Free Groups, Presentations, and Related Topics

Categorical Direct Sums

Suppose X_j, for $j \in J$, is some collection of objects in some mathematical category. By a *direct sum* of the X_j is meant an object S in the category together with morphisms $s_j : X_j \to S$ such that for every object Y in the category and every collection of morphisms $f_j : X_j \to Y$, there *exists* a *unique* morphism $f : S \to Y$ such that $f \circ s_j = f_j : X_j \to Y$.

For example, maybe the category being studied is abelian groups, or left R-modules where R is a ring, or topological spaces, or commutative rings, or (arbitrary) groups. In all these cases, direct sums exist. You know what they are in the first two cases. It is pretty easy to figure out what "categorical direct sums" are in the category of topological spaces and continuous maps. In the last two examples, commutative rings and arbitrary groups, the categorical direct sums are more subtle to construct. We will give the construction for groups. These categorical direct sums are known as "free products" of groups. First, do this easy "uniqueness" exercise about direct sums in any category.

Exercise 1 *In any category, two direct sums, (S, s_j) and (S', s'_j), of the same collection of objects $\{X_j\}$ are "isomorphic" in the category.*

Free Products of Groups

Next, before we construct the correct "direct sum" in the category of groups, make sure you understand why a direct product, say $\mathbb{Z} \times \mathbb{Z}$ to be quite specific, is *definitely not* the categorical "direct sum." The two generators of $\mathbb{Z} \times \mathbb{Z}$ commute. But obviously you could consider two homomorphisms from $\mathbb{Z}$ to some group G so that the two images of $\mathbb{Z}$ do not commute in G. Then you can't find a suitable $\mathbb{Z} \times \mathbb{Z} \to G$ fulfilling the "direct sum" requirement.

Let's call the correct direct sum we are looking for in the category of groups by the symbol $\mathbb{Z} * \mathbb{Z}$. If the first $\mathbb{Z}$ is generated by x and the second $\mathbb{Z}$ is generated by y, then $\mathbb{Z} * \mathbb{Z}$ must contain all sorts of products, like $xyx^3y^{-2}x^{-1}$, with no commuting simplifications. So, this will be the actual construction. $\mathbb{Z} * \mathbb{Z}$ will be constructed as a certain set of words in the alphabet $\{x, y, x^{-1}, y^{-1}\}$, along with a product which just juxtaposes words, with certain obvious cancellations when xs or ys are next to their inverses.

It turns out that it is not really harder to construct $*_j G_j$, the "direct sum" of an arbitrary family of groups in the category of all groups. The construction is called the*free product* of the G_j. The elements of $*_j G_j = W$, will be *reduced words*, sequences $w = g_{i(1)} g_{i(2)} \ldots g_{i(n)}$, where $g_{i(j)} \in G_{i(j)}$, with adjacent indices distinct and all group elements different from the identity. We allow the empty word, $\emptyset$, which will be the identity element of $*_j G_j$. There is a well-defined product on this set, W, of reduced words. Start by simply juxtaposing the words, $w_1 w_2$. If all adjacent indices are distinct, that is the product. Otherwise, the last index of the first word must agree with the first index of the second word, $w_1 w_2 = (\cdots g_j)(h_j \cdots)$ with g_j and h_j both in G_j. Reduce the word by replacing these two letters by the single element $g_j h_j \in G_j$. If that product is not the identity element of G_j, you are finished. If that product is the identity in G_j, remove it. Iterate this procedure with the resulting simplified word until a reduced word is obtained. The only possible simplifications and cancellations occur where remnants of the two original words meet, no choices are ever made about where to simplify, so the product is well-defined. Write the reduced product of two words as $[w_1][w_2]$.

The only difficulty in showing that this set of reduced words, W, with the product just defined, is a group, is the proof of the associative law. Identity element, $\emptyset$, and inverses, are obvious. The problem with associativity is that when three words are juxtaposed, you must perform simplifications in two different orders, so it isn't immediate that you always end up with the same reduced word. This is a technical difficulty, which must be handled one way or another. I'll follow a clever approach which embeds W in a product-preserving way in the group S_W of all permutations of the set W.

Define $u_j : G_j \to S_W$ by the rule $u_j(g_j)(w) = [g_j][w]$. The understanding is $[1_j] = \emptyset \in W$, if $1_j \in G_j$ is an identity element. Note the following exercise is essentially a very special case of associativity in W.

Exercise 2 *Show that $[g_jh_j][w] = [g_j]([h_j][w])$. Hence $u_j : G_j \to S_W$ is a group homomorphism.*

Now define $u : W \to S_W$ by composing permutations, that is $u(g_{i(1)}g_{i(2)}\cdots g_{i(n)}) = u(g_{i(1)}) \circ u(g_{i(2)}) \circ \cdots \circ u(g_{i(n)})$. Then the following exercise is exactly the statement of the desired associativity of the product on W, $([w_1][w_2])([w] = [w_1]([w_2][w])$, but the proof just uses the definition of u, the definition of the product in W, and Exercise 2, and avoids actually dealing with three general elements of W.

Exercise 3 *Show that $u([w_1][w_2]) = u([w_1])u([w_2])$.*

OK, we now have a group structure on the set of reduced words $*_jG_j = W$, and we have obvious group homomorphisms $s_j : G_j \to *_jG_j$, since an element of G_j is a (short) word in W.

Exercise 4 *Show that $(*_jG_j, s_j)$ is a categorical direct sum of the G_j in the category of groups.*

Free Groups and Free Objects

Suppose each $G_j \cong \mathbb{Z}$, an infinite cyclic group. The resulting free product is called a *free group*. Suppose X is any set. For each $x_j \in X$, let $Z_j = \langle x_j \rangle \cong \mathbb{Z}$ denote an infinite cyclic group with generator x_j. A homomorphism $s_j : Z_j \to H$ is the same data as an element $h_j \in H$, since the element $h_j = s_j(x_j)$ determines the homomorphism. Therefore, the free group $F(X) = *_jZ_j$ has the following universal property:

Let $i : X \subset F(X)$ denote the obvious inclusion of the given set of generators of the Z_j into $*_jZ_j = F(X)$. For any group H and any function $f : X \to H$, there *exists* a *unique* group homomorphism $\phi : F(X) \to H$ such that $\phi \circ i = f$.

Note there is a categorical similarity here with the concept of a basis of a vector space, or more generally a basis X of a free module, F, over any ring. X is a subset of F so that every function $f : X \to N$, where N is any module, extends to a unique module homomorphism $\phi : F \to N$. This universal property defines free objects in any category in which the objects are sets and the morphisms are functions. If X is a set and $i : X \to F$ is a function, where F is an object in some such category, then (F, i) is the free object on the set X in the category if for every function $f : X \to N$ from a set X to an object N in the category, there *exists* a *unique* morphism $\phi : F \to N$ in the category such that $\phi \circ i = f$. Another familiar example is found in the category of commutative rings with unit. The free object on X is the polynomial ring $\mathbb{Z}[X]$, that is, polynomials on symbols $x_j \in X$. The universal proof about uniqueness up to isomorphism of objects satisfying some universal property shows that if a free object on X exists then it is unique up to isomorphism.

In the case of free groups, each non-identity element of $F(X)$ has a unique expression $x_{j(1)}^{e(1)}x_{j(2)}^{e(2)}\cdots x_{j(n)}^{e(n)}$, where the $e(j)$ are non-zero integers and adjacent x_js never coincide. The multiplication is juxtaposition, followed by combining powers of any resulting adjacent terms involving the same x_j, and erasing identity elements if they occur. This perhaps seems somewhat more elementary and explicit than our previous construction of the free product of an arbitrary family of groups, but one has the same technical difficulties with associativity in this special case as one has in the general construction.

A rather remarkable theorem is that any subgroup of a free group is also a free group. But one can't say much about the number of generators. If n is a positive integer, or if n is $\aleph_0$, then the free group on 2 generators contains subgroups that are free on n generators. However, here is one result about the number of generators of a free group.

Exercise 5 *If $F \cong F'$, where F and F' are free groups on sets X and X', respectively, then $|X| = |X'|$. (If you are stuck here, do Exercise 6 below first.)*

Generators and Relations

If G is a group and $R \subset G$ is a subset, what is the smallest normal subgroup $N(R) \subset G$ which contains R? The answer is obviously this: $N(R)$ is the set of all finite products of conjugates of elements of R and their inverses. These products must be contained in any normal subgroup of G that contains R, and this set of products is a normal subgroup of G. The quotient projection $p : G \to G/N(R)$ clearly has the following universal property. If $f : G \to H$ is a group homomorphism with $R \subset \ker f$, then there exists a unique homomorphism $\phi : G/N(R) \to H$ such that $f = \phi \circ p : G \to G/N(R) \to H$.

If $X = \{x_j\}$ is a set and $R = \{r_i\} \subset F(X)$ is a subset of the free group on generators X, that is, R is a set of words, then the notation $\langle x_j \mid r_i \rangle = F(X)/N(R)$ is used to denote the group "generated by set X subject to relations R". If $f : X \to H$ is any function from X to a group H such that $f(r_j) = 1 \in H$ for all $r_j \in R$, then there exists a unique group homomorphism $\phi : F(X)/N(R) \to H$ "extending" f. This universal property characterizes $\langle x_j \mid r_i \rangle$ up to isomorphism.

It is very difficult to determine, in fact, in complete generality impossible to determine, whether a group presented with given generators and relations is a finite group or even a non-trivial group. It is also impossible to determine in general whether two words in $F(X)$ become equal in $F(X)/N(R)$. However, given an explicit group G, such as a symmetric group or a semi-direct product group or a matrix group, it is often possible to identify generators and relations which present G, that is, prove $G \cong \langle x_j \mid r_i \rangle$, for certain elements $x_j \in G$ satisfying relations given by words r_i.

Exercise 6 *Show that $\langle x_j \mid x_j x_{j'} x_j^{-1} x_{j'}^{-1}$, for all $j, j' \rangle$ is the free abelian group (i.e. direct sum of $\mathbb{Z}$s) with basis $X = \{x_j\}$. Do this the right way, namely, by showing that the group in question is abelian and has the correct universal property in the category of abelian groups.*

Amalgamated Products

Suppose G and H are two groups and $g : K \to G$ and $h : K \to H$ are two homomorphisms from a third group K to G and H, respectively. Define the amalgamated product $G *_{K,g,h} H$ to be the group $(G * H)/N(R)$, where $R = \{g(x)h(x^{-1}) \mid x \in K\}$. In other words, in the free product $G * H$, impose relations which force the two images of $x \subset K$ to coincide.

Exercise 7 *Show that $G *_{K,g,h} H$, together with the two obvious homomorphisms $u : G \to G *_{K,g,h} H$ and $v : H \to G *_{K,g,h} H$, has the following universal property: For every group L and every pair of homomorphisms $p : G \to L$ and $q : H \to L$ such that $p \circ g = q \circ h : K \to L$, there exists a unique homomorphism $\phi : G *_{K,g,h} H \to L$ such that $\phi \circ u = p$ and $\phi \circ v = q$.*

Of course this exercise is trivial, you just quote two other universal properties. One could construct more elaborate amalgamated products involving several ingredient groups and homomorphisms. But this basic amalgamated product occurs very naturally in topology, providing a computation of the fundamental group of certain unions of two topological spaces, in terms of the fundamental groups of the separate spaces and their intersection. It is useful to not be intimidated by the algebraic details underlying the construction of this group.