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 $G \simeq \mathbb{Z}^n$.

Rmk: In fact even for $G$ of infinite rank $\omega$ we have $G \simeq \mathbb{Z}^\omega$ 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 $x_1, \dots, x_n$. 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 $r \geq 0$, $m_1, m_2, \dots, m_k$ 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 finitely-gen. abelian 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, $\operatorname{coker}(\varphi)$, of a homomorphism $\varphi: \mathbb{Z}^m \to \mathbb{Z}^n$
is $\mathbb{Z}^n/\operatorname{im}(\varphi)$, the codomain mod the image.
We can represent $\varphi$ by a $n \times m$ 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 $\mathbb{Z}^n$

e.g. $\varphi$ represented by $M$
$$\begin{bmatrix} 3 & 0 & 1 \\ 2 & 1 & -4 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = [\underbrace{3y_1 + y_3}_{\cdot x_1}, \underbrace{2y_1 + y_2 - 4y_3}_{\cdot x_2}] \text{ for } y_1, \dots, y_3 \in \mathbb{Z}.$$
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</u> <u>Normal</u> <u>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</u> <u>over</u> $\mathbb{Z}$ and $D = (d_{ij})$ is a $\mathbb{Z}$-matrix whose off-diagonal ($i \neq j$) entries are zero and whose diagonal entries $m_i = d_{i,i} \geq 0$ satisfy $m_1 \mid m_2 \mid m_3 \mid \cdots \mid m_k$.

<u>E.g.</u> A matrix in SNF looks like $D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & & 0 & 0 \end{bmatrix}$. The cokernel will be $\mathrm{coker}(D) = \cancel{\mathbb{Z}/1\mathbb{Z}} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/0\cdot\mathbb{Z}$
$= \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ 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. $M = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \xrightarrow[\text{col from 1st}]{\text{sub. 2nd}} \begin{bmatrix} 1 & 1 \\ -2 & 2 \end{bmatrix} \xrightarrow[\text{col from 2nd, and add 1st row to 2nd}]{\text{sub. 1st}} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = D$ ✓

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

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

9/18

## Action of a group on a set §2.4

Groups are often collections of symmetries. Let's take this idea further.

Def'n Let $G$ be a group and $X$ a set. An action of $G$ on $X$ is a function $G \times X \to X$, denoted $(g,x) \mapsto g \cdot x$, such that $e \cdot x = x \ \forall x \in X$ and $(gh)x = g(hx) \ \forall g,h \in G, x \in X$.

E.g. The symmetric group $S_n$ acts on $X = \{1, 2, \dots, n\}$ by $\sigma \cdot i = \sigma(i)$ for all $\sigma \in S_n$, $i \in X$.

In fact, in general an action of $G$ on $X$ is the same as a homomorphism $G \to S_X$ (the symmetric group of bijections $X \to X$) where $g \in G$ is sent to the function $g \cdot x$, for $x \in X$.

We say the action is faithful if this homomorphism is a monomorphism, i.e., if $g \cdot x = x \ \forall x \in X$ implies $g = e$.

Prop. Every group $G$ acts faithfully on itself $X = G$ by (left) translation: $g \cdot h = gh$.

Proof: Straightforward. ☒

Cor (Cayley) Every finite group $G$ of order $n$ embeds as a subgroup of the symmetric group $S_n$.

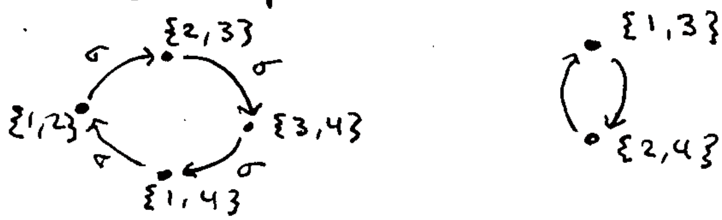
---

Any embedding of $G$ as a subgroup $G \leq S_n$ gives an action of $G$ on $[n] := \{1, 2, 3, \dots, n\}$.

E.g. $G = \mathbb{Z}/4\mathbb{Z} \cong \langle \sigma \rangle \leq S_4$ with $\sigma = (1, 2, 3, 4)$ gives standard action of $G$ on $\{1, 2, 3, 4\}$.

But from this we can get more actions on other sets...

For example, $G$ also acts on $X = \binom{[4]}{2} = \{\text{2-element subsets of } [4]\}$ in a natural way: $\sigma \cdot S = \{\sigma(i) : i \in S\}$ $\forall\, S \in X$.
We can represent this action via this directed graph:




$\Leftarrow$ 2 orbits of $G \curvearrowright X$

<u>Prop.</u> Let $G \curvearrowright X$ ("$G$ act on $X$"). Define $x \sim y$ for $x, y \in X$ if $\exists\, g \in G$ s.t. $g \cdot x = y$. Then $\sim$ is an equiv. rel. on $X$.

<u>Def'n</u> When $G \curvearrowright X$ the equivalence class $\overline{x}$ of $x \in X$ under this equivalence relation is called the <u>orbit</u> of $x$.

<u>Prop.</u> Let $G \curvearrowright X$ and $x \in X$. Then $G_x = \{g \in G : g \cdot x = x\}$ is a subgroup of $G$.

<u>Def'n</u> This $G_x$ is called the <u>stabilizer</u> of $x \in X$.

<u>Thm</u> (Orbit-Stabilizer Theorem) Let $G \curvearrowright X$. Then for any $x \in X$, the cardinality of the orbit of $x$ is $[G : G_x]$.
In particular if $G$ is finite, size of orbit of $x$ is $\frac{|G|}{|G_x|}$.

<u>Pf.</u> Notice $gx = hx$ for $g, h \in G \iff g^{-1}hx = x \iff g^{-1}h \in G_x$
$\iff hG_x = gG_x$ so elements in $x$'s orbit are in bijection w/ cosets of stabilizer $G_x$ $\boxtimes$

<u>E.g.</u> In the previous example, taking $S = \{1,2\}$,
the stabilizer is $G_{\{1,2\}} = \{e\}$, and orbit has size $4 = \frac{4}{1}$.
But with $S' = \{1,3\}$, the stabilizer is $G_{\{1,3\}} = \{e, \sigma^2\}$
and orbit has size $2 = \frac{4}{2}$.

We said before that $G$ acts on itself via (left) translation, but there is another action of $G$ on itself that is very important:

Def'n $G$ acts on $X = G$ by conjugation $(g, h) \mapsto ghg^{-1}$.
We always write this as $ghg^{-1}$ to avoid confusion with $g \cdot h$.
The orbit of $x \in G$ under the conjugation action is called the conjugacy class of $x$, i.e., $\{gxg^{-1} : g \in G\}$.
The stabilizer of $x \in G$ under the conjugation action is called the centralizer of $x$, denoted $C_G(x) = \{g \in G : gx = xg\}$.

Def'n The center of $G$, denoted $Z(G)$, is the set of elements in $G$ that commute with all elements of $G$, i.e. $Z(G) = \{g \in G : gh = hg \ \forall h \in G\}$.

Prop. $Z(G)$ is a normal subgroup of $G$.
Pf: Straightforward. ☒

Prop. $Z(G) = \{g \in G : C_G(x) = G\}$ Pf: Again, immediate from definition ☒

Thm (Class Equation) Let $G$ be a finite group and let $x_1, \ldots, x_n$ be representatives of the conjugacy classes of $G$.
Then $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$.
If $x_1, \ldots, x_m$ are representatives of the conjugacy classes that contain more than one element, then

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)].$$

Pf: The conjugacy classes partition $G$, so the first equality is clear from the orbit-stabilizer theorem.
Then notice $x \in Z(G) \Leftrightarrow [G : C_G(x)] = 1$, so 2nd equality follows. ☒

Let's use the class equation to say something about finite $p$-groups; an important class of finite groups.

<u>Def'n</u> $G$ is a finite $p$-group (for $p$ a prime number) if the order of $G$ is $p^n$ for some $n \geq 0$.

<u>Thm</u> Let $G$ be a nonabelian finite $p$-group. Then $Z(G)$ is a nontrivial normal subgroup ($\neq \{e\}$ or $G$), so $G$ is not simple.

<u>Pf</u>: Look at the class equation $|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$.
By ~~assumption~~ Lagrange's thm, $p$ divides $[G : C_G(x_i)]$ for all the $x_i$, since $[G : C_G(x_i)] \neq 1$ (or else these $x_i$ would be in $Z(G)$). Also clearly $p$ divides $|G|$ by assumption. So then $p$ divides $|Z(G)|$. But $|Z(G)| \neq 0$ since $e \in Z(G)$. So $Z(G)$ must have some other element in it besides $e$, and so $Z(G)$ is nontrivial. Also $Z(G) \neq G$ since $G$ is nonabelian. ☒

We also showed on the homework that the only groups $G$ that have no nontrivial subgroups are $\mathbb{Z}/p\mathbb{Z}$ for $p$ prime, hence these are the only abelian simple groups.

<u>Cor</u> The only finite simple $p$-groups are $\mathbb{Z}/p\mathbb{Z}$.

<u>Note</u>: A more general definition of $p$-group is a group $G$ such that the order of every $g \in G$ is a power of $p$. We will see soon (using Cauchy's thm) why this matches our definition in the case of finite groups.

We will develop more tools to show that finite groups of various orders cannot be simple, in order to possibly understand all finite simple groups (a big goal!)