Ryan Walch
Abstract Project

The Properties of Free Groups

1 Introduction

Combinatorial Group theory is the study of free groups and group presentations. Group presentations are a representation of a group as a set of relations on a generating set. Combinatorial group theory has been motivated by several problems related to what can be deduced from group presentations. For instance, given some product of the generators one could ask if it was equal to the identity. This question is known as the word problem. While the word problem is solvable for certain types of groups in general it is undecidable. One can also ask if two strings of generators are conjugate to each other. Known as the conjuency problem it also undecideble in general. Another enquiry one can make is if the group corresponding to a given group presentation is finite or finitely generated. While the details of these problems are beyond the scope of this paper the concept of a free group was motivated by a need to develop tools to answer these questions. In addition many of these problems while undecidable in general are decidable in free groups.

Free groups are foundational to many aspects of combinatorial group theory. For instance every group is the factor group of some free group. Informally free groups are those in which no relations hold between the elements besides the standard assumption that an element multiplied by its inverse is the identity. The most familiar example of a free group is the group of integers under addition. Another way to interpret a free group is to think of it as a set of finite strings of symbols and their inverses. If the only way to properly change these symbols is to add or remove element inverse pairs then the group is free. In this paper we will define and develop the basic properties of free groups. We will conclude by proving the Nielsen-Schreier Theorem.

2 Free Groups: Definitions and Basic Theorems

We begin with a formal definition of a free group.

Definition Suppose F is a group and $X \subset F$. Then F is a free group if whenever ϕ is a function from X to any group G there exists a unique homomorphic extension of ϕ, $\phi^* : F \to G$.

The inclusion map is the map whose restriction to X is the identity. Note we write function composition from left to right throughout this paper so that $\phi_1\phi_2 = \phi_2 \circ \phi_1$. X is called the basis of F and $|X|$ is called the rank of F. For example the group of integers under addition has basis $\{1\}$ and thus rank 1. This definition captures the notion of a free

group being one with no relations by asserting that an extension exists for every function ϕ and group G. If there was a relation on F then we could find some group G where the relation would not hold between the corresponding elements in the image and the extension would not exist. For instance suppose x, y, $z \in X \subset F$ where F is free. If there was a relation say $xyz = e$ on F then it is reasonable to expect that we could find a group G such that $\phi(x)\phi(y)\phi(z) \neq e$. In this case if ϕ^* is a homomorphic extension of ϕ then

$$e = \phi^*(e) = \phi^*(xyz) = \phi^*(x)\phi^*(y)\phi^*(z) \neq e$$

Since this is a contradiction no extension of ϕ could exist. The requirement that ϕ^* is unique is equivalent to the fact that X generates F.

Proposition 1 *If X is a basis for a free group F then X generates F.*

Proof Let H be the subgroup generated by X and $i_x : X \to H$ be the inclusion map. Because F is free with basis X there exists a unique homomorphism $\phi : F \to H$ which extends i_x. Now let $i_H : H \to F$ be the inclusion map on H. Since $\phi i_H|_X = i_x i_H$, ϕi_h extends $i_x i_H$. The identity function is also an extension of $i_x i_H$ so by the uniqueness of extensions in free groups $\phi i_x = id$. Thus $F = H$.

■

If two free groups are isomorphic then they have the same rank. In fact there is only one free group of a given rank up to isomorphism.

Theorem 2 *Suppose F is a free group with basis X and G is a free group with basis Y. Then $F \cong G$ if and only if $|X| = |Y|$.*

Proof Suppose that $|X| = |Y|$. Then since X and Y are the same cardinalities there exists an one-to-one correspondence $f_1 : X \to Y$ with $f_1^{-1} : Y \to X$. Because F and G are free groups there exists unique homomorphic extensions ϕ_1, ϕ_2 of f_1 and f_1^{-1} respectivly. Because ϕ_2 extends the inverse of the function which ϕ_1 extends, the restriction of $\phi_1\phi_2 : F \to F$ is the identity function. Therefore the identity is a valid extension of $\phi_1\phi_2|_X$ to F. Since extensions from the basis in free groups are unique we can conclude that $\phi_1\phi_2 = id$. Similarly $\phi_1\phi_2 = id$. Thus ϕ_1 must be an isomorphism and $F \cong G$.

Now suppose that $F \cong G$. Let $Hom(F, \mathbb{Z}_2)$ be the set of homomorphisms between F and $\mathbb{Z}_2$. Similarly, let $Hom(G, \mathbb{Z}_2)$ be the set of all homomorphisms between G and $\mathbb{Z}_2$. Because $F \cong G$ the similarity of structure ensures $|Hom(F, \mathbb{Z}_2)| = |Hom(G, \mathbb{Z}_2)|$. There are exactly $2^{|X|}$ functions between F and $\mathbb{Z}_2$ hence we conclude

$$2^{|X|} = |hom(F, \mathbb{Z}_2)| = |hom(G, \mathbb{Z}_2)| = 2^{|Y|}$$

Hence $|X| = |Y|$. ■

We can now give conditions for when a subset of a group is the basis for a free group.

Theorem 3 *Suppose F is a group and $X \subset F$. Then F is a free group with basis X if and only if the following hold:*

1) X generates F
2) There does not exist $x_1x_2...x_n = e$ for $x_i \in X \setminus \{e\}$.

Proof Suppose that F is free with $X \subset F$ a basis for F. By proposition 1 we know that X generates F. To show 2 assume for the purposes of contradiction that there exists an $x_1x_2...x_n = e$ for $x_i \in X \setminus \{e\}$ then for given ϕ we can find some G such that

$$\phi(x_1)\phi(x_2)...\phi(x_n) \neq e$$

.

For example we could choose G to be cyclic of order $n+1$. Because F is free there exists a unique extension ϕ^* of ϕ. Then because ϕ^* must be a homomorphism we know that

$$e_g = \phi^*(e_F) = \phi^*(x_1x_2...x_n) = \phi^*(x_1)\phi^*(x_2)...\phi^*(x_n) \neq e_g$$

We have $e_g \neq e_g$ which is a contradiction. We thus can assume that there are no nontrival products of elements of X equal to the identity.

Now assume that X generates F and that there does not exist $x_1, x_2...x_n = e$ for $x_i \in X \setminus \{e\}$ Let $\phi : X \to G$ be a function to an arbitrary group G. Because X generates F we can write each $f \in F$ uniquely as $f = x_1x_2, ...x_n$ where $x_i \in X$. We can then extend ϕ by defining ϕ^* by

$$\phi^*(x_1x_2...x_n) = \phi(x_1)\phi(x_2)...\phi(x_n)$$

.

ϕ^* is clearly an extension of ϕ because the representation of F as products of the elements of the basis is unique ϕ^* is also the only possible homomorphic extension of ϕ. We can then conclude that F is free with basis X. ■

3 Construction of Free Groups

We can also veiw free groups as formal strings of symbols. Let X be any set. It is possible to construct a free group with basis X. We view the elements of X as symbols. Let X^{-1} be the set of inverses of X. Formally we define a one-to-one correspondence $\nu : X \to X^{-1}$ and say that $\nu(x) = x^{-1}$ is the inverse of x. Let $W(X)$ be the collection of all finite combinations of elements of $X^{\pm} = X \cup X^{-1}$. Elements of $W(X)$ are called words. For any $w \in W(X)$ we say the length of w, denoted $|w|$, is the number of elements of $X \cup X^{-1}$ which make up w. Thus if we write $w = a_1a_2...a_n$ where $a_i \in X^{\pm}$ then $|w| = n$. Note the a_i's do not have to be distinct. We also define the empty word, e consisting of no symbols to have length zero.

Definition A word $w = a_1a_2...a_n$, with $a_i \in X \cup X^{-1}$, is **reduced** if $a_{i+1} \neq {a_i}^{-1}$ for all $1 \leq i < n$.

Reduced words are those which remain after we have removed all pairs of the form aa^{-1}.

Definition An **elementary transformation** of a word consists of adding or removing a pair of elements of the form aa^{-1}.

Let $w_1, w_2 \in W(X)$. We define a relation $\sim$ by $w_1 \sim w_2$ if and only if w_2 can be reached from w_1 by a sequence of elementry transformations.

Lemma 4 *The relation $\sim$ is an equivalence relation on $W(X)$.*

Proof Suppose $w_1, w_2, w_3 \in W(X)$. $w_1 \sim w_1$ as we can add a pair xx^{-1} to w_1 and then remove it. Suppose $w_1 \sim w_2$ then since elementary transformations are reversible we can reverse the steps we used to reach w_2 from w_1. Thus $w_2 \sim w_1$. Lastly suppose $w_1 \sim w_2$ and $w_2 \sim w_3$. Clearly $w_1 \sim w_3$. Therefore $\sim$ is an equivalence relation $W(X)$. ■

Since words are finite strings of symbols there must be a finite number of elementry transformations between words in the same equivalence class.

Lemma 5 *Each equivalence class of $\sim$ contains exactly one reduced word.*

Proof Suppose u and v are two reduced words in the same equivalence class. Let $w_1 w_2 ... w_n$ be the shortest series of words such w_{i+1} is an elementary transformation of w_i were w_1 is an elementary transformation of u and v is an elementary transformation of w_n. Since u is a reduced word and $u \neq v$, $|w_1| > |u|$. Likewise because v is reduced we can conclude that $|w_n| > |v|$. Therefore the length of the words linking u and v must at first increase and at some point decrease. Let m be the smallest value such that $|w_m| > |w_{m+1}|$. We can also see that $|w_m| > |w_{m-1}|$. To reach w_m we must therefore add some aa^{-1} pair to w_{m-1}. We then remove some bb^{-1} to reach w_{m+1}. There are three options for how aa^{-1} relates to bb^{-1}. In each case we will make an arguement based off of the fact that $w_1 w_2 ... w_n$ is the shortest possible sequence of w_i's. Suppose $aa^{-1} = bb^{-1}$ in this case $w_{m-1} = w_{m+1}$. If aa^{-1} and bb^{-1} partially overlap then there must be some string of the form $aa^{-1}a$ Thus to obtain w_m we must be replacing some a in w_{m-1} with $aa^{-1}a$ to obtain w_{m+1} we must be replacing the same $aa^{-1}a$ with a. Thus $w_{m-1} = w_{m+1}$. Lastly suppose that aa^{-1} and bb^{-1} are disjoint. In this case we can shorten the entire chain by simply removing w_{m-1}, w_m and w_{m+1}. By repeatedly shortening the chain we eventually delete all w_i's and conclude that $u = v$. ■

We can now prove that the set of equivalence classes of $\sim$ form a free group with basis X. The identity is the empty word and the group action is juxtaposition. Let $[w]$ denote the equivalence class of w. Note that $[w]$ is just the word in its fully reduced form.

Theorem 6 *The set of equivalence classes of $\sim$ on $W(X)$ forms a free group under juxtaposition.*

Proof Let F be the set of equivalence classes of $\sim$. Clearly F is closed and associative under juxtaposition. The identity is the empty word. The inverse of $[w] = a_1 a_2 ... a_n$ is $a_n^{-1} a_{n-1}^{-1} ... a_1^{-1}$. where a_i are singletons in $W(X)$.

We will now show that F is free with basis X. Let G be an arbitrary group and $\phi : X \to G$ a function. Define $\phi^*[W(X)] \to G$ by

$$\phi^*(e) = e \quad \phi^*(x) = \phi(x) \quad \phi^*(x^{-1}) = (\phi(x))^{-1} \quad \phi$$

for all $x \in X$. If $[x] = a_1 a_2 ... a_n$ for $n > 1$ then define ϕ^* by

$$\phi^*(a_1 a_2 ... a_n) = \phi^*(a_1)\phi^*(a_2)...\phi^*(a_n)$$

.

Clearly ϕ^* is an extension of ϕ. Since X generates $W(X)$ the extension is also unique. We now need to show that ϕ^* is a homomorphism. Let $[a] = x_1 x_2 ... x_n$ and $b = y_1 y_2 ... y_m$. Then

$$\phi^*(a)\phi^*(b) = \phi^*(x_1 x_2 ... x_n)\phi^*(y_1 y_2 ... y_m) = \phi^*(x_1)\phi^*(x_2)...\phi(x_n^*)\phi^*(y_1)\phi^*(y_2)...\phi^*(y_n)$$

$$= \phi^*(x_1 ... x_n ... y_1 ... y_n)$$

Thus ϕ^* is an homomorphism and F is a free group. ■

From now on for notational convience whenever we refer to a word w we will assume it is reduced. Since we may construct a free group from any set using the procedure we outlined above there are free groups of arbitrary rank.

Corollary 7 *There exists Free groups for every rank.*

Proof Simply copy the procedure above and choose X to have the desired cardinality. ■

The below theorem shows one reason we are interested in free groups.

Theorem 8 *Every group is isomorphic to a factor group of a free group.*

Proof Suppose G is a group generated by S. Then there exists a set X such that $|X| = |S|$. Since X and S have the same cardinality we can find a bijection f from X to S. From the above we know there exists a free group F with X as a basis. Since f maps X to G there exists a unique extension $\phi^* : F \to G$ Because f is a bijection it is one to one and on to with respect to the generating set of F. Thus ϕ^* must be onto. We can use the first isomorphism theorem to conclude that $F/ker(\phi^*) \cong G$. ■

4 The Nielson-Schrier Theorem

Every subgroup of a free group is free. The proof requires several lemmas. There are two well known methods to prove this theorem in the literature. Orginally the theorem was proved in 1921 by Neilson. However, this method only works for finitely generated groups. Our paper will use a latter proof known as Schrier's method. With Schriers method we will start with a free group and construct a subset B which we will prove generates a subgroup of F.

First we must define a well ordering on our group. Let F be a free group with basis X. By the well ordering theorem there exists a well ordering of $X^{\pm}, \prec$. We then use this to define an order on F itself.

Definition Let $w = a_1a_2...a_n$ and $v = b_1b_2...b_m$ be words of F. We will define an ordering $<$ as follows. If $n < m$ we say $w < v$. If $m = n$ then $w < v$ if and only if $a_i < b_i$ for the first i in which $a_i \neq b_i$.

This orders words from smallest to biggest with the ordering on $X^{\pm}$ serving as a tie breaker. We now prove a lemma which tells us that this lexiographic ordering behaves as we would expect.

Lemma 9 *Let $w = x_1x_2...x_n$ be a reduced word in F with $x_i \in X \cup X^{-1}$ with $n > 1$. For $v \in F$ if $v < x_1x_2...x_{n-1}$ then $vx_n < w$.*

Proof If $|v| < n-1$ then $|vx_n| < |w|$ thus $vx_n < w$ and we are done. We can then assume that $|v| = n-1$. Since $|v| < x_1x_2, ...x_{n-1}$ there must be some $1 \leq r \leq n-1$ such v differs in the rth letter. Thus we can write $v = x_1...x_{r-1}y_r...y_n - 1 < x_1...x_{n-1}$. We see that adding x_n to end of both sides of this inequality does not change the result and thus $vx_n < w$. ■

We will now look at cosets of F. The idea is that cosets provide a natural way to partition the set. We can then select the smallest member of each partition and use this fact to proceed in the proof. To start we define a transversal which at its heart is a selection of exactly one element from each coset.

Definition Fix $H < F$. Then a **right transversal** for H in F is a subset U consisting of exactly one element from each right coset.

We want to make sure our tranversals have some structure to evoke. With this in mind we define

Definition A subset S of F has the **Schreier property** if all words $w = x_1x_2x_3...x_n$, $w \neq e$.

$$w = x_1x_2x_3...x_n \in S \quad \text{only if} \quad x_1x_2x_3...x_{n-1} \in S$$

A transversal with the Schreir property is called a Schreier tranversal.

Lemma 10 *Every Subgroup H of F has a Schreier transversal obtained by choosing the least element of each right coset in the ordering.*

Proof Let U be a transversal created by selecting the least element from each coset. We will prove that it is a Schreier transversal by proving the contrapositive of the Schreier property. That is we show that $x_1x_2...x_n - 1 \notin U \implies w = x_1...x_n \notin U$. Suppose $x_1x_2...x_{n-1} \notin U$. Then there exists a $v \in x_1x_2...x_{n-1}H$ such that $v < g$ for all $g \in x_1x_...x_{n-1}H$. By the definition of v we know

$$v < x_1x_2...x_{n-1}$$

$$vx_n < x_1x_2...x_n$$

Since $Hv = Hx_1x_2...x_{n-1}$ by construction $Hvx_n = Hx_1x_2...x_{n-1}x_n$. Thus we have found an element smaller then $x_1, ...x_n$ in its coset we can conclude $x_1, ...x_m \notin U$ thus proving the theorem.

■

Let U be a Schreir transversal constructed as in the above lemma for some subgroup H of a free group F. Let $w \in F$. By the definition of a transversal there is a single element in $Hw \cap U$. Denote this element by $\bar{w}$. The following lemma lists some useful facts about $\bar{w}$.

Lemma 11 *Let $w \in F$ and U defined as above. Denote by $\bar{w}$ the unique element in $Hw \cap U$. Then:*

1) $\bar{\bar{w}} = \bar{w}$
2) $\bar{w} = w$ if and only if $w \in U$.
3) $\overline{\overline{ux}x^{-1}} = u$ for $x \in X$, $u \in U$.

Proof One and two follow directly from the definition of coset multiplication and the construction of U. To prove three note that for $u \in U$

$$\begin{aligned} Hux &= H\bar{u}x \\ \implies Hu &= Hux^{-1} \\ \implies \overline{\overline{ux}x^{-1}} &= u \end{aligned}$$

■

Lemma 12 *Let $A = \{ux\overline{ux}^{-1} | \, u \in U x \in X\}$. Then A generates H.*

Proof We claim that A is a subset of H. To see this note that $\overline{ux}$ is part of a coset. This means that there exists an $h \in H$ such that $\overline{ux} = uxh$ Since $uxH = \overline{UX}H$ we can interchange ux with $\overline{ux}$ and multiply by $\overline{ux}^{-1}$ to write $h = ux\overline{ux}^{-1}$. Thus $A \subset H$.

Now let $h = x_1, x_2, ...x_n$ where $x_i \in X$. Define a series of $u_i's$ inductivly by

$$u_1 = e \quad u_{i+1} = \overline{u_i x_i} \text{ for } 1 \leq i \leq n$$

Now let

$$a_i = u_i x_i u_{i+1}^{-1} = u_i x_i \overline{u_i x_i}^{-1}$$

for $1 \leq i \leq n$. Note $a_i \in A$. Consider

$$a_1 a_2 ... a_n = u_1 x_1 x_2 ... x_n u_{n+1}^{-1} = ehu_{n+1}^{-1}$$

Since each $a_i \in A \subset of H$ we can conclude that $u_{n+1}^{-1} = h^{-1} a_1 a_2 ... a_n \in H \implies u_{n+1} \in H$. However $u_{n+1}^{-1} \in U$ and because $U \cap H = \{e\}$ we can conclude that $u_{n+1} = e$ and therefore we can write h as the product of elements in A. Hence A generates H.

■

Lemma 13 *Define:*

$$\begin{aligned} B &= \left\{ ux\overline{ux}^{-1} \middle| \, u \in U, x \in X, ux \notin U \right\} \\ \hat{B} &= \left\{ ux\overline{ux}^{-1} \middle| \, u \in U, x \in X^{-1}.ux \notin U \right\} \\ B^{-1} &= \left\{ b^{-1} \middle| \, b \; inB \right\} \end{aligned}$$

Then $\hat{B} = B^{-1}$ and $A \setminus \{e\} = B \cup B^{-1}$.

Proof Let $x \in X^{\pm 1}$ and $u \in U$ Then by lemma 11 part 3 we can write

$$(ux\overline{ux}^{-1})^{-1} = \overline{ux}x^{-1}u^{-1} = \overline{ux}x^{-1}(\overline{\overline{ux}x^{-1}})^{-1}$$

By lemma 11

$$ux \notin U \leftrightarrow ux \neq \overline{ux} \leftrightarrow u \neq \overline{ux}x^{-1} \leftrightarrow \overline{\overline{ux}x^{-1}} \neq \overline{ux}x^{-1} \leftrightarrow \overline{ux}x^{-1} \notin U$$

If in the above we choose $x \in X$ then we conclude $B^{-1} \subset \hat{B}$. Likewise if we let $x \in X^{-1}$ we can write $\hat{B} \subset B^{-1}$. Thus we conclude $B^{-1} = \hat{B}$. ■

Theorem 14 *Every subgroup of a free group is free.*

Proof We will show that the B of lemma 13 is a basis for $H \leq F$. By Lemma 12 and 13 B generates H. We must now show that no product of $B^{\pm}$ is trival. Let w be a product of $b_i's \in B^{\pm}$. Then we write

$$w = b_1 b_2 ... b_n \quad \text{with} b_i = u_i x_i \overline{u_i x^i}^{-1}$$

Since the middle terms $x...y$ will not cancel we know that $|w| \geq 1$ and can conclude that $w \neq e$. B thus satisfies the criteria of Theorem 3 and thus is a basis of H as a free group. ■

5 Conclusion

In this paper we have explained the baisics of free groups focusing on the properites of their basises, their construction and their subgroups. However we have just scratched the surface of this subject. We have neglected Nielsen transformations and automorphisms of free group. In addition there is also the whole study of group presentations in which free groups play an important role. This paper has hopefully given the reader a taste of the subject and inspired them to go further.

6 Excercises

1. Prove that $\mathbb{Z}$ is a free group.
2. A group P is projective if whenever there is a function $\phi : G :\rightarrow H$, for any groups G,H. If there is a function $\pi : P \rightarrow H$ then there exits a map $\psi : P \rightarrow G$ such that $\psi\phi = \pi$. Prove that a projective group is free.

References

[1] DL Johnson, *Topics in the Theory of Group Presentations*. Cambridge University Press, Cambridge, 1st Edition, 1980.

[2] DL Johnson, *Presentations of Groups*. Cambridge University Press, Cambridge, 1st Edition, 1990.

[3] Gilber Baumslag, *Topics in Combinatorial Group Theory*. Birkhauser, Basel, 1st Edition, 1993.

[4] Robert c. Lyndon and Paul E. Schupp, *Combinatorial Group Theory*. Springer Verlag Press, Berlin, 1st Edition, 1980.