9/16

Free abelian groups & finitely generated abelian groups §2.1, 2.2

A (too) optimistic goal would be to classify all groups up to isomorphism. But for important classes of groups, this is possible. We will do it for a subclass (finitely generated) of abelian groups.

First we need to talk about free abelian groups.

Def'n Let G be an abelian group. A subset $B \subseteq G$ is called a basis (or base) is every element $g \in G$ has a unique expression as $g = \sum_{i=1}^{n} m_i x_i$ with $m_i \in \mathbb{Z}$ and $x_i \in B$.

(Here and throughout we use additive notation for abelian groups)

G is called free if it posseses a basis.

Rmk: This is very similar to notion of basis in linear algebra (over a field) except that the coefficients are in $\mathbb{Z}$.

Thm Let G be a free abelian group and let B_1, B_2 be two bases of G. Then the cardinalities of B_1 and B_2 are the same.

Def'n The rank of a free abelian group G is the cardinality of (any one of its) bases.

Thm Let G be a free abelian group of finite rank n. Then $G \cong \mathbb{Z}^n$.

Rmk In fact even for G of infinite rank ω we have $G \cong \mathbb{Z}^{\omega}$ if this is interpreted suitably (have to use direct sum rather than direct product).

Rmk: We have presentation $\mathbb{Z}^n = \langle x_1, x_2, \ldots, x_n \mid x_i x_j = x_j x_i \rangle$ (making the generators commute makes all elements commute).

Just like every group is a quotient of a free group, every abelian group is a quotient of a free abelian group. We will restrict our attention to finitely generated abelian groups because these are more tractable.

Thm Let G be a finitely generated abelian group, generated by n elements $x_1, \ldots, x_n$. Then $G \cong \mathbb{Z}^n/H$ for some subgroup $H \leq G$.

All of the previous theorems are relatively straightforward. Now we come to the classification theorem, which is more involved:

Thm (Classification of Finitely Generated Abelian Groups)
Let G be a finitely generated abelian group, then there are unique integers $r \geq 0$, $m_1, m_2, \ldots, m_k$ with $m_1 \geq 2$ and $m_1 | m_2 | \cdots | m_k$ "divides"
such that $G \cong \mathbb{Z}^r \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$.

Of course, we can have $r = 0$ (if G is finite) or $k = 0$ (if G is free).

Def'n An element $x \in G$ of a (not necessarily abelian) group G is called torsion if $x^n = 1$ for some $n \geq 1$.

In an abelian group G, the set $\mathrm{Tor}(G)$ of torsion elements (which in additive notation have $nx = 0$ for some $n \geq 1$) forms a subgroup, called the torsion subgroup (or torsion part) of G.

G is called torsion-free if $\mathrm{Tor}(G) = \{0\}$ and in general $G/\mathrm{Tor}(G)$ is called the torsion-free part of G.

So the classification says that for an abelian finitely-gen. gp. G, the torsion part is $\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z}$ and the torsion-free part is $\mathbb{Z}^r$.

Cor For G a fin. gen. abelian gp., also can write G uniquely as
$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{s_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{s_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_\ell^{s_\ell}\mathbb{Z}$$
where the $p_1, p_2, \dots, p_\ell$ are prime numbers (allowed to repeat).

Pf of corollary from thm: If n and m are coprime then
$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ (exercise for you!).
Thus if $m = p_1^{a_1} p_2^{a_2} \cdots p_\ell^{a_\ell}$ is the prime factorization of m,
then $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/p_1^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{a_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z}$. $\boxtimes$

Remark The integers $m_1 | m_2 | \cdots | m_k$ from thm are the invariant factors of G.
The prime powers $p_1^{s_1}, \dots, p_\ell^{s_\ell}$ from cor. are the elementary divisors of G.

E.g. $G = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ is the invariant factor representation,
equiv. to $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, elementary divisor rep.

So how to prove classification of fin. gen. abelian groups?
We know $G \simeq \mathbb{Z}^n/H$ for some subgroup $H \leq \mathbb{Z}^n$.
Normally (haha) we've been quotienting by kernels of homomorphisms,
but since we're dealing with abelian gp's, we can quotient by images.
The cokernel, $\mathrm{coker}(\varphi)$, of a homomorphism $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$
is $\mathbb{Z}^n/\mathrm{im}(\varphi)$, the codomain mod the image.
We can represent φ by a $\overset{n\times m}{\text{matrix}}$ with integer coeff's: $y_1, \dots, y_m$ are gen's of $\mathbb{Z}^m$, $x_1, \dots, x_n$ are gen's of $\mathbb{Z}^n$

φ represented by M

e.g. $\begin{bmatrix} 3 & 0 & 1 \\ 2 & 1 & -4 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = [\underbrace{3y_1 + y_3}_{\cdot x_1}, \underbrace{2y_1 + y_2 - 4y_3}_{\cdot x_2}]$ for $y_1, \dots, y_3 \in \mathbb{Z}$.

Small exercise: We can take m finite, i.e., we only need to impose finitely many relations.

So any fin. gen. ab. gp. G is of form $G \simeq \mathrm{coker}(\varphi)$ for some $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$.
So we need to understand structure of cokernels of $\mathbb{Z}$-matrices.

<u>Thm</u> (<u>Smith Normal Form</u>) Let $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$ be a homo. represented by a $n \times m$ matrix M with coeff's in $\mathbb{Z}$.
Then $M = SDT$ where T $n \times n$ matrix, S $m \times m$ matrix are <u>invertible over $\mathbb{Z}$</u> and $D = (d_{ij})$ is a $\mathbb{Z}$ matrix whose off-diagonal $(i \neq j)$ entries are zero and whose diagonal entries $m_i = d_{i,i}$ satisfy $m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_K$.

<u>E.g.</u> A matrix in SNF looks like $D = \begin{bmatrix} 1&0&0&0&0 \\ 0&2&0&0&0 \\ 0&0&6&0&0 \\ 0&0&0&0&0 \end{bmatrix}$. The cokernel will be

$$\mathrm{coker}(D) = \underbrace{\cancel{\mathbb{Z}/1\mathbb{Z}}}_{} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/0\cdot\mathbb{Z}$$
$$= \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$ in the form we want!

Since multiplying on left and right by invertible over $\mathbb{Z}$ matrices does not change the $\mathbb{Z}$-image, this proves the classification!

To prove the Smith Normal Form theorem, we need an <u>algorithm</u> that tells us how to convert M to SNF via a series of $\mathbb{Z}$-invertible row and column operations:

e.g. $M = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \xrightarrow[\text{col from 1st}]{\text{sub. 2nd}} \begin{bmatrix} 1 & 1 \\ -2 & 2 \end{bmatrix} \xrightarrow[\text{col from 2nd}]{\text{sub. 1st}} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = D$ ✓

<u>Think</u>: RREF and Gaussian elimination. But I skip the full description of the SNF algorithm.

<u>Remark</u>: In fact SNF works for <u>modules</u> over any <u>PID</u> (<u>Principal Ideal Domain</u>). We may return to this later in the semester... //