Day 10

A few more comments on semidirect products.

Proposition: The 8-element quaternion group Q is not a semidirect product.

Proof: The only normal subgroup of Q is the 2-element subgroup $Z = \{\pm 1\}$. The quotient group Q/Z is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So if Q *were* a semidirect product it would have to be a semidirect product of Z with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}2$. But that would mean Q would have a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so it would have 3 elements of order 2 *other than* ± 1. That's not the case.

Proposition: If H and K are two groups, and $\phi : K \to \mathrm{Aut}(H)$ is a homomorphism, you can construct the semi-direct product $T = H \rtimes_\phi K$. If you have an automorphism $\tau \in \mathrm{Aut}(K)$, you can modify ϕ by taking $\phi' = \tau\phi$. The resulting semidirect product $T' = H \rtimes_{\phi'} K$ is isomorphic to T.

Proof: Indeed, the map

$$f : T' \to T$$

defined by $f(hk) = h\tau(k)$ is an homomorphism:

$$f(t_1t_2) = f(h_1k_1h_2k_2) = f(h_1\phi'_{k_1}(h_2)k_1k_2) = h_1\phi'_{k_1}(h_2)\tau(k_1)\tau(k_2) = h_1\phi_{\tau(k_1)}(h_2)\tau(k_1)\tau(k_2).$$

On the other hand

$$f(t_1) = h_1\tau(k_1)$$

and

$$f(t_2) = h_2\tau(k_2).$$

Then

$$f(t_1)f(t_2) = h_1\phi_{\tau(k_1)}(h_2)\tau(k_1)\tau(k_2).$$

Since it's bijective, it's an isomorphism. ## The fundamental theorem of finitely generated abelian groups

Theorem: Let G be a finitely generated abelian group. Then there is an integer $r \geq 0$ and integers $d_1, \ldots, d_k$ all at least two such that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}.$$

Remark: The integer r is determined by G up to isomorphism. There are various ways to standardize the d_i so that they determine G up to isomorphism but we take that up separately.

We will give a more-or-less constructive proof of this theorem.

Let $g_1, \ldots, g_s$ be a generating set for G. Consider the surjective homomorphism

$$\pi : \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{s} \to G$$

that sends the element e_i having a one in position i and zeros elsewhere to g_i.

By the isomorphism theorems, if N is the kernel of this map, then G is isomorphic to $\mathbb{Z}^s/N$. We will study N.

Let's write the elements of $\mathbb{Z}^s$ as column vectors using the basis $\{e_i\}_{i=1}^s$. At first we know very little about N except that it is generated by a (potentially infinite) set of elements of $\mathbb{Z}^s$. Let's choose generators $n_1, n_2, \ldots$ for N and organize them in a matrix with integer entries (and potentially infinitely many columns):

$$\mathbf{N} = \begin{bmatrix} n_{11} & n_{12} & n_{13} & \ldots \\ \vdots & \vdots & \vdots & \vdots \\ n_{s1} & n_{s2} & n_{s3} & \ldots \end{bmatrix}$$

First we are going to show that in fact N is finitely generated, so we can assume N has only finitely many columns.

Subgroups of finitely generated abelian groups are finitely generated.

Lemma: We show first that any subgroup of $\mathbb{Z}^s$ is finitely generated.

Proof: We will proceed by induction on s. If $s = 1$, N is a subgroup of $\mathbb{Z}$, and we know that any such subgroup is of the form $d\mathbb{Z}$ and is therefore generated by one element.

Suppose that any subgroup of $\mathbb{Z}^{s-1}$ is finitely generated and that $n_1, \ldots$ generate $N \subset \mathbb{Z}^s$. Consider the last row of the associated matrix $\mathbf{N}$. The integers $n_{s1}, n_{s2}, \ldots$ generate a subgroup of $\mathbb{Z}$ that is generated by the smallest positive element d of this subgroup, which is the greatest common divisor of all of these n_{sj}. Then there are finitely many indices $i_1, i_2, \ldots, i_p$ and integers $a_1, \ldots, a_p$ such that

$$d = \sum_{j=1}^{p} a_j n_{si_j}.$$

The vector $n = \sum_{j=1}^{p} a_j n_{i_j} \in N$ has d as its last element. For each column n_i of $\mathbf{N}$, there is an integer k_i so that $n_i' = n_i - k_i n$ has a zero in its last entry. The set consisting of n and the n_i' generate N. But the n_i' all belong to a copy $\mathbb{Z}^{s-1}$ since their last entry is zero, so by induction the subgroup of $\mathbb{Z}^{s-1}$ they generate

is finitely generated.
Therefore N is finitely generated.

In fact we've shown that any subgroup of $\mathbb{Z}^s$ is generated by at most s elements because we add at most one generator at each step in the induction.

Corollary: Any subgroup of a finitely generated abelian group G is finitely generated.

Proof: A finitely generated abelian group is a quotient of $\mathbb{Z}^s$. Given a subgroup H of G, it is the image of a subgroup $\tilde{H}$ of $\mathbb{Z}^s$, which is finitely generated. The images of the generators of $\tilde{H}$ in H generate H.

Note: THIS IS FALSE for nonabelian groups.

Proof of the fundamental theorem

As above, given as finitely generated abelian group, choose a surjective map

$$\pi : \mathbb{Z}^s \to G.$$

The kernel N of this map is generated by a set $\mathbf{n}$ of at most s elements, and we can arrange the generators of the kernel into a $s \times s$ matrix $\mathbf{N}$, adding zero columns if necessary.

The matrix $\mathbf{N}$ defines a homomorphism (we use the sa)

$$\mathbf{N} : \mathbb{Z}^s \to \mathbb{Z}^s$$

sending an element of the first $\mathbb{Z}^s$ viewed as a column vector v to the second by matrix multiplication $\mathbf{n}v$. .

The image of this homomorphism is exactly the kernel N of the map π. This is because N is generated by the columns of the matrix $\mathbf{N}$, and if

$$v = \begin{bmatrix} v_1 \\ \vdots \\ v_s \end{bmatrix}$$

is a column vector,

then

$$\mathbf{N}v = \sum_{i=1}^{s} v_i n_i$$

where the n_i are the columns of $\mathbf{N}$, so the collection of products $\mathbf{N}v$ is exactly the subgroup of $\mathbb{Z}^s$ generated by the columns of N.

We showed the following in our discussion of automorphisms.

Lemma: Suppose $f : \mathbb{Z}^s \to \mathbb{Z}^s$ is an automorphism. Then there is an invertible $s \times s$ matrix $\mathbf{F}$ with integer entries so that $f(v) = \mathbf{F}v$ where we write $v \in \mathbb{Z}^s$ as a column vector.

The composition $\mathbf{N} \circ f$ is given by the matrix $\mathbf{NF}$. Since f is an automorphism, the image of $\mathbf{NF}$ in $\mathbb{Z}^s$ is the same as the image of $\mathbf{N}$, namely N.

Now suppose we apply an automorphism k of $\mathbb{Z}^s$ on the right side of the map $\mathbf{N}$. In that case, the image $k(N)$ need not be N, but it is still the case that $\mathbb{Z}^s/g(N)$ and $\mathbb{Z}^s/N$ are isomorphic, and therefore $\mathbb{Z}^s/g(N)$ is isomorphic to our original group G.

Therefore up to isomorphism we can modify our matrix $\mathbf{N}$ by multiplying it on either side by invertible $s \times s$ integer matrices without changing the quotient G we are trying to compute.

In particular we can:

- swap rows and columns of $\mathbf{N}$
- multiply any row or column of $\mathbf{N}$ by ± 1
- do elementary row and column operations on $\mathbf{N}$ – that is, replace a column n_i by $n_i - an_j$ for any integer a, and similarly for rows.

Using these operations, proceed as follows:

0. If the matrix is zero, the G is $\mathbb{Z}^s$ and we're done. Otherwise, swap rows so the first row isn't zero.
1. Make every element in the first row positive, and then swap columns so the smallest element in the first row is in the upper left corner of $\mathbf{N}$. Call that element a.
2. Use elementary column operations to reduce the other elements in the first row to be less than a.
3. Repeat steps 1 and 2 until the upper left entry is the only nonzero entry.
4. Now follow the same process using row operations until the only nonzero entry in the first column is in the upper left corner.
5. Each round of this makes the entry in the upper left corner smaller, so eventually you must reach a point where the first row and column of the matrix are zero, except for the upper left entry, which could be zero or nonzero.
6. Now continue this reduction process on the $(s-1) \times (s-1)$ submatrix.
7. Eventually you reach a diagonal matrix.

When you have a diagonal matrix, you can see that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_{s-r}\mathbb{Z}$$

where r is the number of zero diagonal elements and the d_i are the nonzero ones.

Corollary: If the matrix **N** is invertible, its determinant is the order of G.