Combinatorial Group Theory: An Introduction

Billy Wonderly

University of Puget Sound

Math 434

April 21, 2012

Contents

1 Introduction **2**

2 Free Groups **2**

3 Free Group Construction **3**

3.1 One Free Group 6

4 Group Presentations **7**

4.1 Presenting C_n 7

4.2 Presentation of D_4 8

5 Max Dehn's Problems **8**

6 Conclusion **10**

7 Bibliography **10**

1 Introduction

It is difficult to provide a rigid definition of Combinatorial Group Theory (CGT). The development of CGT mid-19$^{\text{th}}$ century is closely entwined with the development of topology and logic, and has been ultimately wed to Geometric Group Theory. CGT can be generalized as the theory of *free groups*, or as the practice of studying groups using two sets: a set of *generators* and a set of *relators*. This is generally referred to as a *presentation* of a group.

The point of this paper is to provide an introduction to fundamental concepts and basic results of the field. However, the perspective of this paper is coming from abstract algebra, so many of the results regarding logic and topology will not be presented. This paper will cover the definition of free groups, which are fundamental to the study of CGT, as well as investigate many of their properties following their construction. The most striking of these results gives us that every group is isomorphic to a quotient group of a free group. The paper then defines group presentations in light of this result and concludes with a few examples of group presentations.

2 Free Groups

We begin this paper with a definition of free groups as is found in [1].

Definition 1. *Let F be a group and S be a subset of the set of elements of F with a mapping $i : S \to \{F\}$. F is a* ***free group with basis*** *S if for any group G and any map $\phi : S \to \{G\}$, ϕ can be extended uniquely to a group homomorphism $\phi' : F \to G$ satisfying $\phi = \phi' i$*

Free groups are a fundamental concept when studying CGT, and are going to be a novel concept to most people reading a paper that provides an introduction to the subject. So a few questions about uniqueness and existence might be lingering. To start, we will investigate uniqueness of free groups.

Theorem 1. *If F_1 and F_2 are both free on a set S then there exists an isomorphism $\psi : F_1 \to F_2$.*

Proof. Take i_1 and i_2 to be mappings from S to F_1 and F_2, respectively. Then there is a homomorphism $\phi_1 : F_1 \to F_2$ satisfying $i_1\phi_2 = i_2$ due to the definition of a free group. Similarly, there is a homomorphism $\phi_2 : F_2 \to F_1$ satisfying $i_2\phi_1 = i_1$. Thus, i_1=$i_1\phi_1\phi_2$ and, because the extensions are unique, we have that $\phi_1\phi_2$ acts as the identity function on F_1. Similarly we get $\phi_2\phi_1$ acts as the identity function on F_2. Thus, ϕ_1 is an isomorphism and ϕ_2 the inverse isomorphism. $\square$

Although we can already guess that a free group exists, we are required to prove that fact, and the construction of a free group makes the term "free"group feel like a bit of a misnomer.

3 Free Group Construction

In order to prove the existence of groups we will take a constructive approach and must define a few things and construct a few other things using much of the notation from [2].

Definition 2. *Given a finite set of distinct elements $S = \{s_1, s_2, s_3..., s_n\}$, we can define another set $S^{-1} = \{s_1^{-1}, s_2^{-1}, s_3^{-1}..., s_n^{-1}\}$, with elements distinct from one another and distinct from the elements of S, in one-to-one correspondence with S. Elements s_i and s_i^{-1} will be called an* ***inverse pair****. We will call the set S the set of* ***generators****. Furthermore, we form the set $S' = S \cup S^{-1}$ and call S' the set of* ***letters****.*

With a set of letters in hand, we continue with a few predictable definitions.

Definition 3. *We can form sequences of letters, $w = s_1s_2...s_n$, with $s_i \in S'$ and call these strings* ***words****. Furthermore we define the* ***length*** *of w to be the $|w|$ and have it number of letters in w, in this case $|w| = n$. Furthermore, we call the string of length zero to be the* ***empty word*** *and will denote it as* 1.

We form the set of all possible finite length words with letters from S' and call it W. We can provide W with an operation of **concatenation** meaning the product of $w_1, w_2 \in W$ is w_1w_2. However, this will not suffice as a group operation yet. We now define an **elementary reduction** of a word to be the removal or insertion of adjacent inverse pairs. A **reduced** word is a word that contains no adjacent inverse pairs.

Example 1. *Let $w = s_1s_1s_1s_2s_2^{-1}s_1^{-1}$ then we can reduce w to $s_1s_1s_1^{-1}$ then reduce again to get $w' = s_1s_1$, a fully reduced word.*

This defines an equivalence relation $\sim$ on W by $w_1 \sim w_2$ if we can perform elementary reductions on w_1 and obtain w_2. A quick result on the equivalence classes is required to continue, whose proof mimics one found in [2] (labelled van der Waerden's method).

Lemma 1. *The reduced form of a word is unique and there is only one fully reduced word in a given equivalence class.*

Proof. Let W_0 be the set of all fully reduced words in W. Then, for every $s \in S'$ define: $\lambda_s : W^* \to W^*$ in the following manner: take $w \in W^*$, if $w = s^{-1}v$, i.e. w has the letter s^{-1} in its leftmost slot, then

$$\lambda_s(w) = v$$

however, if the product sw is a fully reduced word then

$$\lambda_s(w) = sw$$

Calculate this function for each $w \in W^*$ and every $s \in S'$ and note that λ_s has an inverse function which is $\lambda_{s^{-1}}$, and thus λ_s is an element of permutations of the set W^*, call it P.
Thus, we have a mapping from S' to P. From the definition of free groups we can extend this mapping to give a homomorphism $\lambda' : F(S) \to P$. Let $s_1s_2...s_n = x \in S'$ is a word, then $\lambda_x = \lambda_{s_1}\lambda_{s_2}...\lambda_{s_n}$. Then if we take $a \in F(S)$ such that $a \sim x$ we get

$$\lambda_a(1) = \lambda_{s_1}(\lambda_{s_2}(...(\lambda_{s_n}(1))...)) = \lambda_{s_1}(\lambda_{s_2}(...s_n...)) = \lambda_{s_1}(s_2...s_n) = s_1s_2...s_n$$

From this we get that $a \in F(S)$ provides a function λ_a such that $\lambda_a(1) = x$, thus $\lambda_a(1)$ is the unique reduced word equivalent to x □

We now take $F(S)$ to be the set of equivalence classes of W under $\sim$ and define the operation on $F(S)$ to be: given $[w_1], [w_2] \in F$

$$[w_1][w_2] = [w_1w_2]$$

and we now show that $F(S)$ forms a group.

- **Identity** The empty word.
- **Closure** Given $[w_1], [w_2] \in F(S).[w_1][w_2] = [w_1w_2]$ is the equivalence class of $w_1w_2 \in W$, thus $[w_1w_2]$ is an element of $F(S)$
- **Associative** Given $[w_1], [w_2], [w_3] \in F(S)$ then $([w_1][w_2])[w_3] = [w_1w_2][w_3] = [w_1w_2w_3] = [w_1][w_2w_3] = [w_1]([w_2][w_3])$
- **Inverses** Take an element $w = s_{i_1}s_{i_2}...s_{i_m} \in W$, then the inverse is given as $w^{-1} = s_{i_m}^{-1}...s_{i_2}^{-1}s_{i_1}^{-1}$. So given an element $[w] \in F(S)$ take $[w^{-1}]$ to be its inverse.

With all that we have built so far, we are finally ready to prove existence of a free group.

Theorem 2. *Given a set S, F is a free group with a basis set of the equivalence classes of S, denoted $[S]$ and $|[S]| = |S|$*

Proof. In order to prove $|[S]| = |S|$ we take distinct elements $s_1, s_2 \in S$. Then $[s_1] \neq [s_2]$ since the single letters are fully reduced. Now take any group G and take the mapping $\phi : [S] \to G$ which then defines another mapping $\psi : S \to G$ such that

$$\phi([s]) = \psi(s)$$

Now extend the mapping ψ to apply W by defining $\psi' : W \to G$ by

$$\psi'(w) = \psi'(s_1...s_n) = \psi'(s_1)...\psi'(s_n)$$

If we have $w_1 = w_2 \Rightarrow \psi'(w_1) = \psi'(w_2)$ since the letters will be equivalent. Thus, ψ' maps equivalence classes of words to G and gives us a homomorphism $\psi' : F(S) \to G$ which is an extension of the mapping ϕ and satisfies the definition of a free group. □

Corollary 1. *Given any set S, a free group F with basis S exists.*

Proof. With a set S we can go through the construction previously demonstrated to determine F. □

So we see that not only does one free group exist, but as many free groups exist as there are sets. Also, just as a note, we will say that $F(S)$ is **freely generated** by the set S.

3.1 One Free Group

An example of a free group is the *infinite cyclic group*. Take $S = \{a\}$ and $S^{-1} = \{a^{-1}\}$. Then S freely generates $F(S)$. We have that the set of reduced words is

$$\{...a^{-1}a^{-1}a^{-1}a^{-1}, a^{-1}a^{-1}a^{-1}, a^{-1}a^{-1}, a^{-1}, 1, a, aa, aaa, aaaa, ...\}$$

or, using obvious notation:

$$\{...a^{-4}, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, ...\}$$

We can take arbitrary elements $a^i, a^j \in F_n$ and take their product: $a^i a^j = a^{ij} \in F_n$. The reader will note that this group is isomorphic to $\mathbb{Z}$.
The final theorem of this section displays the power of free groups, but we need one quick definition first.

Definition 4. *The* ***rank*** *of a free group is the number of elements in the set of generators.*

Theorem 3. *A finitely generated group G of order n is isomorphic to a factor group of a free group of rank n.*

Proof. Take the set of generators of G to be $S = \{g_1, ..., g_n\}$, with $|S| = n$. Now form the free group $F(S)$ with basis S, giving $F(S)$ rank n. Let $\phi : S \to G$ be defined to take elements from the set S and map them to their corresponding group elements in G. Then ϕ extends to a homomorphism $\phi' : F(S) \to G$. Since S is a generating set, ϕ' is surjective. By the first isomorphism theorem for groups we have that $G \cong F(S)/\ker(\phi)$ □

4 Group Presentations

Now that we have determined that all groups are intimately related to quotients of free groups, we can build up some terminology and results that allows us to study groups from a different point of view. Since we can define any group as the quotient group of a free group, to make the following discussion easier we will solidify some terminology.

Definition 5. *Let G be a group and $S \subset \{G\}$. The **normal closure** of S in G, denoted N_S, is defined as:*

$$N_S = \{gsg^{-1} | s \in S, g \in G\}$$

Without proof we note that the normal closure of S is the smallest normal subgroup of G containing S.

Definition 6. *Given that $G \cong F(S)/N$, where G is a group, $F(S)$ is the free group over a set S, and N the normal closure of a set $R \subset F$ we say that $\langle S|R\rangle$ is a **presentation** for G. S is called the set of **generators** and R is called the set of **relators**.*

Now what can we do with this new construction? All we have to do given a group G, with a set of generators S, is form the free group $F(S)$, and then find the a subset R of $F(S)$ such that $G \cong F(S)/N_R = \langle S|R\rangle$. Before an example, a few new terms.

Definition 7. *If S is finite then G is **finitely generated** and if R is finite then G is **finitely related**. Finally, if G is both finitely generated and related then G is **finitely presented**.*

We also note that a presentation of a group is generally a group of cosets, so although one will normally see $G = \langle S|R\rangle$ written, it is not totally accurate. Rather, $G \cong \langle S|R\rangle$ is the accurate interpretation. To understand group presentations better, let us look at a few examples.

4.1 Presenting C_n

Let $G = \langle a\rangle$, i.e. G is a cyclic group generated by a. Thus we can take our generating set to be $S = \{a\}$. Then the free group $F(S)$ looks just like the free group of the infinite cyclic group.

However, we are in the finite cyclic group and require that $a^n = 1$, so we take $R = \{a^n\}$ and form the proper quotient group. Thus each time a^n is found it gets sent to the identity and C_n has the presentation $\langle a | a^n = 1 \rangle$

4.2 Presentation of D_4

From Judson we know that D_4 has generators r and s, so we can take $S = \{r, s\}$. Now we form the free group $F(S)$ and we get all possible strings of r's, s's and their inverses. However, we know that in $D_4, r^4 = id, s^2 = id$ and $srsr = id$, so we let our set of relators be $R = \{r^4, s^2, srsr\}$. Now we form the normal closure N_R and take the quotient group $F(S)/N_R$. We can very informally interpret the formation of the quotient group as sending each element of the normal subgroup to the identity. Now we can say that D_4 has a presentation $\langle r, s | r^4 = 1, s^2 = 1, srsr = 1 \rangle$, often times the relators are implicitly equal to 1 unless other noted, so the presentation can also be given $D_4 = \langle r, s | r^4, s^2, srsr \rangle$

5 Max Dehn's Problems

In the early 1900's, Max Dehn (a student of David Hilbert) followed in his mentor's footsteps and proposed a series of problems regarding finite presentations. The three problems can be found in any of [1], [2] or [3] (which shows how fundamental they are to CGT) and are stated thus:

1. **The Word Problem** Given a group G with presentation $\langle S|R \rangle$, is there an algorithm which will determine whether or not a given element in G is equivalent to the identity element?

2. **The Conjugacy Problem** Given a group G with presentation $\langle S|R \rangle$, does an algorithm exist that will determine if two words are conjugate in G?

3. **The Isomorphism Problem** Given two groups G_1 and G_2, each given by finite presentations $\langle S_1|R_1 \rangle$ and $\langle S_2|R_2 \rangle$ respectively, is there an algorithm which will determine if G_1 is isomorphic to G_2?

These problems influenced the development of CGT and the following results regarding the word problem are given. This paper was unable to reach far enough into the machinery of CGT to provide proofs of the following results, but they provide examples of how powerful a tool CGT is. These results are presented in either [1] or [2].

Theorem 4. *The word problem for finitely generated free groups is solvable.*

Proof. This result comes directly from the process of reducing words. In a finitely generated free group a word w is equal to the identity if w reduces to the empty word. □

However, this result carries us only so far. Dehn provided solutions for the word problem for several topological groups, but no general result was provided until W. Magnus proved his in 1932.

Theorem 5. *A group G which has a finite presentation and only one relator has a solvable word problem*

Although this result was very promising and a great achievement in tackling the word problem, in 1954 a shocking result was proven by P.S. Novikov

Theorem 6. *There exists a finitely presented group with an unsolvable word problem.*

What was (and is) so shocking about this is that it implies there are groups we are unable to answer even the most simple question: is an element the identity? Furthermore, whether or not an element is of finite order. Without being able to answer these questions we have a difficult time determining if a group is abelian, simple, or trivial. Unfortunately it means that, unfortunately, given any finite presentation we may not be able to say anything about the group or elements of the group. This result also implies a negative result for the conjugacy problem for finitely presented groups: if we can't even determine if a word is the identity we would have a hard time determining if a word is even conjugate to the identity. However, some positive results have surfaced. For example, if a group is known to be abelian then it has a solvable word problem and the presentation of the group can be reduced by a technique called *Nielsen transformations*, a process that can be found in [2]. Additionally, techniques such as *small cancellation theory* have been developed to aid the study of group presentations. Finally, solving the word and conjugacy problems for knot groups allowed mathematicians to classify mathematical knots in the 1970's.

6 Conclusion

In the course of this paper we have provided a construction for one of the fundamental elements of CGT, the free group, and reached several results for free groups. In particular we have discussed that every group is isomorphic to a quotient group of a free group. This result gave us the structure to build group presentations. Finally, we examined some important results regarding the famous "word problem"which exhibit the utility of CGT. I hope this paper provided enough vocabulary and exposure to help the reader in any future excursion into CGT.

7 Bibliography

References

[1] D. E. Cohen *Combinatorial Group Theory: a topological approach*, Cambridge University Press, New York, 1989.

[2] R.C. Lyndon and Paul E. Schupp *Combinatorial Group Theory*, Springer-Verlag, New York, 1977.

[3] B. Changler and W. Magnus *The Hisotry of Combinatorial Group Theory: a Case Study in the History of Ideas*, Springer-Verlag, New York, 1982.