Section 6: Direct Products

One way to build a new groups from two old ones, say G, H, is to take the set $G \times H$ of ordered pairs of elements, the first from G and the second from H, and give them the obvious operation: G's operation on the first coordinates and H's on the second. This group is called the *direct product* of G and H, and G, H are called the *factors.* We have already seen this in at least one of the exercises: 2.1**g)** was $\mathbb{R} \times (\mathbb{R} - \{0\})$, with addition in the first coordinate and multiplication in the second. And of course in the context of linear algebra, $\mathbb{R}^n$ is just the direct product of n copies of $\mathbb{R}$ under addition (along with scalar multiplication to make it a vector space) — notice that we can have as many factors as we like, so that our elements can be, not just ordered pairs, but ordered triples, ordered quadruples, etc. (Technically, they can also be "infinituples", and that can yield some interesting results, but we'll only look at finite ones, at least for a while.)

One reason that this construction is useful is that the product is usually no "nicer" than either of its factors. For example:

- Of course if both factors G, H are finite groups, then $|G \times H| = |G||H|$ is also finite; but if either is infinite, then the direct product is infinite.
- If either factor is nonabelian, then the direct product is nonabelian.
- If either is not cyclic, then the direct product is not cyclic. (But if both are cyclic, the direct product may still not be cyclic. See below.)

So, for example, if we wanted a nonabelian group of order 80, we could use $Q_8 \times \mathbb{Z}_{10}$.

There are some pretty obvious subgroups of a product. For example, $G \times \{e_H\}$ "behaves just like" G and $\{e_G\} \times H$ "behaves just like" H. If A is any subgroup of G and B is any subgroup of H, then $A \times B$ is a subgroup of $G \times H$. And depending on what G, H are, there are probably others as well: We know that in $\mathbb{R}^2$, all the lines through the origin are additive subgroups, but only two — the axes — are of the form (subgroup of $\mathbb{R}$)$\times$(subgroup of $\mathbb{R}$).

Sometimes it can be useful to realize that a group "behaves just like" a direct product of groups. For example, V is essentially the same group as $\mathbb{Z}_2 \times \mathbb{Z}_2$. And suppose k, n are positive integers with $k < n$; then while $\mathcal{S}_n$ is a large group, with $n!$ elements, its subgroup H_k, the set of all functions f for which $f(\{1, 2, \ldots, k\}) = \{1, 2, \ldots, k\}$ and $f(\{k+1, k+2, \ldots, n\}) = \{k+1, k+2, \ldots, n\}$, behaves just like $\mathcal{S}_k \times \mathcal{S}_{n-k}$, and has $k!(n-k)!$ elements.

Prop: Let $G_1, G_2, \ldots, G_n$ be groups, and $x_i \in G_i$ for $i = 1, 2, \ldots, n$. Then the order of the element $(x_1, x_2, \ldots, x_n)$ of $G_1 \times G_2 \times \ldots \times G_n$ is the least common multiple of the orders of the x_i's.

Pf: The identity of the product is the n-tuple of identities, and for any positive integer m, $((x_1, x_2, \ldots, x_n)^m = (x_1^m, x_2^m, \ldots, x_n^m)$, so this power is the identity exact when m is a multiple of the order of all the x_i's. So the least power of the n-tuple that gives the identity is the least common multiple of the orders of the x_i's.//

Cor: Let $G_1, G_2, \ldots, G_n$ be finite cyclic groups. Then $G_1 \times G_2 \times \ldots \times G_n$ is cyclic iff the orders of the G_i's are pairwise relatively prime.

Pf: The order of $G_1 \times G_2 \times \ldots \times G_n$ is the product of the orders of the G_i's, so the direct product is cyclic iff it has an element with that order. If x_i is a generator of G_i for each i, then the least common multiple of the orders of the x_i's is equal to their product exactly when their orders are pairwise relatively prime, and in that case $(x_1, x_2, \ldots, x_n)$ is a generator. If they are not relatively prime, then for any element $(y_1, y_2, \ldots, y_n)$ of $G_1 \times G_2 \times \ldots \times G_n$, $o(y_i)|o(x_i)$, so the least common

multiple of the orders of the y_i's is at most the least common multiple of the orders of the x_i's and hence less than the order of $G_1 \times G_2 \times \ldots \times G_n$; so the direct product has no generator and is not cyclic.//

Challenge: If either of G, H is infinite cyclic, and the other is nontrivial, can $G \times H$ be (obviously infinite) cyclic?

Section 7: Functions

Saracino wrote this chapter before Math 250 existed, so there is really nothing in this chapter that you don't already know:

- A function f from a set X to another set Y (which may be X) is a set of ordered pairs (x, y) where $x \in X$, $y \in Y$, and every element of X is the first component in exactly one of the ordered pairs in f — but the way we really think of f is as an "association" of each x in X to the element y in Y for which (x, y) is an ordered pair in f. In this case we denote y by $f(x)$, call y the "image of x under f", and write $f : X \to Y : x \mapsto y$.

- For a function $f : X \to Y$, X is called the "domain" of f, Y is the "codomain", and $\{f(x) \in Y : x \in X\}$, denoted $f(X)$, is called the "image" of f. (Some books use the word "range" for the codomain, while others use it for the image, so I'll try to avoid it entirely.)

- If $f : X \to Y$ and $g : Y \to Z$ are functions, then the "composition" of f and g is the function $g \circ f : X \to Z$, defined by $(g \circ f) : X \to Z : x \mapsto g(f(x))$. This is meaningful only if the domain of g contains as a subset the image of f.

- For a subset A of X, the set $f(A) = \{f(a) \in Y : a \in A\}$ is the "image of A under f", a subset of Y. For a subset B of Y, the set $f^{-1}(B) = \{x \in X : f(x) \in B\}$ is the "inverse image of B under f", a subset of X. (Shortly we will define, for certain restricted f's, an inverse function f^{-1}; but this use of the symbol f^{-1}, acting on subsets rather than elements of the codomain, makes sense for any function. It should be noted, however, that $f^{-1}(B)$ may be empty — this is the case if $B \cap f(X) = \emptyset$ — or much larger than B, if there are many elements of X with the same image in B.)

- A function $f : X \to Y$ is "one-to-one", or "injective", if different elements of X always have different images in Y. This property is usually checked via the contrapositive: assuming that elements x_1, x_2 of X have the same image $f(x_1) = f(x_2)$ in Y, and showing (somehow) that $x_1 = x_2$.

- A function $f : X \to Y$ is called "onto Y" (I will try to include the codomain in this terminology, though many do not), or "surjective", if $f(X) = Y$, i.e., if every element of Y is $f(x)$ for at least one x in X.

- If $f : X \to Y$ is both one-to-one and onto Y, then f is called a "one-to-one correspondence" or "bijection". (The adjectival form, corresponding to "injective" and "surjective" is "bijective".) In this case, reversing the components in all of the ordered pairs that make up f gives a new function $f^{-1} : Y \to X$, called the "inverse (function)" of f. It has the property that $f \circ f^{-1}$ is the identity function $y \mapsto y$ on Y and $f^{-1} \circ f$ is the identity function $x \mapsto x$ on X.