MATH 3311, FALL 2025: LECTURE 31, NOVEMBER 12

Video: `https://youtu.be/qO5B0v3q2cA`

Finitely generated abelian groups

Definition 1. Suppose that G is a group and $X \subset G$ is a subset. The **subgroup generated by** X, denoted $\langle X \rangle \leq G$ is the smallest subgroup of G containing X.

Remark 1. This notion makes sense, since the intersection of any collection of subgroups containing X is once again a subgroup containing X, so $\langle X \rangle$ can be taken to be the intersection of all subgroups containing X.

Remark 2. More concretely, we have

$$\langle X \rangle = \{x_1^{\pm 1} x_2^{\pm 2} \cdots x_m^{\pm -1} : \ x_i \in X, \ m \geq 1\}.$$

That is, we take all possible products of elements of X as well as of their inverses.

Remark 3. If $X = \{x\}$ is a singleton, then $\langle X \rangle = \langle x \rangle$ is just the cyclic subgroup generated by the element x.

Definition 2. G is **finitely generated** if there is a finite subset $X \subset G$ such that $\langle X \rangle = G$. In other words, there is a finite set of symbols such that every element of G can be expressed as a product of such symbols.

We will be concerned with the problem of *classifying* finitely generated abelian groups. That is, we want a complete, non-redundant list of such groups up to isomorphism. But before we enter the abelian realm, let us look at the following non-abelian example.

Example 1. Take

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{Z}, \ ad - bc = 1 \right\}$$

This is actually a *group* under matrix multiplication: The condition on the determinant tells us that we can write the inverse as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Elements of $\mathrm{SL}_2(\mathbb{Z})$ can be obtained as follows. Note that the condition $ad - bc = 1$ shows that the pairs a, b, a, c, c, d and b, d are all relatively prime. In other words, the entries of each row and column of the matrix have to be relatively prime to each other.

Conversely, if a, b are relatively prime, then by Bezout we can find c, d such that $ad - bc = 1$ (why?), and so we can find a matrix in $\mathrm{SL}_2(\mathbb{Z})$ with the first row given by (a, b). For example, we have

$$\begin{pmatrix} 2 & 3 \\ -1 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In particular, $\mathrm{SL}_2(\mathbb{Z})$ is an *infinite* group.

In any case, two matrices we can find in here are

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \ ; \ S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Note that we have $T^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ for any $m \in \mathbb{Z}$ and we have $S^2 = -I_2$ is the negative identity matrix. So T does not have finite order while S has order 4.

A non-trivial result now is that $\mathrm{SL}_2(\mathbb{Z}) = \langle \{S, T\} \rangle$: So this is a *non-abelian, finitely generated infinite* group.

Let us now move firmly into the abelian world. The starting point for our classification is the following observation.

Definition 3. For $1 \leq i \leq m$, the i-th **standard basis vector** $\overrightarrow{\mathbf{e}}_i \in \mathbb{Z}^m$ is the element with 1 as its i-th coordinate and 0s everywhere else. For example, in $\mathbb{Z}^3$, we have

$$\overrightarrow{\mathbf{e}}_1 = (1,0,0), \overrightarrow{\mathbf{e}}_2 = (0,1,0), \overrightarrow{\mathbf{e}}_3 = (0,0,1).$$

Remark 4. The element $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ can be written (uniquely) as a linear combination $\sum_{i=1}^m a_i \overrightarrow{\mathbf{e}}_i$.

Observation 1. Suppose that G is an abelian group and $X = \{x_1, \ldots, x_m\} \subset G$ is a finite subset of elements. Then there is a unique homomorphism

$$f : \mathbb{Z}^m \to G$$

such that $f(\overrightarrow{\mathbf{e}}_i) = x_i$ for $i = 1, \ldots, m$.

Proof. The point is that, because of the homomorphism property, given this description for standard basis vectors, we must have

$$f((a_1, \ldots, a_n)) = f(\sum_{i=1}^m a_i \overrightarrow{\mathbf{e}}_i) = f(a_1 \overrightarrow{\mathbf{e}}_1 + \cdots + a_m \overrightarrow{\mathbf{e}}_m) = f(a_1 \overrightarrow{\mathbf{e}}_1) f(a_2 \overrightarrow{\mathbf{e}}_2) \cdots f(a_m \overrightarrow{\mathbf{e}}_m) = x_1^{a_1} \cdots x_m^{a_m}.$$

Here, in the third and fourth equalities, we have used the homomorphism property of f: Note that $f(a_i \overrightarrow{\mathbf{e}}_i) = f(\overrightarrow{\mathbf{e}}_i)^{a_i}$, because we are using multiplicative notation for the operation in G.

So the only possibility for f as a function is $f((a_1, \ldots, a_m)) = x_1^{a_1} \cdots x_m^{a_m}$. We need to know that this is a *homomorphism*. For this, note:

$$\begin{aligned} f((a_1, \ldots, a_m)) \cdot f((b_1, \ldots, b_m)) &= (x_1^{a_1} \cdots x_m^{a_m})(x_1^{b_1} \cdots x_m^{b_m}) \\ &= x_1^{a_1+b_1} \cdots x_m^{a_m+b_m} \\ &= f((a_1+b_1, \ldots, a_m+b_m)) \\ &= f((a_1, \ldots, a_m) + (b_1, \ldots, b_m)). \end{aligned}$$

Here, in the second line, we have used the *abelianness* of G to collect all the powers of each x_i together. □

Remark 5. We didn't actually use the full strength of abelianness of G. You just needed the elements $x_1, \ldots, x_m$ to commute with each other. So we can say that there is a canonical *bijection*

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

Observation 2. If f is as in Observation 1, then we have

$$\mathrm{im}\, f = \langle X \rangle \leq G.$$

Proof. This follows from the description of f in the proof of Observation 1, combined with Remark 2. □

Observation 3. If f is as in Observation 1, then f is surjective if and only if $\langle X \rangle = G$.

Putting this all together, we get:

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 $H \trianglelefteq \mathbb{Z}^m$ such that we have an isomorphism

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

Proof. Observations 1-3 tell us that (1)⇔(2), and the equivalence (2)⇔(3) is just the first isomorphism theorem. □