Lecture 10-4: Free groups and the Nielsen-Schreier Theorem

October 4, 2024

I will wrap up group theory with a brief treatment of free groups. Part of this material is in Dummit and Foote (section 6.3, pages 215-220).

Recall from linear algebra that every vector space over a field has a basis, which is such that every vector in the space is a unique linear combination of basis vectors. There is an analogous construction in group theory, this time producing only certain special groups rather than all of them. Given a group G and a subset S of G such that $s^{-1} \notin S$ whenever $s \in S$, one says that G is free on S or freely generated by S if for every $g \in G$ there are unique elements $s_1, \dots, s_n$ such that $g = s_1 \dots s_n$, where for each i either $s_i \in S$ or $s_i^{-1} \in S$ and no $s \in S$ appears next to s^{-1} among the s_i. (In particular, the identity element 1 is uniquely realized as the empty product of elements of S). For example, if $G = \langle g \rangle$ is cyclic, then G is freely generated by $S = \{g\}$. Given any abstract set S, there is a group $F(S)$ freely generated by S. Start with the set of strings $s_1 \dots, s_n$ of symbols (called words) such that for all i either $s_i \in S$ or s_i is the formal symbol s^{-1} for some $s \in S$.

Define the word $s = s_1 \dots s_n$ to be reduced if no $s \in S$ appears next to s^{-1} among the s_i. Call n the length of s. Let $F(S)$ consist of all reduced strings. Define a product on this set by decreeing that $(s_1 \dots s_n)(t_1 \dots t_m)$ is the unique string obtained from the concatenation $s_1 \dots s_n t_1 \dots t_m$ by deleting pairs of successive terms ss^{-1} or $s^{-1}s$ for $s \in S$ until the resulting string is reduced. I will take it as clear that this reduced string is unique (but see pages 216 and 217 for a proof of this). Then it is clear that this product is associative and has the empty string as the multiplicative identity; defining $(s_1 \dots s_n)^{-1} = s_n^{-1} \dots s_1^{-1}$ (where of course one takes $(s^{-1})^{-1}$ to be s if $s \in S$) we see that $F(S)$ is closed under inverses, so is a group. We call S a free basis of $F(S)$; the cardinality of S is called the rank of $F(S)$ (p. 218). We will see later that the rank of a free group is well defined.

Any map π from the set S into a group H extends uniquely to a homomorphism from $F(S)$ to H, sending the word $s_1 \ldots s_n$ to the product $\pi(s_1) \ldots \pi(s_n)$, where $\pi(s^{-1})$ is taken to be $\pi(s)^{-1}$ (Theorem 17, p. 217). In particular, if G is generated by a subset S (so that any $g \in G$ is a product of elements of S and their inverses) then there is a surjective homomorphism from the free group $F(S)$ onto G.

Now any subspace S of a vector space V over a field has a basis which can be enlarged to a basis of V. Remarkably (and for totally different reasons) any subgroup of a free group F likewise admits a free basis, though this basis does not in general sit inside any basis of F.

Nielsen-Schreier Theorem: Theorem 19, p. 218

Any subgroup of a free group is free.

Proof.

This argument is not in the text; see for example Schaum's Outline on group theory. Let G be free on the set S. Begin by fixing a total order $<$ on the elements of S; extend it to the disjoint union of S and $S^{-1} = \{s^{-1} : s \in S\}$ by decreeing that $s < s^{-1}$ for $s \in S, s < t^{-1}, s^{-1} < t, s^{-1} < t^{-1}$ if and only if $s < t$, for $s, t \in S$. Extend $<$ to a total order on all reduced words by decreeing first that $s = s_1 \ldots s_m < t = t_1 \ldots t_n$ if either $m < n$ or $m = n$ and the least index i with $s_i \neq t_i$ has $s_i < t_i$. Given a subgroup H of G and a right coset Hx of H in G, denote the unique $<$-smallest word in Hx by $\bar{x}$. The set T of all $\bar{x}$ as Hx runs through the right cosets of H is called a Schreier transversal: it consists of exactly one element of every right coset of H in G and if a reduced word $s_1 \ldots s_n$ lies in T then so too does every initial subword $s_1 \ldots s_i$ for $i \leq n$, by the way $\bar{x}$ was chosen. In particular the empty word 1 is the unique representative of $1H$ in T. □

Proof.

For $s \in S$, $g \in G$ write $h_{g,s} = \bar{g}s\overline{(gs)}^{-1} \in H$, so that $\overline{g}s = h_{g,s}\overline{(gs)}$. One checks immediately that $h_{g,s}$ is unchanged if g is replaced by another element hg in its right coset Hg, so that $h_{g,s} = h_{\overline{g},s}$ for all $g \in G$. Also if we define $h_{g,s^{-1}}$ for $s \in S$ in the same way as $h_{g,s}$, so that $h_{g,s^{-1}} = \overline{g}s^{-1}\overline{(gs^{-1})}^{-1}$, then one checks that $h_{g,s^{-1}} = h^{-1}_{gs^{-1},s}$. Thus the $h_{g,s}$ and $h_{g,s^{-1}}$ generate the same group as the $h_{g,s}$ alone. Also $h_{g,s} = 1$ if and only if $gs \in T$, and similarly for $h_{g.s^{-1}}$. Now I claim that the $h_{g,s}$ different from 1 as s runs over S and t over T freely generate H. □

Proof.

Indeed, given any product $h = s_1 \dots s_n$ lying in H with $s_i \in S$ or $s_i^{-1} \in S$, we have $\overline{s_1 \dots s_n} = 1$. Repeatedly using the definition of the $h_{g,s}$, we first write $\overline{s_1 \dots s_{n-1}} s_n$ as $h_{s_1 \dots s_{n-1}, s_n} \overline{s_1 \dots s_n} = h_{s_1 \dots s_{n-1}, s_n}$, then write $\overline{s_1 \dots s_{n-2}} s_{n-1} s_n$ as a multiple of $\overline{s_1 \dots s_{n-1}} s_n$, and so on, eventually realizing h as a product of various terms $h_{g,s}$ and $h_{g,t^{-1}}$. A typical $h_{t,s} \neq 1$ takes the form $t_1 \dots t_m s s_n^{-1} \dots s_1^{-1}$, where $t_1 \dots t_m$ is a reduced word for $t \in T$ and $s_1 \dots s_n$ is a reduced word for ts. We cannot have $t_m = s^{-1}$, lest $ts = t_1 \dots t_{m_1}$ lie in T, which would force $h_{t,s} = 1$; similarly we cannot have $s = s_n$. Hence the word $t_1 \dots t_m s s_n^{-1} \dots s_1^{-1}$ is reduced, as is its inverse. □

Proof.

Consider the product ww' of two words $w = t_1 \ldots t_m s s_n^{-1} \ldots s_1^{-1}$, $w' = t_1 \ldots t_p t u_1^{-1} \ldots u_1^{-1} \ldots u_q^{-1}$. If the product $s_n^{-1} \ldots s_1^{-1}$ wipes out the $t_1 \ldots t_p t$, then $t_1 \ldots t_p t$ to coincide with an initial subword $s_1 \ldots s_i$ of $s_1 \ldots s_n$ and so lies in T, forcing $w' = 1$. If $s_n^{-1} \ldots s_1^{-1}$ alone does not wipe out $t_1 \ldots t_p t$ but $s s_n^{-1} \ldots s_1^{-1}$ does, then $w' = w^{-1}$. Thus any nonempty reduced product of nonidentity $h_{s,t}$ and $h_{s,t}^{-1}$ terms is different from 1 (its final subword is the same as that of its last term), and the nonidentity $h_{s,t}$ freely generate H, as claimed. □

We can make this result more precise by determining which generators $h_{t,s}$ are equal to 1. We have $h_{t,s} = 1$ if and only if $ts \in T$. For every nonidentity element $x \in T$, the reduced word for t either ends in either s or s^{-1}, for some $s \in S$. If it ends in s, then $xs^{-1} \in T$ and the element $h_{xs^{-1},s} = 1$; if it ends in s^{-1}, then $xs \in T$ and $h_{t,s} = 1$. These are the only $h_{t,s}$ equal to 1. So in particular if S and T are both finite, say equal to n and m, respectively, then of the mn elements $h_{s,t}$ for $s \in S, t \in T$, exactly $m - 1$ are equal to 1.

Corollary

A subgroup of index m of a free group of rank n is free of rank $nm - m + 1$.

In particular, free groups of finite rank can admit free subgroups of larger rank, or even infinite rank. For example, starting out with the free group G of rank two generated by x, y and moding out by the normal subgroup H generated by all conjugates of x, we find that the quotient group is the free group on one generator y. Here the Schreier transversal constructed in the above proof is $\{y^n : n \in \mathbb{Z}\}$ (taking $y < x$); all nonidentity elements here end with y, so the free generators of H are the conjugates $y^n xy, y^{-n}$ as n runs over $\mathbb{Z}$ and H has infinite rank.

More generally, given a free group G on generators $s_1, s_2 \dots$ and various words $w_1, w_2, \dots$ on these generators, the quotient G/N of G by the subgroup N generated by all conjugates of the w_i is normal in G; it is said to be presented by the relations $w_i = 1$ (see p. 218); note that any homomorphism π from G to another group H with all w_i lie in the kernel uniquely induces a homomorphism from G/N to H. We have seen above that any finitely generated group is a homomorphic image of a free group of finite rank; the above results show that a subgroup with index m of a group generated by n elements is generated by at most $nm + 1 - m$ elements. A subgroup of a finitely generated group of infinite index need not be finitely generated.