

**MATH 3311, FALL 2020: LECTURE 25, OCTOBER 28**

Finitely generated abelian groups

Recall the following from Homework 3:

**Fact 1.** Giving a homomorphism  $f : \mathbb{Z} \rightarrow G$  is equivalent to specifying the element  $f(1) = g \in G$ ; if  $G$  is an abelian group with operation given by addition, then  $f$  is now given by  $f(n) = f(n \cdot 1) = n \cdot g$ .

We will now find that giving *tuples* of elements in an abelian group  $G$  is equivalent to giving a homomorphism from another family of groups. Namely, for every  $d \in \mathbb{Z}_{\geq 1}$ , we consider

$$\mathbb{Z}^d = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{d\text{-times}}.$$

In this group, we have the  $d$  standard basis elements

$$\vec{e}_i = (0, \dots, 0, 1, \dots, 0),$$

with 1 in the  $i$ -th position and 0s elsewhere.

**Fact 2.** Giving a homomorphism  $f : \mathbb{Z}^d \rightarrow G$  from  $\mathbb{Z}^d$  to an abelian group  $G$  is equivalent to specifying  $d$ -elements  $g_1 = f(\vec{e}_1), g_2 = f(\vec{e}_2), \dots, g_d = f(\vec{e}_d) \in G$ . Then  $f$  is determined by the formula:

$$f((a_1, \dots, a_d)) = a_1 f(\vec{e}_1) + \cdots + a_d f(\vec{e}_d) = a_1 g_1 + \cdots + a_d g_d.$$

How can we apply this to the study of finite abelian groups? Suppose that  $G$  is a finite abelian group with  $G = \{g_1, \dots, g_d\}$ . By the previous fact, we have a homomorphism

$$f : \mathbb{Z}^d \xrightarrow{\vec{e}_i \mapsto g_i} G.$$

**Observation 1.** We obtain a factoring diagram

$$\begin{array}{ccc} \mathbb{Z}^d & & \\ \pi \downarrow & \searrow f & \\ \mathbb{Z}^d / \ker f & \xrightarrow[\bar{f}]{} & G. \end{array}$$

In particular,  $G$  is isomorphic to the quotient  $\mathbb{Z}^d / \ker f$ .

*Proof.* The bottom arrow is injective by general properties of the factoring triangle (why?). The diagonal arrow is surjective since every element of  $G$  is in its image by definition. This implies that the bottom arrow is also surjective, and hence an isomorphism.  $\square$

What the observation tells us is that understanding quotients of  $\mathbb{Z}^d$  by its subgroups would help us understand all finite abelian groups. But it would do a little more than that.

**Question 1.** Suppose that we have a subgroup  $H \leq \mathbb{Z}^d$  and an isomorphism  $\mathbb{Z}^d / H \xrightarrow{\cong} G$ . What does this mean for  $G$ ?

To answer this, let us consider the factoring triangle:

$$\begin{array}{ccc} \mathbb{Z}^d & & \\ \pi \downarrow & \searrow f & \\ \mathbb{Z}^d / H & \xrightarrow[\bar{f}]{} & G. \end{array}$$

The fact that the bottom arrow is an isomorphism is equivalent to two facts:

- $\ker f = H$ ;
- $f$  is surjective.

But note that  $f$  is determined by  $g_i = f(\vec{e}_i)$ ,  $1 \leq i \leq d$  by the formula

$$f((a_1, \dots, a_d)) = a_1 g_1 + \dots + a_d g_d.$$

This shows that the image of  $f$  consists exactly of the integer linear combinations of  $g_1, \dots, g_d$ . That is, we find:

**Observation 2.**  $f$  as above is surjective if and only if every element of  $G$  is an integer linear combination of  $g_1 = f(\vec{e}_1), \dots, g_d = f(\vec{e}_d)$ .

This leads to the following definition:

**Definition 1.** An abelian group  $G$  is **finitely generated** if one of the following equivalent conditions holds for some integer  $d \in \mathbb{Z}_{\geq 1}$ :

- (1) There are elements  $g_1, \dots, g_d \in G$  such that every element  $g \in G$  is of the form

$$g = a_1 g_1 + \dots + a_d g_d$$

for  $a_1, \dots, a_d \in \mathbb{Z}$ .

- (2) There is a surjective homomorphism  $f : \mathbb{Z} \xrightarrow{\vec{e}_i \mapsto g_i} G$ .

- (3)  $G$  is isomorphic to a quotient  $\mathbb{Z}^d/H$  for some subgroup  $H \leq \mathbb{Z}^d$ .

In this situation, we will say that  $g_1, \dots, g_d$  **generate**  $G$ .

*Remark 1.* You can think of this in terms of linear algebra: What we are doing is starting with finitely many elements and looking at their ‘span’, which is the set of all of their integer linear combinations. This basically gives us the smallest subgroup that can contain these elements. They *generate* the group, when this smallest subgroup is the full group itself.

*Example 1.* By Observation 1, any finite group is finitely generated: it is generated for instance by the set of all its elements.

*Example 2.*  $\mathbb{Z}^d$  is finitely generated: the standard basis elements  $\vec{e}_1, \dots, \vec{e}_d$  generate it. Alternatively  $\mathbb{Z}^d$  is isomorphic to the quotient  $\mathbb{Z}^d/\{0\}$  of itself.

*Example 3.* If  $G_1$  and  $G_2$  are finitely generated by  $d$  and  $m$  elements respectively, then  $G_1 \times G_2$  will be generated by  $d + m$  elements. Namely, if  $G_1$  is generated by  $g_1, \dots, g_d$  and  $G_2$  is generated by  $h_1, \dots, h_m$ , then  $G_1 \times G_2$  will be generated by

$$\{(g_i, 0) : 1 \leq i \leq d\} \cup \{(0, h_j) : 1 \leq j \leq m\}.$$

For instance,  $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}^d$  will be a finitely generated abelian group, because each of the factors is so.

You will prove the following on problem 9 on Homework 9:

**Proposition 1.** Every subgroup  $H \leq \mathbb{Z}^d$  is isomorphic to  $\mathbb{Z}^m$  for some  $m \leq d$ .

**Corollary 1.** For any subgroup  $H \leq \mathbb{Z}^d$ , there is a homomorphism

$$f : \mathbb{Z}^m \rightarrow \mathbb{Z}^d.$$

such that  $f(\mathbb{Z}^m) = \text{im } f = H$ .

*Proof.* Choose an isomorphism  $\mathbb{Z}^m \xrightarrow{\cong} H \leq \mathbb{Z}^d$ , and think of it as a homomorphism

$$f : \mathbb{Z}^m \rightarrow \mathbb{Z}^d.$$

□

So we have the following sequence of deductions:

- Understanding quotients of  $\mathbb{Z}^d$  for all  $d$  (that is, finitely generated abelian groups) will help us understand all finite abelian groups.
- Understanding subgroups of  $\mathbb{Z}^d$  is the same as understanding quotients of  $\mathbb{Z}^d$ .

- Understanding homomorphisms  $f : \mathbb{Z}^m \rightarrow \mathbb{Z}^d$  is the same as understanding subgroups of  $\mathbb{Z}^d$ .

What we see is that we need to study a rather concrete set of objects: Homomorphism from  $\mathbb{Z}^m$  to  $\mathbb{Z}^d$ . This is what we will do next week.