

Math 504, 10/7

Last time we learned that every subgroup of a free group is free, but in the Alice in Wonderland world of free groups subgroups can require more generators than the free group itself (even infinitely many generators). The free group construction can be generalized to something called the *free product*. Let G_1, \dots, G_k be any k groups. Their free product, often denoted $G_1 * G_2 * \dots * G_k$, consists by definition of all words x_1, \dots, x_n where each x_i lies in some G_j and no two consecutive x_i lie in the same G_j . We multiply any two words $x_1, \dots, x_n, y_1, \dots, y_m$ as before by first concatenating them as $x_1, \dots, x_n y_1, \dots, y_m$ then replacing any pair $z_i z_j$ of consecutive terms lying in the same G_j by their product in G_j . In the special case where each $G_i = \mathbf{Z}$, we just get the free group on k generators s_1, \dots, s_k (where now we write words as products of powers of the s_i instead of products of the s_i and their inverses), but in general the construction does not give a free group. You will study two examples of it in homework this week: the free product of two copies of \mathbf{Z}_2 turns out to be infinite dihedral, while the free product of \mathbf{Z}_3 and \mathbf{Z}_2 turns out to be the so-called modular group $PSL_2(\mathbf{Z})$. It contains a copy of the free group F_2 on two generators but is not itself free.

Given the free group F on a set $S = \{s_1, \dots, s_k\}$ and any map π from S to another group H , it extends uniquely to a homomorphism from F into H , which is onto if the image of π generates H . This observation provides the basis for the theory of group presentations: given F as above and a set W of words in it, the group *presented by S and the W* is by definition the quotient of F by the normal subgroup of it generated by all conjugates of elements of W . The theory of group presentations is a whole subject in its own right, which we won't have time for in any detail, but let me mention a couple of intriguing examples. Look first at the *triangle groups* generated by three elements x, y, z with relations $x^{r_1} = y^{r_2} = z^{r_3} = xyz = 1$. This group turns out to be finite if and only if r_1, r_2, r_3 satisfy the key inequality in our classification of finite subgroups of SO_3 in the first week, namely $(1/r_1) + (1/r_2) + (1/r_3) > 1$. The finite groups that one gets are exactly the noncyclic groups arising in the classification: the triple $(r_1, r_2, r_3) = (2, 2, m)$ gives the dihedral group of order $2m$, while the triples $(2, 3, 3), (2, 3, 4), (2, 3, 5)$ give the symmetry groups of the tetrahedron, octahedron, and icosahedron, respectively, of orders 12, 24, and 60. The symmetric group S_n turns out to be a *Coxeter group*; my colleague Sara Billey will run a topics course on such groups and related topics next quarter. This group is generated by the transpositions $s_i = (i, i+1)$ of adjacent letters $i, i+1$, for $1 \leq i \leq n-1$; its defining relations are $s_i^2 = 1$ for all i , $s_i s_j = s_j s_i$ for $|i-j| \geq 2$, and finally $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ if $1 \leq i \leq n-2$. A famous problem in group theory called the *Burnside problem* considers the group $B(n, k)$ generated by n elements x_1, \dots, x_n with defining relations $w^k = 1$ for all words w in the x_i . The question is when this group is finite. It is quite easy to see that $B(n, 2)$ is the direct product of n cyclic groups of order 2, so is finite; it is not too difficult to show that $B(2, 3)$ is finite (and in fact has order 27). Burnside himself showed that $B(m, 4)$ is finite (though quite large), but as of 2005 at least, it is still not known whether $B(2, 5)$ is finite (though $B(m, 6)$ is!) It is known that $B(2, n)$ is infinite for any odd $n > 665$,

but the case of even n turns out to be much more difficult.

An easy (but very important) special case occurs when we mod out by the commutator $x_i x_j x_i^{-1} x_j^{-1}$ of any two generators x_i, x_j of a free group, say on n generators. The resulting group is isomorphic to \mathbf{Z}^n (each cyclic factor \mathbf{Z} being generated by one of the x_i) and is called *free abelian of rank n* ; its structure is much less chaotic than that of the (honest) free group on n generators. Indeed, it is easy to see by induction on n that any subgroup of \mathbf{Z}^n is isomorphic to \mathbf{Z}^m for some $m \leq n$: this is well known for $n = 1$, and in general, given a subgroup S of \mathbf{Z}^n , one looks at the set of first coordinates of its elements and argues that this set is either 0 or a cyclic subgroup of \mathbf{Z} , say generated by a , where $v = (a, a_2, \dots, a_n)$ lies in S . In this case it is easy to show that S is the direct sum of the cyclic subgroup generated by v and the intersection $S \cap 0 \times \mathbf{Z}^{n-1}$; since the intersection is free abelian, so is S . (The only small fly in the ointment is that it is possible for a proper subgroup of \mathbf{Z}^n to be isomorphic to \mathbf{Z}^n itself.) As a consequence *the free groups F_m, F_n on n and m generators are not isomorphic if $n \neq m$* , for if they were, then the quotients $\mathbf{Z}^m, \mathbf{Z}^n$ of F_m, F_n by their commutator subgroups would be isomorphic. Actually, the above arguments do not quite show that \mathbf{Z}^n is not isomorphic to \mathbf{Z}^m if $n \neq m$, but we will prove this in the next lecture.