Takehome 2

Due Tuesday, March 23rd

This assignment will walk you through a proof of the structure theorem for finite abelian groups. **There are many important results from Lecture 18 that you will need, so I recommend watching that first if you haven't yet!** We will prove the following:

Theorem 1 (Fundamental Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group. Then:*

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s},$$

for a unique sequence of integers $(n_1, n_2, \cdots, n_s)$ with each $n_i \geq 2$ and $n_{i+1} | n_i$.

Recall that we call the decomposition from Theorem 1 the *invariant factor decomposition*. We will deal with the existence and uniqueness of such a decomposition separately. Our first goal is the following proposition, which does most of the heavy lifting.

Proposition 2. *Every finite abelian group is the direct product of cyclic groups.*

1. Step one is to reduce the problem to finite abelian p-groups. Let G be a *finite abelian* group.
   (a) Explain why G has a *unique* Sylow p-subgroup for each prime p. This justifies our use of the word *the* in the following.
   (b) Suppose G has order $p^\alpha q^\beta$ for distinct primes p and q. Let P be the Sylow p-subgroup, and Q the Sylow q-subgroup. Show that $G \cong P \times Q$.
   (c) In general the prime factorization of $|G|$ is $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$. Show by induction on t that G is the product of its Sylow subgroups. Explicitly, this means that if P_i is the Sylow p_i-subgroup for $i = 1, \cdots, t$, then

   $$G \cong P_1 \times P_2 \times \cdots \times P_t.$$

   (d) Explain why if we prove Proposition 2 for each of the P_i, then we have proved Proposition 2 for G.

By Exercise 1, we have reduced the proof of Proposition 2 to following:

Proposition 3. *Let A be an abelian p-group i.e., one of prime power order p^α. Then A is a product of cyclic groups.*

We will do this by induction on α. An important base case will be the case of *elementary abelian p-groups*, defined in **Lecture 18**. We record the definition and basic property below.

Definition/Proposition 4 (Stated and proved in Lecture 18)**.** *An abelian p group E of order p^r is called a elementary abelian p-group if every $x \in E$ has order $\leq p$. If E is an elmentary abelian p-group of order p^r then:*

$$E \cong \underbrace{Z_p \times \cdots \times Z_p}_{r\text{-times}}.$$

Note: We proved Definition/Proposition 4 in Lecture 18, you don't need to reproduce the proof here, but it isn't a bad idea to review the proof.

2. Let A be a nontrivial abelian p-group. Define the p-power map $\varphi : A \to A$ by the rule $\varphi(x) = x^p$.
   (a) Show that φ is a homomorphism.
   (b) Let $A_p = \ker\varphi = \{a : a^p = 1\} \trianglelefteq A$. Show that A_p is an elementary abelian p-group.
   (c) Let $A^p = \operatorname{im}\varphi = \{a^p : a \in A\} \leq A$. Show that $A/A^p \cong A_p$. (Hint, show they are elementary abelian p-groups of the same order, then apply Definition/Proposition 4).
   (d) Conclude $|A^p| < |A|$. This will be a crucial ingredient for our induction step.
3. We will now prove Proposition 3 by induction on $|A|$.
   (a) First the base case: show that Proposition 3 is true if $|A| = p$.

   We now proceed by induction. For the remainder of this problem you may now assume that Proposition 3 holds for all abelian p-groups smaller than A.

   (b) Show that A^p is the product of cyclic groups. That is $A^p = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle$. (Use the induction hypothesis).
   (c) Show that $A^p \cap A_p$ is an elementary abelian group of order p^t. (Hint: it is clear that it is elementary abelian (why?), so it remains to show it contains p^t elements.)
   (d) We now split into two cases. For the first case, assume that $A_p \leq A^p$
      i. For each generator x_i of A^p (from part (b)), show that there is some $y_i \in A$ with $y_i^p = x_i$.
      ii. Let $A_0 = \langle y_1, \cdots, y_t \rangle$. Show that $A_0 \cong \langle y_1 \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_t \rangle$. (It might be useful to use induction on t).
      iii. Show that $A^p \trianglelefteq A_0$ and that A_0/A^p is an elementary abelian group of order p^t.
      iv. Use part (c) and (d)(iii) to show that $|A_0| = |A|$. Conclude that Proposition 3 holds for A.
   (e) For the second case $A_p \not\leq A^p$, so we know there is some $x \in A_p$ with $x \notin A^p$.
      i. Let $\overline{A} = A/A^p$, and let $\pi : A \to \overline{A}$ be the natural projection. Let $\overline{x} = \pi(x)$. Show that $|x| = |\overline{x}| = p$.
      ii. Show that $\overline{A} \cong \langle \overline{x} \rangle \times \overline{E}$ for some subgroup $\overline{E} \leq \overline{A}$. (Hint: first notice $\overline{A}$ is elementary abelian (why?). Now this should look a lot like the induction step of proof of Definitions/Proposition 4 in Lecture 18).
      iii. Let $E = \pi^{-1}(\overline{E}) \leq A$. Show that $A \cong E \times \langle x \rangle$. Conclude that Proposition 3 holds true for A.

You proved Proposition 3, and therefore by 1(d), also Proposition 2! In **Lecture 18** we described a process which put a product of cyclic groups into an *elementary divisor form*. We also described a process that took a finite abelian group in elementary divisor form, and produced its *invariant factor decomposition*. We will not reproduce that here, and instead assert that this implies the existence part of Theorem 1. Therefore only the uniqueness statement remains. You will need the following definition.

Definition 5. *Let G be a group. The exponent of G is the minimum n such that $x^n = 1$ for all $x \in G$.*

4. We finish by proving the uniqueness part of Theorem 1. We first record that the exponenet of a finite abelian group is related to its invariant factor decomposition.

   (a) Let G be a group and suppose it has the following invariant factor decomposition:

   $$G \cong Z_{n_1} \times \cdots \times Z_{n_s}.$$

   Show that the exponent of G is n_1.

   (b) Let G be a group, and suppose it has 2 invariant factor decompositions. That is:

   $$G \cong Z_{n_1} \times \cdots \times Z_{n_s} \cong Z_{m_1} \times \cdots \times Z_{m_t}.$$

   Use part (a) and the cancellation lemma from HW8 Problem 8 in descending induction to show that $s = t$ and $n_i = m_i$ for every i.