H and K are finite groups. For if $w \equiv h_1 k_1 \dots h_n k_n \neq_{H\star K} 1$ is a reduced word, since H and K are residually finite they have normal subgroups finite index N and M respectively such that the $h_i \notin N$ and the $k_i \notin M$. Hence the image of w in the quotient group $(H/N) \star (K/M)$ is reduced and has the same length as w and so is not equal to 1. So it suffices to show this latter, which is the free product of two finite groups, is residually finite. Hence we can assume from now on that H and K are finite groups.

Now assume $w \equiv h_1 k_1 \dots h_n k_n \neq_{H\star K} 1$ is a reduced word of length m. Let Ω_m be the collection of all elements of $H \star K$ of length at most m, so that Ω_m is a finite set. We let H act on Ω_m by the following rule: if $u \in \Omega_m$ the $h \cdot u = hu$ if the length of hu after reduction is $\leq m$; otherwise $h \cdot u = u$. Once can check this is an action and therefore it defines a homomorphism $\alpha : H \to Sym(\Omega_m)$, the group of all permutations of Ω_m. Similarly define an action of K on Ω_m which gives a homomorphism $\beta : K \to Sym(\Omega_m)$. Hence, by the definition of free product, there is a homomorphism $\gamma : H \star K \to Sym(\Omega_m)$ which extends these. Thus the two actions extend to an action of $H \star K$ on Ω_m.

Now the element w acting on $1 \in \Omega_m$ yields w, that is $w \cdot 1 = w$ and so w acts non-trivially. Thus $\gamma(w) \neq 1$ in $Sym(\Omega_m)$ and this later is a finite group. Thus for any non-trivial element w we have found a homomorphism to a finite group which sends w to a non-trivial element. Hence $H \star K$ is residually finite. This completes the proof.

Since a free group is a free product of infinite cyclic groups, we conclude

Corollary 3.8 *Free groups are residually finite.*

Linear groups provide a rich source of residually finite groups because of the following which we state without proof.

Theorem 3.9 (Malcev) *A finitely generated linear group (group of matrices) is residually finite.*

At last we are ready to prove an assertion we made in connection with the hopfian property.

Theorem 3.10 (Malcev) *Finitely generated residually finite groups are hopfian.*

For suppose that G is finitely generated and residually finite. Let $\psi : G \to G$ be an epimorphism. Let H be a subgroup of finite index, say $n = [G : H]$. Then $\psi^{-1}(H)$ is again a subgroup of finite index n in G (which contains $\ker \psi$). If K is another subgroup of G having this same index n, so $H \neq K$, then $\psi^{-1}(H) \neq \psi^{-1}(K)$. Hence ψ^{-1} defines an injection from the set Θ_n of subgroups of G having index n into itself. But by the exercises above Θ_n is a finite set and so ψ^{-1} must be a bijection. Thus

$$\ker \psi \subseteq \bigcap_{H \in \Theta_n} H.$$

Hence $\ker \psi$ lies in the intersection of all of the subgroups of finite index in G. Since G is residually finite, that intersection is the trivial subgroup, so ψ is an isomorphism. This completes the proof.

Chapter 4

Subgroup Theory

We are going to discuss the structure of subgroups of various kinds of groups introduced above.

4.1 Subgroups of Free Groups

We first consider subgroups of free groups. The general case is easily dealt with, but in the case of a finitely generated subgroup algorithms and more information are available.

4.1.1 The general case

The fundamental group of a graph Y is easy to compute. We first choose a maximal tree T in Y. Contracting T to the base point yields a bouquet of circles at the base point, one circle for each edge of Y not in T. Hence the fundamental group of Y is free with basis the loops formed by connecting the edges not in T to the base point by paths in T from their vertices.

Using this observation we prove the following *Nielsen-Schreier* theorem.

Theorem 4.1 *Subgroups of free groups are free.*

The fundamental group of any graph is free. A free F group is the fundamental group of a suitable graph X. A subgroup H of F is the fundamental group of a corresponding covering space Y of X. But Y is again a graph, so H is free.

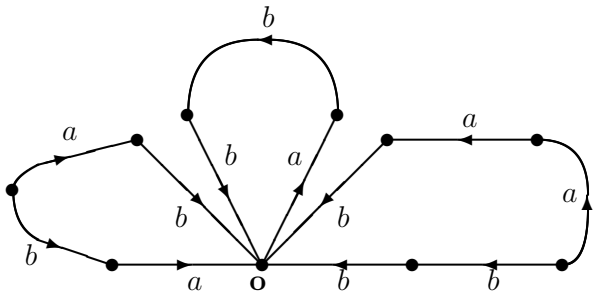
4.1.2 Finitely generated subgroups of free groups

Let F be a free group and H the subgroup of F generated by a finite set of words $H =< w_1, \ldots, w_m >$. We know that H is actually a free group, but

the w_i may not be a free basis. There are graphical and computational methods available to construct a basis for H which give algorithms for deciding membership in H and computing coset representatives. It is convenient to discuss an extended example of these methods rather than give a theoretical description.

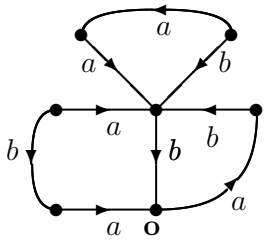
Suppose for example that we are interested in the free group F with two free generators a and b. Consider the subgroup H of F generated by the three words $w_1 = b^{-2}a^2b, w_2 = ab^2, w_3 = b^{-1}a^{-1}ba$.

We begin by forming three loops in the plane joined at a common vertex labeled **o**. We then subdivide each loop and orient and label the resulting edges according the the words w_i in the usual manner. This gives us the following initial (oriented and labeled) graph.

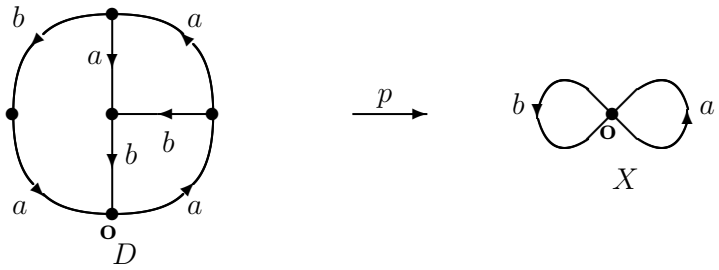


Initial graph

Now observe that there are four edges labeled b coming into the vertex **o**. We identify these edges and also identify the vertices they come from to reduce the graph to the following:



In this graph there are two edges labeled a and two edges labeled b entering the central vertex. If we first identify the b edges and then the a edges, we obtain (after two steps) the graph D shown at the left below.



This graph D now has the property that at any vertex at most one edge arriving at that vertex is labeled by a given generator and at most one edge leaving that vertex is labeled by a given generator. We say that such a graph is *reduced*.

Observe that there is a continuous map p from this graph D to the standard space X with fundamental group F consisting of two oriented loops at $\mathbf{o}$ labeled by a and b. The map p sends all the vertices to $\mathbf{o}$ and the oriented edges homeomorphically onto the corresponding oriented loops. Observe that the induced map on fundamental groups has $p_*(\pi_1(D, \mathbf{o})) = H \subseteq F = \pi_1(X, \mathbf{o})$ since the image is generated by the words w_i.

Let $\tilde{X}$ denote the universal covering space of X. So $\tilde{X}$ is a tree and at each vertex there is exactly one edge leaving and one edge entering labeled by each of the generators a and b. As it stands D is not a covering space of X. But we can enlarge D to a covering space Y of X by adding infinite branches from $\tilde{X}$ corresponding to missing edges. For example at $\mathbf{o}$ there is no outgoing edge labeled b. So in $\tilde{X}$ we remove an outgoing branch labeled b (that is, the component obtained by cutting that edge) and glue this branch on to D at $\mathbf{o}$. The map p extends to this added branch in the obvious way. Repeating this for each missing edge at each vertex of D we obtain a space Y and an extension of p. Now (Y, p) is a covering space since at each vertex there is exactly one edge leaving and one edge entering labeled by each of the generators a and b. Moreover, since Y is formed by attaching trees at various vertices of D, the graph D is a deformation retract of Y and $p_*(\pi_1(Y, \mathbf{o})) = p_*(\pi_1(D, \mathbf{o})) = H$.

In general, starting with a finite set of generators for a subgroup H of F, we obtain in this way a graph D_H and a covering space $Y_H \supseteq D_H$ corresponding to H. Now the index of H in F is the number of vertices of Y_H which is infinite unless $Y_H = D_H$. Thus the graph D_H constructed in this way is a covering space of X if and only if H has finite index in F.

Thus one way to think of D is as the *core* of the covering space Y corresponding to H obtained by removing all infinite tree branches. But there is also way to regard D as the graph of a finite state automaton for determining

membership in H.

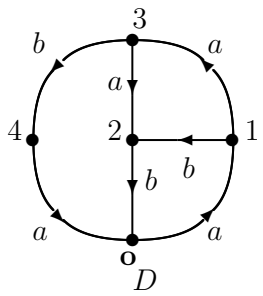
For suppose u is a freely reduced word in the generators of F. By covering space theory, $u \in H$ if and only if tracing out the word u starting from $\mathbf{o} \in Y$ along the corresponding labeled edges we return to $\mathbf{o}$ exactly at the end of u. Since u is freely reduced the corresponding path must must consist of a path in D possibly followed by a path off into one of the added branches at the end. Thus $u \in H$ if and only if u corresponds to a path entirely in D which returns to $\mathbf{o}$ at the end.

To determine membership of a freely reduced word u in H, we start tracing out u in D from $\mathbf{o}$. If there is ever no edge corresponding to the next symbol in u, then we know $u \notin H$ (in Y we would go off into one of the infinite branches here). If we finish the path corresponding to u and are not at $\mathbf{o}$, then again $u \notin H$. Finally if we finish at $\mathbf{o}$, then $u \in H$ so the test was successful.

Remark: D can also be used to compute a unique coset representative with respect to H for any word in F.

So the vertices of D can be regarded as the states of a finite state automaton and the edges as giving the transition instructions depending on the next symbol being read.

The information needed here is conveniently described in tabular form which we call the *automaton table*. First we number the vertices of D in some manner, for instance as shown below (with 0 the number of $\mathbf{o}$).



D

The table is to have one row for each vertex. The columns of the table correspond to the generators of F and their inverses. The number j in row i in the column headed by generator a means there is an edge with label a from vertex i to vertex j. The number j in row i in the column headed by inverse a^{-1} of a generator means there is an edge with label a from vertex j to vertex i. If there is no edge at vertex i with the given label a -1 is placed in the table.

The automaton table for the graph D of our example is shown at the left below:

Automaton Table

Vertex	Label a	a^{-1}	b	b^{-1}
o	1	4	-1	2
1	3	**o**	2	-1
2	-1	3	**o**	1
3	2	1	4	-1
4	**o**	-1	-1	3

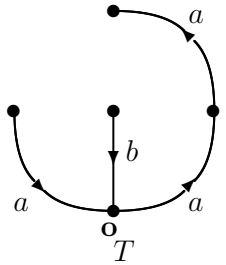
Edge Table

Edge	Label	Initial	Terminal
1	a	0	1
2	b	2	0
3	a	4	0
4	b	1	2
5	a	1	3
6	a	3	2
7	b	3	4

With any graph we can also associate what we term an *edge table*. This is a table with one row for each edge of the graph. Each edge is considered in the positive orientation of the labeling generator, and the row in the table for the edge contains the labeling generator and the numbers of the initial and terminal vertices. The edge table for our example D is shown at the right above.

It is computationally quite easy to pass between these two tables if the graph is reduced. To even write down the automaton table we must have a reduced graph. But the edge table makes sense in general, and the reduction process described before can be carried out on a computer using the edge table for the graph.

In order to write down a *Nielsen basis* for the subgroup H we first select a maximal tree T in D with root **o**. First we choose an edge from each vertex at distance 1 from **o** back to **o** - this gives a subtree T_1. Then choose an edge from each vertex at distance 2 from **o** back to T_1 - this gives a larger tree T_2; and so on. There is a simple procedure for doing this by passing through the above automaton table d times where d is the maximum distance of any vertex from **o**. Such a maximal tree for our example is shown below.



In such a maximal tree T there is a unique reduced path from any vertex to **o**. This information is conveniently recorded in the following table which completely describes T.

Vertex	Previous	Label	Distance
o	-	-	0
1	**o**	a^{-1}	1
2	**o**	b	1
3	1	a^{-1}	2
4	**o**	a	1

As usual, H is free on the omitted edges, and a Nielsen basis for H is

$$u_1 = a\underline{b}b, \quad u_2 = aa\underline{a}b, \quad u_3 = aa\underline{b}a$$

where the underlined symbol corresponds to the edge omitted from T. This underlined symbol is isolated in the sense it remains uncancelled when forming freely reduced words in the u_i.

Exercise 4.1 *Let F be the free group with free basis $\{a, b\}$ and consider the subgroup $H =< ba^{-1}, b^{-1}a, a^3, aba >$ generated by the listed elements. Determine the automata graph D_H of H. Also find the corresponding automaton table and edge table. Finally find a Nielsen basis for H. What is the index of H in F?*

Exercise 4.2 *Repeat the previous exercise for the subgroup*

$$K =< a^2, ab^2, ab^{-2}, b^{-1}ab^{-1}, b^{-1}a^{-1}b^{-1} > .$$

If we are given two finite sets of elements of F which generate subgroups H and K, we can find the corresponding reduced automata graphs D_H and D_K as above. We also have two maps $p_H : D_H \to X$ and $p_K : D_K \to X$.

Now form the pull-back Z of these two maps. Then Z is a graph with vertex set the collection of pairs (u, v) where u is a vertex of D_H and v is a vertex of D_K. There is an edge labeled by a generator a from vertex (u_1, v_1) to vertex (u_2, v_2) in Z if and only if there is both an edge labeled by a in D_H from u_1 to u_2 and an edge labeled by a in D_K from v_1 to v_2.

The component of the vertex $(\mathbf{0}_H, \mathbf{0}_K)$ in the pull-back graph Z of these two graphs is then a reduced graph which accepts exactly those words in $H \cap K$, and so it is the graph $D_{H\cap K}$. In particular, $H \cap K$ is finitely generated and this gives an algorithm for finding its automata graph and hence a set of generators. In particular we have proved the following.

Theorem 4.2 (Howson) *The intersection of two finitely generated subgroups of a free group is again finitely generated.*

Exercise 4.3 *Let F, H and K be as in the previous two exercices. Determine the automata graph $D_{H\cap K}$ of their intersection. Also find the corresponding automaton table and edge table. Finally find a Nielsen basis for $H \cap K$. What is the index of $H \cap K$ in F?*

4.2 Subgroups of presented groups

Suppose we are given a group G by a presentation. It is convenient to write this presentation as

$$G =< a_1, a_2, \ldots \mid r_1 = 1, r_2 = 1, \ldots >$$

although the sets of generators and relations need not be countable. Our notation will be cumulative for this section and somewhat at variance from that used in other sections.

Suppose that H is a subgroup of G. We want to find a presentation for H. To this end, we inductively choose a set of words T in the generators of G which are a transversal for the right cosets Hx of H in G. First we choose the empty word 1 as the representative of H. By the *length* of a coset Hx we mean the length of the shortest word in the generators of G representing an element of Hx. Suppose that representatives have been chosen for all cosets of length n. For each coset of length $n+1$, select an element of length $n+1$, say $a_{i_1}^{\epsilon_1} \ldots a_{i_n}^{\epsilon_n} a_{i_{n+1}}^{\epsilon_{n+1}}$. Then as representative of this coset, choose the element

$$\overline{a_{i_1}^{\epsilon_1} \ldots a_{i_n}^{\epsilon_n}} a_{i_{n+1}}^{\epsilon_{n+1}}$$

where $\overline{a_{i_1}^{\epsilon_1} \ldots a_{i_n}^{\epsilon_n}}$ is the representative already chosen for $a_{i_1}^{\epsilon_1} \ldots a_{i_n}^{\epsilon_n}$.

If $x \in G$ we denote the coset chosen representative of x by $\overline{x}$ so $\overline{x} \in T$. We use the letters K and M as variables ranging over these the chosen representatives in T. Observe that by construction an initial segment of a representative is again a representative.

Topological interpretation: We can realize G in the standard way as the fundamental group of a 2-complex X with a single 0-cell, so $G \cong \pi_1(X, \mathbf{o})$. Let Y be the covering space corresponding to H so $H = \pi_1(Y, \tilde{\mathbf{o}})$. We then choose an "expanding maximal tree" T based at $\tilde{\mathbf{o}}$. Each coset of H corresponds to a 0-cell of Y, and the unique reduced path in T joining $\tilde{\mathbf{o}}$ to a 0-cell can be taken as a coset representative. Again an initial segment of a representative is a representative.

We want to find a presentation for H. To this end, for each $K \in T$ and each generator a_i of G we introduce a new symbol s_{K,a_i}. Each such symbol is to represent the element $Ka_i(\overline{Ka_i})^{-1}$ of H. We now define a *rewriting process* τ which assigns to each word in the a_i a corresponding word in the s_{K,a_i}. Given a word $w \equiv a_{i_1}^{\epsilon_1} \ldots a_{i_n}^{\epsilon_n}$ in the generators of G, we define $\tau(w)$ as follows: $\tau(w)$ is the word obtained from w by replacing the j-th symbol $a_{i_j}^{\epsilon_j}$ by the following rule: if $\epsilon_j = 1$ replace $a_{i_j}^{\epsilon_j}$ by in $s_{K,a_{i_j}}$ where

$$K = \overline{a_{i_1}^{\epsilon_1} \ldots a_{i_{j-1}}^{\epsilon_{j-1}}},$$

and if $\epsilon_j = -1$ replace $a_{i_j}^{\epsilon_j}$ by in $s_{K,a_{i_j}}^{-1}$ where

$$K = \overline{a_{i_1}^{\epsilon_1} \dots a_{i_j}^{\epsilon_j}}.$$

Remark: In the topological interpretation the path corresponding to $Ka_i(\overline{Ka_i})^{-1}$ goes out along K in the maximal tree T, then across the edge labeled a_i then back to $\tilde{\mathbf{o}}$ in the tree T. If the edge labeled a_i is in T then the path back to $\tilde{\mathbf{o}}$ is the same as that going out, so the whole path is homotopically trivial. Otherwise it is a genuine loop in the 1-skeleton of $\tilde{Y}$. The set of such loops generate $\pi_1(Y, \tilde{\mathbf{o}})$. The effect of τ is to express any path as a product of these followed by the unique path in T back to $\tilde{\mathbf{o}}$. If the path is closed, it expresses the path in terms of the generators for $\pi_1(Y, \tilde{\mathbf{o}})$.

Observe that it can happen that Ma_i and $\overline{Ma_i}$ are freely equal (topologically they are homotopic in T). In this case we must have $s_{M,a_i} =_H 1$.

With the above notation we are now ready to specify how to present subgroups of groups given by presentations.

Theorem 4.3 (Reidemeister-Schreier) *Suppose that G is a group given by a presentation*

$$G =< a_1, a_2, \dots \mid r_1 = 1, r_2 = 1, \dots >$$

and that H is a subgroup of G. Choose a transversal T and introduce a rewriting process τ as above. Then H can be presented as follows:

1. generators*: s_{K,a_i} for each $K \in T$ and each a_i*
2. relators*: $s_{M,a_i} = 1$ whenever Ma_i and $\overline{Ma_i}$ are freely equal; and $\tau(Kr_jK^{-1}) = 1$ for each $K \in T$ and each relator r_j in the presentation for G.*

In case the index of H in G is finite (so the number of $K \in T$ is finite) and the number of a_i's is finite (so G is finitely generated) we can draw the following consequences.

Corollary 4.4 *1. If G is a finitely generated group and H a subgroup of finite index, then H is finitely generated.*

2. If G is a finitely presented group and H a subgroup of finite index, then H is finitely presented.

Here are some exercises in carrying out the Reidemesister-Schreier procedure for presenting subgroups.

Exercise 4.4 *Let $G = S_3 = D_3 =< a, b \mid a^2 = b^3 = 1, aba = b^{-1} >$ which is the non-abelian group of order 6. Use the Reidemeister-Schreier method to obtain a presentation for $H =< b >$ the normal subgroup of order 3. Then use Tietze transformations to simplify the presentation you get. Repeat the exercise for the subgroup $< a >$ which has order 2 but is not normal.*

Exercise 4.5 *Let $G =< a, b \mid b^{-1}ab = a^2 >$ and let H be the normal closure of a, that is the kernel of the map from G onto the infinite cyclic group $< b >$. Use the Reidemeister-Schreier method to obtain a presentation for H. Then use Tietze transformations to simplify the presentation you get.*

Exercise 4.6 *Let F be the free group with basis $\{a, b\}$ and let $H = [F, F]$ be its commutator subgroup. Find a free basis for H by using the Reidemeister-Schreier method to obtain a presentation for H.*

4.3 Subgroups of free products

The subgroups of an (ordinary) free product have a particularly simple structure as described in the following.

Theorem 4.5 (Kurosh Subgroup Theorem) *Let $G = \star_{i\in I} H_i$ be the free product of a collection of groups H_i. If A is a subgroup of G, then A decomposes as a free product of the form*

$$A = F \star (\star_{i\in I}(\star_{j\in J(i)} A \cap u_j H_i u_j^{-1}))$$

where F is a free group. That is, A is the free product of a free group and of various subgroups which are the intersections of A with conjugates of the H_i.

A fairly straight forward proof using covering spaces can be found in Massey's text [5]. It also follows from the more general results described in the next section.

Note that applying the Kurosh Subgroup Theorem to the free product of infinite cyclic groups implies that subgroups of free groups are free. Here are a few other special cases.

Corollary 4.6 *If a subgroup A of a free product $G = \star_{i\in I} H_i$ intersects each conjugate of an H_i trivially, then A is a free group. In particular if A is a normal subgroup which intersects each H_i trivially, then A is free.*

Corollary 4.7 *The kernel of the epimorphism $H \star K \to H \times K$ is a free group.*

4.4 Groups acting on trees

The subgroup structure of amalgamated free products and HNN extensions is more difficult to describe. In fact one considers a more general notion of a *graph of groups* which is a graph together with a collection of groups corresponding to vertices and a collection of (sub)groups corresponding to edges end embeddings of the edge groups into the vertex groups of their initial and terminal vertices. There is a notion of the *fundamental group* of such a graph of groups; ordinary free products, amalgamated free products and HNN extensions are all special cases.

By considering the universal cover, such a graph of groups acts on a suitable tree (all actions here are without inversions). The stabilizers of vertices are the vertex groups and the stabilizers of edges are the edge groups. Conversely any group acting on a tree has a description in these terms. In particular, a group is free if and only if it acts freely on a tree. Hence subgroups of free groups are free.

Using these methods rather detailed structural information about subgroups of all these objects can be obtained. The reader is referred to the book by Serre [9] or the notes by Scott and Wall [8] for two different (but related) accounts of this theory.

Chapter 5

Decision Problems

5.1 The word and conjugacy problems

A finite presentation π of a group is a piece of notation such as

$$< x_1, \ldots, x_n \mid r_1 = 1, \ldots, r_m = 1 >$$

where the x_i are letters in some fixed alphabet and the r_j are words in the x_i and their inverses x_i^{-1}. The group presented by π, denoted $gp(\pi)$, is the quotient group of the free group on the x_i by the normal closure of the r_j. Usually it is not necessary to distinguish so carefully between a group and its presentation and we often write simply

$$G =< x_1, \ldots, x_n \mid r_1 = 1, \ldots, r_m = 1 >$$

to mean the G is the group defined by the given presentation.

It is convenient to introduce some notation for several decision problems we will consider. Suppose that G is a finitely presented group defined by a presentation as above. Then the *word problem* for G is the decision problem

$$WP(G) = (?w \in G)(w =_G 1).$$

Here the "?" is intended as a sort of quantifier and should be read as "the problem of deciding for an arbitrary word w in G whether or not ...." A closely related problem is the *equality problem*:

$$EqP(G) = (?w_1, w_2 \in G)(w_1 =_G w_2).$$

Of course, $w_1 =_G w_2$ if and only if $w_1 w_2^{-1} =_G 1$ so that an algorithm for solving either of $WP(G)$ or $EqP(G)$ easily yields an algorithm for solving the

other. On the other hand, from the viewpoint of computational complexity, these problems are subtly different.

Again using this "?" quantifier, the *conjugacy problem* for G is

$$CP(G) = (?u, v \in G)(\exists x \in G)(x^{-1}ux =_G v).$$

If H is a finitely generated subgroup of G and if H given by say a finite set of words which generate it, then the *generalized word problem* for H in G is the problem of deciding for an arbitrary word w in G whether or not w lies in the subgroup H, that is

$$GWP(H, G) = (?w \in G)(w \in H).$$

When the subgroup H is an arbitrary finitely generated subgroup rather than a fixed one we write simply $GWP(G)$.

On the face of it, each of these algorithmic problems appears to depend on the given presentation. We will show below that the solvability of each of these problems is independent of the finite presentation chosen. It can happen that for a particular finitely presented group each of the above problems is solvable. For instance, if G is a finite group given by a multiplication table presentation, it is easy to describe algorithms for solving $WP(G)$, $CP(G)$ and $GWP(G)$. Similarly, if $F =< x_1, \ldots, x_n \mid >$ is a finitely generated free group $WP(F)$ is solved by freely reducing and $CP(F)$ is solved by cyclically permuting and freely reducing. The $GWP(H, F)$ for finitely generated subgroups H of F is more difficult and its solution is due to Nielsen (see [4]).

Finally, in terms of the "?" notation, the *isomorphism problem* for finitely presented groups is

$$IsoP = (?\pi_1, \pi_2 \text{ finite presentations})(gp(\pi_1) \cong gp(\pi_2)).$$

We assume the reader is familiar with the rudiments of the theory of algorithms and recursive functions. Thus a set of objects is *recursive* if there is an algorithm for deciding membership in the set. A set S of objects is *recursively enumerable* if there is an algorithm for listing all the objects in S. It is easy to see that every recursive set is recursively enumerable. Moreover, a set S is recursive if and only if both S and its complement are recursively enumerable. A diagonal argument can be used to prove the important result that there exists a set which is recursively enumerable but not recursive. This fact is in a sense the source of all undecidability results in mathematics.

Each of the above decision problems is recursively enumerable in the sense that the collection of questions for which the answer is "Yes" is recursively enumerable. For instance, the set of words w of G such that $w =_G 1$ is

recursively enumerable. For it is the set of words freely equal to a product of conjugates of the given finite set of defining relations and this set can (in principle) be systematically listed. Thus $WP(G)$ is recursively enumerable. Now $WP(G)$ is recursively solvable (decidable) exactly when the set of words $\{w \in G \mid w =_G 1\}$ is recursive. So $WP(G)$ is recursively solvable if and only if $\{w \in G \mid w \neq_G 1\}$ is recursively enumerable.

Similarly, one can systematically list all true equations between words of G and all true conjugacy equations so that $EqP(G)$ and $CP(G)$ are recursively enumerable. $GWP(H, G)$ is recursively enumerable since one can list the set of all true equations between words of G and words in the generators of H. Finally, if two presentations present isomorphic groups, then one can be obtained from the other by a finite sequence of Tietze transformations. Since the set of presentations obtainable from a given one by a finite sequence of Tietze transformations is recursively enumerable, it follows that $IsoP$ is recursively enumerable.

We recall the notion of Turing reducibility. If A and B are two sets of objects, we write $A \leq_T B$ if an (hypothetical) algorithm to answer questions about membership in B would yield an algorithm to answer questions about A. Thus the decision problem for A is reducible to that for B. One way to make this precise is through the theory of recursive functions. Recursive functions can be defined as the collection of functions obtained from certain base functions (like multiplication and addition) by closing under the usual operations of composition, minimalization and recursion. A function is said to be B-recursive if it is among the functions obtained from the base functions together with the characteristic function for B by closing under the usual operations. Then $A \leq_T B$ is defined to mean that that the characteristic function of A is B-recursive. Of course, if B is already recursive (that is, membership in B is decidable) and if $A \leq_T B$ then A is also recursive.

Now the relation $\leq_T$ is a partial order so we can form the corresponding equivalence relation. Two sets of objects A and B are *Turing equivalent* $A \equiv_T B$ if each is Turing reducible to the other, that is both $A \leq_T B$ and $B \leq_T A$. In terms of this notation there are some obvious relationships among our decision problems:

$$EqP(G) \equiv_T WP(G) \leq_T CP(G)$$

$$WP(G) \equiv_T GWP(1, G) \leq_T GWP(G).$$

We have already observed the first equivalence. Since $w =_G 1$ if and only if w and 1 are conjugate in G it follows that $WP(G) \leq_T CP(G)$. The other assertions are clear.

A *recursive presentation* is a presentation of the form

$$< x_1, \ldots, x_n \mid r_1 = 1, r_2 = 1, \ldots >$$

where $r_1, r_2, \ldots$ is a recursively enumerable set of words. A finitely generated group G is *recursively presented* if it has a recursive presentation. Of course finitely presented groups are recursively presented but the converse is false. The word problem and conjugacy problem are defined for recursively presented groups as before and they are still recursively enumerable problems.

Lemma 5.1 *Let G be a finitely generated group given by a recursive presentation*

$$G =< x_1, \ldots, x_n \mid r_1 = 1, r_2 = 1, \ldots > .$$

Suppose that H is a finitely generated group with generators $y_1, \ldots, y_m$ and that $\phi : H \to G$ is an injective homomorphism. Then H has a recursive presentation of the form

$$H =< y_1, \ldots, y_n \mid q_1 = 1, q_2 = 1, \ldots >$$

where $q_1, q_2, \ldots$ is a recursively enumerable set of words in $y_1, \ldots, y_m$. Moreover, $WP(H) \leq_T WP(G)$.

Proof: Let $F =< y_1, \ldots, y_m \mid >$ be the free group with basis $y_1, \ldots, y_m$. Now we can write $\phi(y_i) = u_i$ $(i = 1, \ldots, m)$ where the u_i are certain words on $x_1, \ldots, x_n$. There is then a unique homomorphism $\psi : F \to G$ such that $\psi(y_i) = u_i$ $(i = 1, \ldots, m)$ and since ϕ is injective we have $H \cong F/ker\ \psi$. Now the set of all formal products of the words u_i and their inverses is a recursively enumerable set of words of G. The set of words of G equal to the identity is also recursively enumerable. Hence the intersection of these two sets is a recursively enumerable set of words, and it follows that $ker\ \psi$ is a recursively enumerable set of words on $y_1, \ldots, y_m$. The first claim follows by taking $q_1, q_2, \ldots$ to be a recursive enumeration of $ker\ \psi$.

For the second claim, suppose that we have an algorithm A_G to solve the word problem for G. We describe an algorithm to solve the word problem for H as follows: let $w(y_1, \ldots, y_m)$ be an arbitrary word in the generators of H. Since ϕ is injective, $w =_H 1$ if and only if $\phi(w) =_G 1$. Now $\phi(w) = w(u_1, \ldots, u_m)$ so we can apply the algorithm A_G to decide whether or not $w(u_1, \ldots, u_m) =_G 1$. If so, then $w =_H 1$; if not, then $w \neq_H 1$. This algorithm solves the word problem for H. Thus $WP(H) \leq_T WP(G)$ completing the proof.

Lemma 5.2 *For finitely presented groups (respectively finitely generated, recursively presented groups), the word problem, conjugacy problem and generalized word problem are algebraic invariants. That is, for any two presentations π_1 and π_2 of the same group on a finite set of generators, $WP(\pi_1) \equiv_T WP(\pi_2)$, $CP(\pi_1) \equiv_T CP(\pi_2)$ and $GWP(\pi_1) \equiv_T GWP(\pi_2)$.*

Proof: The proof is in each case similar to the proof of the second part of the previous lemma except that ϕ is an isomorphism. We omit the details.

The main local unsolvability result is the following:

Theorem 5.3 (Novikov-Boone) *There exists a finitely presented group whose word problem is recursively unsolvable.*

The original proofs of this result proceed along the following lines: start with a Turing machine T whose halting problem is unsolvable. That is, the problem of deciding whether the machine started with an arbitrary tape in a certain state will eventually halt is unsolvable. Constructions of Markov and of Post, associate to such a Turing machine a certain semigroup $S(T)$ whose defining relations mimic the transition rules defining the Turing machine T. They show a code word incorporating a tape and state of T is equal in $S(T)$ to a particular fixed halting word, say q_0, if and only if T halts when started with that tape and state.

Groups $G(T)$ having unsolvable word problem are constructed by in turn mimicking the defining relations of $S(T)$ inside a group. The construction is not so direct as the Markov-Post construction and involves starting with free groups and performing a number of HNN-extensions and/or free products with amalgamation. Nevertheless, there is a direct coding of a tape and state of T as a word w of $G(T)$ so that $w =_{G(T)} 1$ if and only if the machine T halts when started with that tape and state. Since T has an unsolvable halting problem, it follows that $G(T)$ has unsolvable word problem.

A readable account of the Novikov-Boone Theorem along these lines can be found in the textbook by Rotman [7].

In view of the previously noted relationships among our various decision problems, the Novikov-Boone Theorem has the following immediate corollary:

Corollary 5.4 *There exists a finitely presented group G such that $WP(G)$, $CP(G)$ and $GWP(G)$ are all recursively unsolvable.*

We turn now to briefly consider other local decision problems concerning elements in a group.

The structure of finitely generated abelian groups can be completely determined from a finite presentation of such a group, and in particular one can solve the word problem for such groups. Consequently, if G is an arbitrary finitely presented group one can effectively determine the structure of its abelianization $G/[G,G]$. So for instance, there is an algorithm to decide whether G is perfect, that is $G = [G,G]$. Moreover, since one can solve the word problem for $G/[G,G]$ it follows that one can decide of a arbitrary word w of G whether or not $w \in [G,G]$.

However, it would seem that any property of elements a finitely presented group which is not determined by the abelianization $G/[G,G]$ will be recursively unrecognizable. The following result show a few common properties of elements are not recognizable.

Theorem 5.5 (Baumslag, Boone and Neumann) *There is a finitely presented group G such that there is no algorithm to determine whether or not a word in the given generators represents*

1. *an element of the center of G;*
2. *an element which commutes with a given element of G;*
3. *an n-th power, where $n > 1$ is a fixed integer;*
4. *an element whose class of conjugates is finite;*
5. *a commutator;*
6. *an element of finite order > 1.*

Proof: Fix a finitely presented group U having unsolvable word problem. Define G to be the ordinary free product of U with a cyclic group of order 3 and an infinite cyclic group, that is,

$$G = U * < s \mid \ > * < t \mid t^3 = 1 > .$$

We use the commutator notation $[x,y] = x^{-1}y^{-1}xy$. In the following, w is a variable for an arbitrary word in the generators of U.

The center of G is trivial so w lies in the center of G if and only if $w =_U 1$. So there is no algorithm to determine whether an arbitrary word of G lies in the center. This gives the first assertion. Similarly, w is permutable with s if and only if $w =_U 1$ which establishes the second assertion. The element $s^n[t,w]$ is an n-th power if and only if $w =_U 1$ establishing the third assertion. The conjugacy class of w is finite if and only if $w =_U 1$ since if $w \neq_U 1$ the

conjugates $s^{-i}ws^i$ would all be distinct. This gives the fourth assertion. For the fifth assertion, note that $[s,t]w$ is a commutator if and only if $w =_U 1$. Finally for the sixth assertion, observe that tw has infinite order if and only if $w \neq_U 1$, while if $w =_U 1$ then tw has order 3. This completes the proof.

5.2 Higman's embedding theorem

In contrast to the difficulties encountered for finitely presented groups, it is easy to give examples of finitely generated, recursively presented groups with unsolvable word problem. For example, let $S \subset \mathbb{N}$ be a recursively enumerable set of natural numbers which is not recursive. Define the recursively presented group

$$H_S =< a,b,c,d \mid a^{-i}ba^i = c^{-i}dc^i \ \forall i \in S > .$$

Now H_S can be described as the free product with amalgamation of the free group $< a,b \mid >$ and the free group $< c,d \mid >$ amalgamating the subgroup (freely) generated by the left hand sides of the indicated equations with the subgroup (freely) generated by the right hand sides. It follows from the normal form theorem for amalgamated free products that $a^{-i}ba^ic^{-i}d^{-1}c^i =_{H_S} 1$ if and only if $i \in S$. Thus $S \leq_T WP(H_S)$ and so $WP(H_S)$ is recursively unsolvable.

Using this observation Graham Higman gave a very different proof of the unsolvability of the word problem. Indeed he proved the following remarkable result:

Theorem 5.6 (Higman Embedding Theorem) *A finitely generated group H can be embedded in a finitely presented group if and only if H is recursively presented.*

That finitely generated subgroups of finitely presented groups are recursively presented is contained in our first lemma above. The difficult part of this theorem is to show that a recursively presented group can be embedded in a finitely presented group.

The Novikov-Boone Theorem is an easy corollary. For let H_S be the finitely generated, recursively presented group with unsolvable word problem constructed above. By Higman's Embedding Theorem, H_S can be embedded in a finitely presented group, say G_S. Then by an earlier lemma, $WP(H_S) \leq_T WP(G_S)$ and so G_S has unsolvable word problem.

Higman's Embedding Theorem has a number of other remarkable aspects. It provides a complete characterization of the finitely generated subgroups of

finitely presented groups - namely they are the recursively presented groups. It also provides a direct connection between a purely algebraic notion and a notion from recursive function theory. Another consequence is the existence of universal finitely presented groups.

Corollary 5.7 (Higman) *There exists a universal finitely presented group; that is, there exists a finitely presented group G which contains an isomorphic copy of every finitely presented group.*

To prove this one systematically enumerates all finite presentations on a fixed countable alphabet. The free product of all of these can be embedded in a two generator group which will be recursively presented. This group can then be embedded in a finitely presented group which is the desired universal group.

5.3 The isomorphism problem and recognizing properties

In this section the existence of a finitely presented group with unsolvable word problem is applied to obtain a number of global unsolvability results.

Consider the problem of recognizing whether a finitely presented group has a certain property of interest. For example, can one determine from a presentation whether a group is finite? or abelian? It is natural to require that the property to be recognized is *abstract* in the sense that whether a group G enjoys the property is independent of the presentation of G.

An abstract property P of finitely presented groups is *recursively recognizable* if there is an effective method which when applied to an arbitrary finite presentation π determines whether or not $gp(\pi)$ has the property P. More formally, P is *recursively recognizable* if $\{\pi \mid gp(\pi) \in P\}$ is a recursive set of finite presentations.

It turns out that very few interesting properties of groups are recursively recognizable. To formulate the key result we need the following definition.

Definition 5.1 *An abstract property P of finitely presented groups is said to be a* Markov property *if there are two finitely presented groups G_+ and G_- such that*

1. *G_+ has the property P; and*
2. *if G_- is embedded in a finitely presented group H then H does not have property P.*

These groups G_+ and G_- will be called the positive *and* negative witnesses *for the Markov property P respectively.*

It should be emphasized that if P is a Markov property then the negative witness does not have the property P, nor is it embedded in any finitely presented group with property P.

For example the property of being finite is a Markov property. For G_+ one can take $< a \mid a^2 = 1 >$ which is a finite group. For G_- one can take the group $< b, c \mid b^{-1}cb = c^2 >$ which is an infinite group and therefore not embedded in any finite group.

Similarly, the property of being abelian is a Markov property. Indeed the two groups chosen as witnesses for the property of being finite will also serve as witnesses for the property of being abelian.

An example of a property which is not a Markov property is the property of being perfect, that is $G/[G, G] \cong 1$. For it is not hard to show (and indeed will follow from the constructions given below) that any finitely presented group can be embedded in a perfect finitely presented group. Hence there can be no negative witness G_- for the property of being perfect.

An abstract property P of finitely presented groups is *hereditary* if H embedded in G and $G \in P$ imply that $H \in P$, that is, the property P is inherited by finitely presented subgroups. A property of finitely presented groups P is *non-trivial* if it is neither the empty property nor is it enjoyed by all finitely presented groups. Suppose P is a non-trivial, hereditary property of finitely presented groups. Then, since P is non-trivial, there are groups $G_+ \in P$ and $G_- \notin P$. But if G_- is embedded in a finitely presented group H, then $H \notin P$ because P is hereditary. Thus P is a Markov property with witnesses G_+ and G_-. This proves the following:

Lemma 5.8 *If P is a non-trivial hereditary property of finitely presented groups, then P is a Markov property.*

Another useful observation is the following:

Lemma 5.9 *If $\emptyset \neq P_1 \subseteq P_2$ are properties of finitely presented groups and if P_2 is a Markov property, then P_1 is also a Markov property.*

For if G_- is a negative witness for P_2 and if $K \in P_1$, then P_1 is a Markov property with positive and negative witnesses K and G_-.

Recall from the previous section that Higman has constructed a universal finitely presented group, say U. If P is a Markov property with positive and negative witnesses G_+ and G_-, then G_- is embedded in U so $U \notin P$. Moreover, if U is embedded in a finitely presented group H then so

is G_- and hence $H \notin P$. Thus P is a Markov property with positive and negative witnesses G_+ and U. Hence U is a negative witness for every Markov property.

The main unsolvability result concerning the recognition of properties of finitely presented groups is the following:

Theorem 5.10 (Adian-Rabin) *If P is a Markov property of finitely presented groups, then P is not recursively recognizable.*

Before indicating a proof of this result, we note the following easy corollaries:

Corollary 5.11 *The following properties of finitely presented groups are not recursively recognizable:*

1. *being the trivial group;*
2. *being finite;*
3. *being abelian;*
4. *being nilpotent;*
5. *being solvable;*
6. *being free;*
7. *being torsion-free;*
8. *being residually finite;*
9. *having a solvable word problem;*
10. *being simple;*
11. *being automatic.*

For each of (1) through (9) is a non-trivial, hereditary property and hence is a Markov property. For (10), it is known that finitely presented, simple groups have solvable word problem and hence, by the above lemma, being simple is a Markov property. Similarly for (11), automatic groups have solvable word problem and so being automatic is a Markov property.

Corollary 5.12 *The isomorphism problem for finitely presented groups is recursively unsolvable.*

For by (1) in the previous corollary there is no algorithm to determine of an arbitrary presentation π whether or not $gp(\pi) \cong 1$.

Proof of the Adian-Rabin Theorem: We are going to give a simple proof of the Adian-Rabin Theorem which is our modification of one given by Gordon. The construction is quite straightforward and variations on the details can be applied to obtain further results. So suppose that P is a Markov property and that G_+ and G_- are witnesses for P. We also have available a finitely presented group U having unsolvable word problem.

Using these three items of initial data, we construct a recursive family of finite presentations $\{\pi_w \mid w \in U\}$ indexed by the words of U so that if $w =_U 1$ then $gp(\pi_w) \cong G_+$ while if $w \neq_U 1$ then G_- is embedded in U. Thus $gp(\pi_w) \in P$ if and only if $w =_U 1$. Since U has unsolvable word problem, it follows that P is not recursively recognizable.

The family $\{\pi_w \mid w \in U\}$ is rather like a collection of buildings constructed from playing cards standing on edge. Such a building can be rather unstable so that if an essential card is removed (corresponding to $w =_U 1$) then the entire structure will collapse. The main technical result needed is the following.

Lemma 5.13 (Main Technical Lemma) *Let K be a group given by a presentation on a finite or countably infinite set of generators, say*

$$K =< x_1, x_2, \ldots \mid r_1 = 1, r_2 = 1, \ldots > .$$

For any word w in the given generators of K, let L_w be the group with presentation obtained from the given one for K by adding three new generators a, b, c together with defining relations

$$\begin{aligned} a^{-1}ba &= c^{-1}b^{-1}cbc && (5.1)\\ a^{-2}b^{-1}aba^2 &= c^{-2}b^{-1}cbc^2 && (5.2)\\ a^{-3}[w,b]a^3 &= c^{-3}bc^3 && (5.3)\\ a^{-(3+i)}x_iba^{(3+i)} &= c^{-(3+i)}bc^{(3+i)} \quad i = 1, 2, \ldots && (5.4) \end{aligned}$$

where $[w, b]$ is the commutator of w and b. Then

1. *if $w \neq_K 1$ then K is embedded in L_w by the inclusion map on generators;*

2. *the normal closure of w in L_w is all of L_w; in particular, if $w =_K 1$ then $L_w \cong 1$, the trivial group;*

3. *L_w is generated by the two elements b and ca^{-1}.*

If the given presentation of K is finite, then the specified presentation of L_w is also finite.

Proof: Suppose first that $w \neq_K 1$. In the free group $< b, c \mid >$ on generators b and c consider the subgroup C generated by b together with the right hand sides of the equations (1) through (4). It is easy to check that the indicated elements are a set of free generators for C since in forming the product of two powers of these elements or their inverses some of the conjugating symbols will remain uncancelled and the middle portions will be unaffected.

Similarly, in the ordinary free product $K* < a, b \mid >$ of K with the free group on generators a and b consider the subgroup A generated by b together with the left hand sides of the equations (1) through (4). Using the assumption that $w \neq_K 1$ it is again easy to check that the indicated elements are a set of free generators for A.

Thus assuming $w \neq_K 1$, the indicated presentation for L_w together with the equation identifying the symbol b in each the two factors is the natural presentation for the free product with amalgamation

$$\begin{array}{ccc} (K* < a, b \mid >) & * & < b, c \mid > . \\ A & = & C \end{array}$$

So if $w \neq_K 1$, then K is embedded in L_w establishing the first claim.

Now let N_w denote the normal closure of w in L_w. Clearly $[w, b] \in N_w$ so by equation (3), $b \in N_w$. But equations (1) and (2) ensure that a, b, c are all conjugate and so a, b, c all belong to N_w. Finally, since each of the system of equations (4) can be solved to express x_i in terms of a, b, c, it follows that $x_i \in N_w$ for $i = 1, 2, \ldots$. Thus each of the generators of L_w belongs to N_w and so $L_w = N_w$. This verifies the second assertion.

Finally, let M be the subgroup of L_w generated by b and ca^{-1}. Equation (1) can be rewritten as $b(ca^{-1})b(ca^{-1})^{-1}b^{-1} = c$ so that $c \in M$. But then from $ca^{-1} \in M$ it follows that $a \in M$. Finally from the system of equations (4) which can be solved for the x_i in terms of a, b, c it follows that $x_i \in M$ for $i = 1, 2, \ldots$ and so $M = L_w$. (For later use we note that neither equation (2) nor equation (3) was used in the proof of the final assertion). This completes the proof of the lemma.

Using this technical lemma it is easy to complete the proof of the Adian-Rabin Theorem. We are given the three finitely presented groups U, G_+ and G_- which can be assumed presented on disjoint alphabets as follows:

$$U =< y_1, \ldots, y_k \mid r_1 = 1, \ldots, r_\rho = 1 >$$

$$G_- =< s_1, \ldots, s_m \mid u_1 = 1, \ldots, u_\sigma = 1 >$$

$$G_+ =< t_1, \ldots, t_n \mid v_1 = 1, \ldots, v_\tau = 1 >$$

Let $K = U * G_-$ the ordinary free product of U and G_- presented as the union of the presentations of its factors. Since U has unsolvable word problem, K also has unsolvable word problem. Also both U and G_- are embedded in K by the inclusion map on generators. For any word w in the generators of U (these are also generators of K) form the presentation L_w as in the Main Technical Lemma. Finally we form the ordinary free product $L_w * G_+$.

A presentation π_w for these groups $L_w * G_+$ can be obtained by simply writing down all of the above generators together with all of the above defining equations. Such a presentation is defined for any word w in U whether or not $w \neq_U 1$. But it follows from the lemma that if $w \neq_U 1$ then the group G_- is embedded in $gp(\pi_w) = L_w * G_+$ and so $gp(\pi_w) \notin P$ by the definition of a Markov property. On the other hand, if $w =_U 1$ then by the lemma $L_w \cong 1$ and so $gp(\pi_w) \cong G_+$ and hence $gp(\pi_w) \in P$.

Thus we have shown that the recursive collection of presentations

$$\{\pi_w \mid w \text{ a word in } U\}$$

has the property that $gp(\pi_w) \in P$ if and only if $w =_U 1$. Since U has unsolvable word problem, it follows that P is not recursively recognizable. This completes the proof of the Adian-Rabin Theorem.

Bibliography

[1] M. Hall Jr., "The theory of groups", Macmillan, New York, 1959.

[2] D. L. Johnson, "Presentations of groups", LMS Lecture Notes **22**, Cambridge University Press,Cambridge 1976.

[3] R. C. Lyndon and P. E. Schupp, "Combinatorial Group Theory", Springer-Verlag, Berlin-Heidleberg-New York,1977.

[4] W. Magnus, A. Karrass and D. Solitar, "Combinatorial Group Theory", Wiley, New York, 1966 (also Dover reprint 1976)

[5] W. S. Massey, "Algebraic Topology: an introduction", Graduate Texts in Matematics **56**, Springer-Verlag, Berlin-Heidleberg-New York, 1977.

[6] C. F. Miller III, *Decision problems for groups - survey and reflections*, pp 1-59 in "Algorithms and Classification in Combinatorial Group Theory", MSRI Publications No. 23, edited by G. Baumslag and C. F. Miller III, Springer-Verlag, 1992.

[7] J. J. Rotman, "An introduction to the theory of groups" (4th edition), Springer Graduate Texts in Mathematics **148**, Springer-Verlag, Berlin-Heidleberg-New York, 1995.

[8] P. Scott and C. T. C. Wall, *Topological methods in group theory*, in "Homological Group Theory", pp 137-203 in LMS Lecture Notes **36**, edited by C. T. C. Wall, Cambridge University Press, 1979.

[9] J-P Serre, "Trees", Springer-Verlag, Berlin-Heidleberg-New York,1980.

[10] J. Stallings, *The topology of finite graphs*, Inventiones Math. **71** (1983), 551-565.