ACTING FREELY

GABRIEL GASTER

1. Preface

This article is intended to present a combinatorial proof of Schreier's Theorem, that subgroups of free groups are free. While a 'one line' proof exists using the theory of covering spaces, the advantage of this proof (besides its pleasing, combinatorial nature) is that the techniques employed generalize and are useful in other proofs. The fundamental idea at play is that if a group acts freely on a graph X, then the Cayley graph is a contraction of X. Using this idea, one reveals a structure at work whenever a group acts freely on a graph–and the result, along with some stronger consequences relating the index and rank of a subgroup, falls out. This paper assumes the audience has had a short first course in algebra and some familiarity with groups and group actions.

2. Free Groups

A *free* group comes from thinking about the most loosely defined, general notions of *torsion-free*[1] groups. Intuitively speaking, they are the barest groups with the simplest structure. We will see that any group is the quotient of a subgroup of a free group modulo some equivalence relations. That is, any group sits embedded within the structure of a free group. Before more discussion of their concrete structure, with an eye toward the *universal property*, we come to the following

Definition 2.1. Given any set $S = \{s_i | i \in I\}$, the *free* group generated by S, $F(S)$, is the unique group such that there is an injection $\iota : S \to F(S)$, and for *any* other group H and *any* map $\varphi : S \to H$ there is a unique group homomorphism $\widetilde{\varphi} : F(S) \to H$ such that $\widetilde{\varphi} \circ \iota(s) = \varphi(s)\ \forall\ s \in S$, making the folowing diagram commute. We call S the *generating set* for $F(S)$.

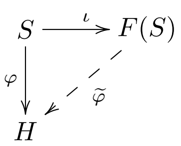

Figure 1

Example 2.2. Given the set $S = \{s\}$, $F(S)$ would, by the definition, be a group containing $\iota(s)$. We can conclude that the cyclic group generated by $\iota(s)$, $\langle \iota(s) \rangle = \{\iota(s)^k \mid k \in \mathbb{Z}\} \subset F(S)$.

Date: August 15, 2006.

[1] i.e. having no non-identity elements of finite order

Now, there is an injection from our generating set S into any old (non-empty) group H, including, say $\mathbb{R}^+$ under multiplication, which is torsion-free, i.e.

$$\text{for all } s \in \mathbb{R}^+, \text{ and any } i, j \in \mathbb{Z}, i \neq j \implies s^i \neq s^j.$$

It's therefore clear that for there to exist a homomorphism $\widetilde{\varphi} : F(S) \to \mathbb{R}^\times$, it must be that $\iota(s) \neq 1 \in F(S)$ and, furthermore, $\langle \iota(s) \rangle$ must have infinite order. If this were not the case, then

$$\exists\ k \in \mathbb{N} \text{ s.t. } \iota(s)^k = 1 \text{ and}$$
$$\widetilde{\varphi} \circ (\iota(s))^k = \widetilde{\varphi}(1) = (\widetilde{\varphi} \circ \iota(s))^k$$

even though $\varphi(s)^k \neq 1$, and the diagram would not commute. $\searrow\!\swarrow$ Thus, $\langle \iota(s) \rangle \subset F(S)$. Since $\langle \iota(a) \rangle \cong \mathbb{Z}$, we have obtained an injective homomorphism $\gamma : \mathbb{Z} \to F(S)$. If $\langle \iota(s) \rangle \neq F(S)$ and there was $t \in F(S)$ s.t. $t \notin \langle \iota(s) \rangle$, then $\widetilde{\varphi}(t)$ could $= \widetilde{\varphi}(s)$ or $= \widetilde{\varphi}(s)^2$ or $= \widetilde{\varphi}(s)^3$. In any case, because t is not in any way related to the set S, the choice of $\widetilde{\varphi}(t)$ does not affect whether or not the diagram (1) commutes. Therefore there is not a unique $\widetilde{\varphi}$. $\searrow\!\swarrow$

That's great because it's just what we could have hoped for; plus we've proven our first

Claim 2.3. *The free group generated by one element is isomorphic to the infinite cyclic group, namely* $\langle \mathbb{Z}, + \rangle$.

Note that there's another, perhaps simpler proof that $F(\{s\}) = \mathbb{Z}$. It uses an extremely useful

Lemma 2.4. *If an object $F(A)$ exists as defined by the universal property, (i.e. that $F(A)$ is the unique object that makes the following Figure 2 of structure preserving maps commute) then it is unique (up to some structure preserving, bijective map).*

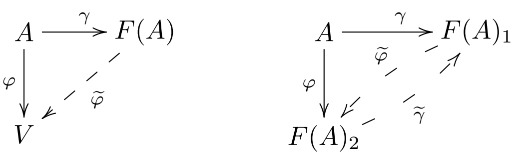

FIGURE 2

Proof. Say there were two objects $F(A)_1$ and $F(A)_2$ that made the diagram commute. Then there would be a map from $\widetilde{\varphi} : F(A)_1 \to F(A)_2$ and $\widetilde{\gamma} : F(A)_2 \to F(A)_1$, and the second diagram would commute. That would mean that $\widetilde{\varphi} \circ \widetilde{\gamma} : F(A)_1 \to F(A)_1$ and, since the diagram commutes, $\widetilde{\varphi} \circ \widetilde{\gamma}$ is the identity, proving that $\widetilde{\varphi}$ is a bijective structure preserving map, whence $F(A)_1 \cong F(A)_2$. $\square$

From Example 2.2 we saw that, for $S = \{s\}$, $\langle \iota(s) \rangle \cong \mathbb{Z}$ satisfies the constraints of the universal property; we could have immediately then concluded from Lemma 2.4 that $F(S) = \mathbb{Z}$.

With this tool in hand, we turn to the question of finitely-generated free groups, i.e. $F(S)$ for which $S = \{s_1, s_2, \ldots, s_k\}$. Just as before, as we immediately concluded (from the closure of the binary operation) that $\langle \iota(s) \rangle \subset F(\{s\})$, we can now conclude that $\langle \iota(s_1), \iota(s_2), \ldots, \iota(s_k)\rangle = S^* \subset F(S)$. For which S^* is all possible finite reduced 'words' of the form

$$\iota(s_{i_1})^{\epsilon_1}\iota(s_{i_2})^{\epsilon_2}\cdots\iota(s_{i_1})^{\epsilon_{i_k}}$$

for which $s_{i_j} \in S$, $\epsilon_i \in \{\pm 1\}$ and for all $j \in \{1, \ldots, k\}$, $s_j = s_{j+1} \implies \epsilon_j = \epsilon_{j+1}$. You should check that S^* is a group in which the group operation is, simply, place two words next to each other and if you see an $\iota(s_j)$ next to an $\iota(s_j)^{-1}$, cross 'em out. Since any group containing an injection from S will contain elements of this form, S^* satisfies the universal property and, by Lemma 2.4, we've proven our second

Theorem 2.5. *If S has finitely many elements then $F(S) = S^*$.*

N.B. The fact that ι is an injection allows us to see $S \subset F(S)$. Since we've proven the existence of unique free groups for finite sets S, and since the notation $\iota(a)$ is so cumbersome, in practice, and for the rest of this article, we'll say that $S \subset F(S)$, and $F(S)$ has elements which are words of the form ${a_1}^{\epsilon_1}{a_2}^{\epsilon_2}\cdots{a_k}^{\epsilon_k}$ for $a_i \in S$.

We would want that $F(S_1) \ncong F(S_2)$ for $|S_1| \neq |S_2|$, i.e. that free groups with different numbers of generators are actually different. The first case is simple.

Lemma 2.6. *$F(\{s\}) \ncong F(\{s_1, s_2\})$.*

Proof. The order of the letters matters in the words of S^*; if $s_1s_2 = s_2s_1$ then there would not be a homomorphism from $F(\{s_1, s_2\})$ to a non-abelian group G with trivial center to make the diagram in Figure 1 commute. That means that $s_1s_2 \neq s_2s_1$ and $F(\{s_1, s_2\})$ is not abelian. But $F(\{s\}) \cong \langle \mathbb{Z}, +\rangle$, which is abelian. □

The more general case requires a bit work–first dealing with the *free abelian* group.

Claim 2.7. *For $n \neq m$, $\mathbb{Z}^m \ncong \mathbb{Z}^n$*

Proof. Assume the opposite, that $\mathbb{Z}^m \cong \mathbb{Z}^n$, then $\mathbb{Z}^m/2\mathbb{Z}^m \cong \mathbb{Z}^n/2\mathbb{Z}^n$. But $|\mathbb{Z}^m/2\mathbb{Z}^m| = 2^m$ and $|\mathbb{Z}^n/2\mathbb{Z}^n| = 2^n$. But then the groups have different cardinality so they cannot be isomorphic. □

Claim 2.8. *$F(S_1) \ncong F(S_2)$ for $|S_1| \neq |S_2|$.*

Proof. The proof is obvious once we consider the abelianizations of the two groups, i.e. $F(S_1)/F'(S_1)$, where $F'(S_1)$ is the *commutator* supgroup, i.e. $F'(S_1) = \{aba^{-1}b^{-1} | a, b \in F(S_1)$. It follows that $F'(S_1) \trianglelefteq F(S_1)$ and $F(S_1)/F'(S_1)$ is abelian. Then if $F(S_1) \cong F(S_2)$, then $F'(S_1) \cong F'(S_2)$, and finally $F(S_1)/F'(S_1) \cong F(S_2)/F'(S_2)$.

On the other hand, there is a canonical homomorphism (by the universal property) $\widetilde{\varphi} : F(S_1) \to \mathbb{Z}^{|S_1|}$ commuting with $\varphi : S_1 \to \mathbb{Z}^{|S_1|}$. The homomorphism sends $\{a_1, a_2, \ldots, a_{|S_1|}\}$ to the $\mathbb{Z}$-basis consisting of elements containing one 1 and the rest 0's. Clearly, $F'(S_1) \subset \ker(\widetilde{\varphi})$. Consider an element of the $\ker(\widetilde{\varphi})$, without loss of generality, assume the first letter in the word has positive power, i.e. $a_1{a_2}^{\epsilon_2}\cdots{a_k}^{\epsilon_k}$. We see that $\sum_{a_i=s_j} \epsilon_i = 0$; i.e. the sum of the powers of identical 'letters' is 0. Clearly words of this form of length 0 belong to the commutator subgroup. Inducting on the length of the words, given a word of length $n + 1$, $a_1{a_2}^{\epsilon_2}\cdots a_{n+1}^{\epsilon_{n+1}}$, then it must be in some coset of $F(S_1)/\ker(S_1)$. Then multiplying by an element of $F'(S_1) \subset \widetilde{\varphi}$ will not change the element's coset. We know

$\sum_{a_i=a_1} \epsilon_i = 0$, so consider the occurence of the inverse of a_1 in the word; say it occurs after p letters. Then $a_1 a_2{}^{\epsilon_2} \cdots a_{n+1}^{\epsilon_{n+1}} = a_1 \underbrace{w}_{\text{`p letters'}} a_1{}^{-1} a_{p+2}{}^{\epsilon_{p+2}} \cdots a_{n+1}^{\epsilon_{n+1}}$. But $a_1{}^1 w a_1{}^{-1} a_{p+2}^{\epsilon_{p+2}} \cdots a_{n+1}^{\epsilon_{n+1}}$ and $(w a_1 w^{-1} a^{-1}) a_1{}^{-1} \cdots a_{n+1}^{\epsilon_{n+1}}$ are in the same coset, containing $(w a_1 w^{-1} a^{-1}) a_1{}^{-1} \cdots a_{n+1}^{\epsilon_{n+1}} = a_{p+2}{}^{\epsilon_{p+2}} \cdots a_{n+1}^{\epsilon_{n+1}}$, namely the coset $F'(S_1)$. Then $F'(S_1) = \ker(\widetilde{\varphi})$. But then by the first isomorphism of theorem, $F(S_1)/F'(S_1) \cong \mathbb{Z}^{|S_1|}$. Similarly, $F(S_2)/F'(S_2) \cong \mathbb{Z}^{|S_2|}$. Since generators of a group will generate any quotient of the group, we see $F(S_1)/F'(S_1) \cong \mathbb{Z}^{|S_1|} \ncong \mathbb{Z}^{|S_2|} \cong F(S_2)/F'(S_2)$, so $F(S_1) \ncong F(S_2)$. □

That's great because now, in good faith, we can finally name different free groups! We can say that the *rank* of a free group $F(S)$ is the order of the generating set $|S| = k$. We write $k = r_{F(S)}$, and $F(S) = F_k$. Much of the work we've done has been working up to the following

Theorem 2.9. *The rank of a free group is well-defined.*

3. Graphs

Given a group G and a set S, recall that we say G *acts* on the right on S if

(1) For the identity, $1 \in G$ and for all $s \in S$, $s \cdot 1 = s$.
(2) For any $g, h \in G$, $s \in S$, $(s \cdot g) \cdot h = s \cdot (gh)$.

Note that it follows from 1 and 2 that $g \in G$ yields a bijection from S to itself.

Example 3.1. The symmetric group on n elements, S_n, acts on any set of n elements–indeed, S_n is all possible bijections from a set of n elements to itself. Since any finite group G, $|G| = n$, is a subgroup of $S_{n!}$, then in fact, any group action on a set can be seen a subgroup of the permutations of $S_{n!}$.

An *oriented graph* Γ is a set of elements called *vertices* (the singular form is vertex), denoted $\text{vert}(\Gamma) = V$, and a collection of ordered pairs of vertices called *edges*, $\text{edge}(\Gamma) = E$. For $v_1, v_2 \in V$, if $(v_1, v_2) = e \in E$ then the *origin* of e, $o(e) = v_1$, while the *tail* of e, $t(e) = v_2$. We say two vertices are *adjacent* if they are the origin and tail of some edge. A *path* is a set of vertices $\{v_1, \ldots, v_k\}$ so that for all $i \in \{1, \ldots, k-1\}$, either (v_i, v_{i+1}) or $(v_i + 1, v_i) \in E$. A *directed path* is a path in which for all $i \in \{1, \ldots, k-1\}$, $(v_i, v_{i+1}) \in E$. The length of a path $\{v_1, \ldots, v_k\}$ is k. A *circuit* is a path of non-trivial length from a vertex to itself. A graph is *connected* if for all $v_1, v_2 \in V$, there is a path $\{v_1, \ldots, v_2\}$. A *tree* is a connected, non-empty graph containing no circuits.

Any connected graph will contain trees as subgraphs–indeed the paths from any vertex to any other will yield subtrees. The subtrees of a graph could be ordered by inclusion. Clearly the finite union of trees in an ascending chain will be be a tree. If the infinite union were not a tree, it would contain a circuit which would be realized after a finite union (since circuits are finite). Therefore, if a graph X has subtrees T_i for $i \in I$; then any chain $T_{i_1} \subset T_{i_2} \subset T_{i_3} \cdots$ is bounded above by the tree $\bigcup_{i_j \in I} T_i$ and, by Zorn's Lemma, there is a maximal subtree T of X.

Claim 3.2. *A maximal subtree T of X contains all vertices of X.*

Proof. If T did not contain all the vertices of X, then there would be $v \in \text{vert}(X)$ so that $v \notin \text{vert}(T)$. But X is connected, so $\forall x \in \text{vert}(T)$, there is a path from x to v. Consider all paths from $\text{vert}(T)$ to v. There is a path $P := \{x_1, x_2, \ldots, x_{n-1}, v\}$ of minimum length[2]. For all $y \in P$ such that $y \neq x_1 \in$vert(T), $y \notin$vert(T), otherwise the path $\{y, \ldots, x_{n-1}, y\}$ would have shorter length than P. But then, since the adjoining of distinct paths to trees is still a tree, $T \cup P$ is a bigger subtree of X, contradicting the assumption that T was maximal. □

Example 3.3. Given a group G and a set $S \subset G$, one could construct the graph $\Gamma(G, S)$ in which vert$\Gamma(G, S) = G$ and, between any two vertices $g, h \in G$ there is an edge (g, h) if and only if there is a $s \in S$ so that $gs = h$. $\Gamma(G, S)$ is called the *Cayley Graph* of G.

In the previous example, G could act naturally on $\Gamma(G, S)$ under the group operation, i.e. for $g \in G$, g takes a vertex $v \in \Gamma(G, S)$ to $gv \in G$, another vertex of $\Gamma(G, S)$. The Cayley graph in some sense gives us a physical representation of an abstract group. This allows us to draw conclusions about a group based off of observations of its Cayley Graph.

Claim 3.4. $\Gamma(G, S)$ *is connected if and only if* S *generates* G.

Proof. Say $\Gamma(G, S)$ is connected, that means that for all $h \in G$ there is some series $(s_i) \in S$, $i \in I$ so that $\left(\prod_{i \in I} s_i\right)(1) = g$, i.e. S generates G. Likewise, we can conclude that if S generates G then $\Gamma(G, S)$ is connected. □

Aside. So we see that if S is not a generating set, $\Gamma(G, S)$ is disconnected. If we can draw conclusions about $\Gamma(G, S)$ when it is connected, those conclusions could extend to the case when $\Gamma(G, S)$ is disconnected: breaking down $\Gamma(G, S)$ into the disjoint union of connected components, our old observations apply. Therefore we restrict our considerations to $\Gamma(G, S)$ for S, a generating set.

This new machinery devoloped allows us to draw powerful analogies between properties of groups (free-ness, finitely generated, abelian, etc.) and properties of the graphs (tree-ness, connectedness, etc.) in which they act on.

Claim 3.5. $\Gamma(G, S)$ *is a tree if and only if* G *is a free group with generating set* S.

Proof. If G is free with basis S, then for all $g \in G$, $g = {a_1}^{\epsilon_1} {a_2}^{\epsilon_2} \cdots {a_k}^{\epsilon_k}$ (see Theorem 2.5), with $a_i \in S$, $\epsilon_i \in \{\pm 1\}$, and $\epsilon_i = \epsilon_{i+1}$ if $a_i = a_{i+1}$. Since S generates G, from Claim 3.4, we see that Γ is connected.

If Γ were not a tree, it would contain a circuit. That means, for some vertex $v_1 \in$vert(Γ), there is a path of non-trivial length from v_1 to v_1, namely $\{v_1, v_2, \ldots, v_p, v_1\}$. Then there are two distinct paths from v_1 to v_p, namely

$$\begin{aligned} a_1 a_2 \cdots a_n(v_1) &= v_p \\ b(v_1) &= v_p \end{aligned}$$

for $b \neq a_1$, $a_i \neq a_{i+1}^{-1}$ where $i \in \{1, 2, \ldots, n\}$. But that means, in G

$$\begin{aligned} a_1 a_2 \cdots a_n(v_1) &= b(v_1) \text{ whence,} \\ a_1 a_2 \cdots a_n &= b, \end{aligned}$$

a contradiction. $\searrow\swarrow$

If Γ is a tree, S clearly generates G since Γ is connected. If G is not a free group, then $\exists\ \hat{g} \neq 1 \in F(S)$ whose image in G is 1. Then, let us choose $\hat{g}$ of minimum

[2] by the well ordering principle

length[3], i.e. $\hat{g} = a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}$ for $a_i \in S$, $\epsilon_i \in \{\pm 1\}$, and smallest n (**N.B.** We can do this since the length of elements of $F(S)$ is in $\mathbb{Z}_{\geq 0}$, a well-ordered set). But then we see that

$$a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n}(1) \quad = \quad 1$$

and there is a circuit from 1 to 1. □

Note that a group's action on a graph not only gives a bijection of the graph onto itself, but it also gives a *morphism* of the graph to itself (a map of edges and vertices, respectively, preserving adjacency). This follows from the associativity of the group action.

An *inversion* of an edge (e_1, e_2) is (e_2, e_1). If a group acts without inversion, then $\forall g \in G$, $(e_1, e_2) \in$edge(X), $g(e_1, e_2) \neq (e_2, e_1)$. If a group acts without inversion, then the morphism of the graph maps vertices to vertices, without changing the direction of any of the edges. One might even say a morphism without inversion is a morphism that preserves the orientation (direction) of the graph.

A group's action partitions a set into orbits. If a group acts on a graph (V, E), the orbit of a vertex v is $\{x \in V | \exists\ g \in G \text{ s.t. } g(v) = x\}$. It's clear the orbits of the group action partition the graph into equivalence classes. If that's the case, then we can make the

Definition 3.6. If a group, G, acts on a graph, X, without inversion, then the quotient graph X/G, X mod G, is the partitioning of the edges and vertices into equivalence classes via the group action. That is, for $v_1, v_2 \in$vert(X), $v_1 \sim v_2$ if there is $g \in G$ s.t. $g(v_1) = v_2$. Then there is a map φ : vert$(X) \to$ vert(X/G). Likewise, if there is an edge (v_1, v_2) for $v_1, v_2 \in$vert(X), then there is an edge $(\varphi(v_1), \varphi(v_2)) \in$edge$(X/G)$.

Aside. Why should we specify that G act without inversion on X in order to take the quotient graph? If G acted with inversion, then the orientation of the quotient graph X/G would not be inherited from X. The orientation of Cayley Graphs plays an essential role in revealing the group structure. If the Cayley Graph were unoriented, then Cayley Graph of $\mathbb{Z}_2$ would be a tree, invalidating our key Claim 3.5.

Example 3.7. Consider the infinite ordered path $P = \mathbb{Z}$ with no circuits. For $a_1, a_2 \in \mathbb{Z}$, $(a_1, a_2) \in$edge(P) if and only if $a_2 - a_1 = 1$. Note, $P = \Gamma(\mathbb{Z}, 1)$.

Let $\mathbb{Z}$ act on P, for $n \in \mathbb{Z}$, $p \in P$, by $n : p \mapsto p + n$. Then clearly $\mathbb{Z}$ acts on P without inversion–if an edge were inverted that would mean there was $n \in \mathbb{Z}$ such that $(a_1 + n) - (a_2 + n) = 1$, which would contradict the assumption that $a_2 - a_1 = 1$.

Clearly connectedness is preserved under the quotient map. Similarly, if there is a circuit in X, then there will be a circuit in X/G. The converse is taken care of in the following

Claim 3.8. *For a group G acting without inversion on a connected graph X, every subtree T' of X maps onto a subtree of X/G under the quotient map.*

---

[3]The length of an element in $F(S)$ is defined analogously to the length of a path in $\Gamma(F(S), S)$. One might define the length of $f \in (F(S)$ to be the length of the path from 1 to $f \in \Gamma(G, S)$

Proof. Consider the set of all subtrees of X whose image under the quotient map is in T'. This set can be ordered under inclusion, and, by Zorn's Lemma, it has a maximal element T. Say the image of T is $\widetilde{T} \neq T'$. Then there is $e' \in$edge(T') such that there is no $e \in$edge$(\widetilde{T})$ and $o(e) \in$vert$(\widetilde{T})$. If $t(e') \in$vert$(\widetilde{T})$ then there is a path from $o(e') \to t(e')$, $P \subset$ vert$(\widetilde{T})$ which means that $e' \notin P$ and another distinct path, namely e' from $o(e') \to t(e')$. At the same time, $\{e'\} \cup P \subset$ vert(T), so T contains a circuit, contradicting the fact that T is a tree.

But then there is an $e \in$edge(X) such that $o(e) \in$edge(T) and $t(e) \notin$edge(T). But then adjoining the edge e and the vertex $t(e)$ to T is a bigger tree whose image under the quotient map is in T', contradicting the maximality of T. □

So every tree in X/G 'lifts' to a tree in X. A lift, T of a maximal tree of X/G is called a *tree of representatives*. The name suggests that the tree should be representative of G's action on X. This is exactly the case. Every vertex of T is contained in a distinct orbit of G and every orbit has a 'representative' vertex in T. To see that every orbit is covered, we realize that a maximal tree T' of X/G contains all vertices of X/G. Then if T is a tree of representatives for X, then T maps onto T' under the quotient map. Therefore any orbit of G will map to a vertex in X/G, and there will be a $t \in$vert(T) which maps to that vertex.

4. Free Actions on Trees

We say a group action is *transitive* on a graph if for any two vertices in the graph, there is a group element than can send one to the other. If a group action on a graph is 'non-trivial' then non-trivial group elements act non-trivially, that is, they don't leave *every*thing fixed. We're looking for a stronger constraint on a group's action.

Definition 4.1. A group's action on a graph is *free* if non-trivial group elements leave *nothing* fixed, i.e. for any $g \in G,\ v \in \text{vert}(\Gamma),\ g \neq e,\ \implies g(v) \neq v$.

Curious that we should describe a group's action as free–given that we already have a notion of what it means for a group to be free. It's clear that groups act freely[4] and transitively[5] on their Cayley Graphs. To a certain extent, a group's action on the Cayley Graph extends to a group's action on any graph. If a group acts freely on a tree, then it need not act transitively. If, however, we contract the graphs so that the group does act transitively, we come to the Cayley Graph. This is exactly the construction that we will use later on in the proof of Theorem 4.2. Here is where the power of the machinery developed is felt: through proving things (easily) about a group's action on it's Cayley Graph, we derive facts about a group's action on any graph. In this manner, we derive (very easily) facts about the structures of these groups.

It's not hard for one to imagine that these ideas are related, that if a group's action on a graph is free then the group is free. This is not so far from the truth.

There is one exeption though, if a group acts freely on a circuit of length n, a simple (and not very efficient) upper bound for the cardinality of the group is $n!$: there are only finitely many non-trivial morphisms of a graph onto itself. Since free groups are infinite, clearly free groups cannot act freely on circuits. Therefore, if a

[4]by virtue of there being a unique idempotent that is the identity in a group

[5]by virtue of cancellation in any group

group acts freely on a graph with no circuits, it makes sense that the group might be free. So, accounting for this case, we get our

Theorem 4.2. *Let G act freely on a tree X, then G is a free group. In particluar, let T be a tree of representatives for $X/G := X^*$. If $S = \{g \neq 1 | g \in G, \exists\ e \in edge(T), o(e) \in vert(T)$ and $t(e) \in vert(Tg)\}$, then S generates G.*

Proof. $T \to X^*$ is injective since T is a tree of representatives, i.e. $T \subset X$ is the lift of a maximal subtree of X^*. $(T)g \to (Tg)$, i.e. there is a bijection from G to translates of T and the translates are pairwise disjoint for non-trivial $g \in G$.

Let X' be the contraction graph of X, crushing Tg to a single vertex called (Tg). X' is a tree; if not, there is some circuit, i.e. two distinct paths from $(T) \in \text{vert}(X')$, to $\hat{T}$. That is, there are paths $P_1 = \{(Ts_1), (Ts_2), \cdots, (Ts_n) = \hat{T}\}$ and $P_2 = \{(Tt_1), (Tt_2), \cdots, (Tt_m) = \hat{T}\}$ for $s_i, t_i \in G$. Considering some $v \in \text{vert}(T)$, $(v)s_1s_2 \cdots s_n, (v)t_1t_2 \cdots t_m \in \text{vert}(\hat{T})$. But since $\hat{T}$ and T are distinct trees in X, they are connected and there is a distinct path $P_3 = (v)s_1s_2 \cdots s_n \to (v)t_1t_2 \cdots t_m$. Then the $P_1 \cup P_3 \cup (P_2)^{-1}$ is a circuit in X.

So there is a bijection $\alpha : \text{vert}(X') \to \text{vert}\ \Gamma(G, S)$, giving an isomorphism $\varphi : X' \to \Gamma(G, S)$. Thus G acting freely on $\Gamma(G, S)$ implies that G acts freely on X', which in turn implies that G is free with basis S. □

So we have characterized free groups in terms of their actions on any graphs by their actions on their Cayley Graphs. A free action on a graph is pretty special–it follows immediately from the definition that, if a group acts freely on a graph, any subgroup will also act freely on a graph. Thus, with no undue timeliness, we have arrived at a big time idea, and it's only a

Corollary 4.3 (Schreier)**.** *Every subgroup of a free group is free.*

5. Subgroups of Free Groups

We now progress to some counting arguments, relating the index of a subgroup to the rank of a subgroup. First we need some preliminary ideas about trees. In a path $\{a_1, a_2, \ldots, a_n\}$ for $a_i \neq a_j$ for $i \neq j$, the number of vertices is one more than the number of edges. This seems like it should generalize to trees, too, and it does.

Lemma 5.1. *If Γ is a connected graph with finitely many vertices, $v = |vert(\Gamma)|$, $e = |edge(\Gamma)|$, then*

$$e = v - 1 \iff \Gamma \text{ is a tree.} \tag{1}$$

Proof. If Γ is a trivial tree, namely the tree with one vertex, then equation (1) holds. Inducting on finite trees, we see that any finite tree is the union of finitely many finite paths. A finite path clearly satisfies the equality. If T' is the graph resulting in adjoining a finite path P to a tree T, since adjoining entails identifying one vertex of P to T, if $v_P = |\text{vert}(P)|$, $e_P = |\text{edge}(P)|$ and $v_T = |\text{vert}(T)|$, $e_T = |\text{edge}(T)|$ then $v_{T'} := \text{vert}(T') = v_P + v_T - 1$, while $e_{T'} := \text{edge}(T') = e_P + e_T$, i.e.

$$\begin{aligned} e_{T'} &= e_P + e_T \\ &= (v_P - 1 + v_T) - 1 \\ &= v_{T'} - 1 \end{aligned}$$

If $e = v - 1$, let Γ' be a maximal subtree of Γ. Then $v' = |\text{vert}(\Gamma')|$, $e' = |\text{edge}(\Gamma')|$, and $e' = v' - 1$ since Γ' is a tree. Also, we proved in Claim (3.2) that $v' = v$. Clearly, since Γ' is a subtree of Γ, $e' \leq e$. But then

$$\begin{array}{rcrcccc} v'-1 & = & e' & \leq & e & = & v-1 \\ v-1 & = & e' & \leq & e & = & v-1 \\ & \Longrightarrow & e' & = & e & & \end{array}$$

And $\Gamma' = \Gamma$, so our maximal tree was the whole graph. □

We can now apply this characterization of trees to the tactics in our proof of Theorem 4.2, obtaining an analogous relation on the quotient graph.

Theorem 5.2. *Let G act freely on a directed tree X. We know from Theorem 4.2 that G is free, generated by S. Let T be a tree of representatives mod G, then if $X^* = X/G$ has finitely many vertices, vert(X^*) $= V^*$, and edge(X^*) $= E^*$, then*

$$|S| - 1 \quad = \quad |E^*| - |V^*|$$

Proof. Let W be a set of directed edges that start in T and don't end in T. From Theorem 4.2, we saw that $|S| = |W|$. Similarly, let W^* be the image of W in X^*. Clearly W is in bijection with W^* since W consists of edges between different orbits of X under G. So $|W| = |W^*|$, and $|S| = |W^*|$.

Let $T^* \subset X^*$ be the image of $T \subset X$, T^* is a maximal tree of X^*, so $|V^*| = |\text{vert}(T^*)|$.

For $e \in E^*$, either $e \in$edge(T^*) or $e \in$edge(W^*): in X^*, every edge, e starts in T^* since it's a maximal tree. If e ends in T^* then $e \in$edge(T^*)–since otherwise there would be a circuit. If e does not end in T^*, by definition, it's in W^*. We've shown that $E^* = \text{edge}(T^*) \amalg W^*$, i.e. $|E^*| = |W^*| + |\text{edge}(T^*)|$. Then

$$\begin{aligned} |E^*| - |V^*| &= (|W^*| + |\text{edge}(T^*)|) - |\text{vert}(T^*)| \\ &= |W^*| + (|\text{edge}(T^*)| - |\text{vert}(T^*)|) \\ &= |W^*| - 1 \qquad \text{(applying Lemma 5.1 since } T^* \text{ is a tree)} \\ &= |S| - 1 \end{aligned}$$

proving the theorem. □

This tells us, in particular, the quotient of the cayley graph $\Gamma(F(S), S)$ by $F(S)$ is a single vertex with $|S|$ edges. But it can also give us some strong constraints on the possible index of free groups of a given rank. Really, the theorem gives us a correspondance between the index of a subgroup and its rank.

Corollary 5.3 (Schreier)**.** *For G, a free group with generating set S, $H < G$ so that $|G : H| = n$,*

$$r_H - 1 \quad = \quad n(r_G - 1)$$

Proof. Let $\Gamma = \Gamma(G, S)$ be the Cayley Graph of G; it is a tree on which G acts freely. Then if $\Gamma_1 = \Gamma/G$ and $\Gamma_2 = \Gamma/H$, $v_1 = |\text{vert}(\Gamma_1)|$ and $v_2 = |\text{vert}\Gamma_2)|$,

$e_1 = |\text{edge}(\Gamma_1)|$ and $e_2 = |\text{edge}(\Gamma_2)|$, then by virtue of H having index n in G, $v_1 n = v_2$ and $e_1 n = e_2$. By application of Theorem 5.2, we see

$$\begin{aligned} n(r_G - 1) &= n(e_1 - v_1) \\ &= e_2 - v_2 \quad \text{but} \\ e_2 - v_2 &= r_H - 1 \quad \text{whence} \\ n(r_G - 1) &= r_H - 1 \end{aligned}$$

□

So we know that subgroups of free groups are free. Corollary 5.3 tells us that the index of a subgroup of a free group uniquely determines that subgroup's rank. This is a powerful tool for analyzing subgroups of free groups.

Example 5.4. If F_2 is generated by $\{x, y\}$, consider a homomorphism $\varphi : F_2 \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(x) = \varphi(y) = 1 \in \mathbb{Z}/n\mathbb{Z}$. Clearly, $\ker(\varphi) \triangleleft F_2$ and, since $[\mathbb{Z}/n\mathbb{Z} : \langle 1 \rangle] = n$, $[F_2 : \ker(\varphi)] = n$. Therefore, by Corollary 5.3, $\ker(\varphi)$ is a free group of rank $n + 1$.

This proves that $F_i \trianglelefteq F_2$ for all $i \in \mathbb{N}$, $i \geq 2$. It's obvious that $F_1 < F_2$ since the generating set of F_1 is contained in the generating set of F_2. It is also worth note that F_1 is not a finite index subgroup of F_2–this follows trivially from Corollary 5.3 as well. In addition, $F_2 < F_n \ \ \forall n \in \mathbb{N}_{\geq 2}$. F_1 is also the exception here, since it is cyclic and only contains subgroups isomorphic to itself or the trivial group. So we have every finitely generated free group as a subgroup of the free group of rank 2 and we have that the free group of rank 2 is a subgroup of every other free group with the exception of $F_1 \cong \mathbb{Z}$.

References

[1] Serre, J.-P. *Trees.* 13-30, Springer-Verlag, 1980.
[2] Smith, Geoff. *Topics in Group Theory.* Springer-Verlag, 2000.