MATH 3311, FALL 2025: LECTURE 32, NOVEMBER 14

Video: `https://youtu.be/OnWWmZj46x4`
Recall the following important result from last time:

Proposition 1. *Suppose that G is an abelian group. Then the following are equivalent:*

(1) G is finitely generated.
(2) There exists $m \geq 1$ and a surjective *homomorphism $f : \mathbb{Z}^m \to G$.*
(3) There exists $m \geq 1$ and a subgroup $H \trianglelefteq \mathbb{Z}^m$[1] *such that we have an isomorphism*

$$\mathbb{Z}^m/H \xrightarrow{\simeq} G.$$

Proof. (1)⇒(2): If $\langle X \rangle = G$ for a finite subset $X = \{x_1, \dots, x_m\}$, then we can write down a unique homomorphism $f : \mathbb{Z}^m \to G$ with $f(\vec{\mathbf{e}}_i) = x_i$. The image of this homomorphism is exactly $\langle X \rangle = G$, and so f is the desired surjective homomorphism.

(2)⇒(3): The factoring triangle (or the first isomorphism theorem) gives us:

$$\mathbb{Z}^m/\ker f \xrightarrow{\simeq} \mathrm{im}\, f = G.$$

So (3) holds with $H = \ker f$.

(3)⇒(2): Let $\overline{f} : \mathbb{Z}^m/H \xrightarrow{\simeq} G$ be the isomorphism. Then the composition

$$f = \overline{f} \circ \pi : \mathbb{Z}^m \xrightarrow{\pi} \mathbb{Z}^m/H \xrightarrow[\overline{f}]{\simeq} G$$

is *surjective*.

(2)⇒(1): If $f : \mathbb{Z}^m \to G$ is surjective, then the finite set $X = \{f(\vec{\mathbf{e}}_1), \dots, f(\vec{\mathbf{e}}_m)\}$ generates G (why?). □

Note that we used the following observation that we saw last time:

Observation 1. For any group G, there is a canonical *bijection*

$$\mathrm{Hom}(\mathbb{Z}^m, G) \xrightarrow[\simeq]{f \mapsto (f(\vec{\mathbf{e}}_1, \dots, f(\vec{\mathbf{e}}_m)))} \{m\text{-tuples of commuting elements in } G\}.$$

Example 1. Suppose that $G = \mathbb{Z}^2$. Then giving a homomorphism $\mathbb{Z}^3 \to G$ amounts to specifying three elements of $\mathbb{Z}^2$. For instance, we can do

$$\vec{\mathbf{e}}_1 \mapsto (2,2)\ ;\ \vec{\mathbf{e}}_2 \mapsto (0,0)\ ;\ \vec{\mathbf{e}}_3 \mapsto (1,0)$$

This homomorphism will send (a_1, a_2, a_3) to $(2a_1 + a_3, 2a_1)$, and so for instance we will have

$$f((1,1,1)) = (3,2).$$

As it happens, this map is not surjective, because the second coordinate of any element in the image will always be *even*.

Example 2. If we take the above example, but instead change the image of $\vec{\mathbf{e}}_1$: Send $\vec{\mathbf{e}}_1$ to $(2,1)$. This changes the homomorphism to:

$$(a_1, a_2, a_3) \mapsto (2a_1 + a_3, a_1).$$

This will now be surjective. However, neither homomorphism in these two examples is injective: they both send $\vec{\mathbf{e}}_2$ to 0.

So our job is now clear: understand what quotients of $\mathbb{Z}^m$ look like. For this, we will need:

Proposition 2. *Let $H \leq \mathbb{Z}^m$ be a subgroup. Then $H \simeq \mathbb{Z}^n$ for some $n \leq m$.*

[1] Note that any subgroup of the abelian group $\mathbb{Z}^m$ is automatically normal.

Proof. The proof will be by induction on m.

For the base case of $m = 1$, we note that every subgroup of $\mathbb{Z}$ looks like $d\mathbb{Z}$ for some integer $d \in \mathbb{Z}$, and so is isomorphic to $\mathbb{Z}$ (if $d \neq 0$) or to $\{0\} = \mathbb{Z}^0$ (if $d = 0$).

Now, for the inductive step: Consider the subgroup

$$\mathbb{Z}^{m-1} \simeq \{(a_1, \ldots, a_{m-1}, 0) : \; a_i \in \mathbb{Z}\} \leq \mathbb{Z}^m.$$

The subgroup $H \cap \mathbb{Z}^{m-1} \leq \mathbb{Z}^{m-1}$ is now isomorphic (by our inductive hypothesis) to $\mathbb{Z}^{n'}$ for some $n' \leq m - 1$.

Now, the quotient $H/(H \cap \mathbb{Z}^{m-1})$ is isomorphic to the image of H in the quotient $\mathbb{Z}^m/\mathbb{Z}^{m-1} \xrightarrow[\simeq]{(a_1,\ldots,a_m)\mapsto a_m} \mathbb{Z}$. This image is a subgroup of $\mathbb{Z}$ and so is isomorphic to $\mathbb{Z}^r$ for $r = 0$ or $r = 1$ (this is our base case).

Therefore, Problem 9 on Homework 11 tells us that we have $H \simeq \mathbb{Z}^{n'+r}$. Since $n' \leq m - 1$ and $r \leq 1$, $n = n' + r \leq m$, and the proof is complete. $\square$

Example 3. The fact from HW 11 used above is particular to the case where the quotient is isomorphic to a power of $\mathbb{Z}$. For instance, $\mathbb{Z}/4\mathbb{Z}$ admits $\mathbb{Z}/2\mathbb{Z}$ as the subgroup generated by 2 and the quotient is again isomorphic to $\mathbb{Z}/2\mathbb{Z}$. However, $\mathbb{Z}/4\mathbb{Z}$ is *not* isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.