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.

   Proof. Let $P \leq G$ be a Sylow p-subgroup. Since G is abelian, $P \trianglelefteq G$. All Sylow p-subgroups are conjugate, and P is the only conjugate of P, so it is unique. □

   (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 $G \cong P \times Q$.

   Proof. Notice that $P \cap Q = 1$ by Lagrange's theorem, and that $P, Q \trianglelefteq G$ since G is abelian. Therefore by the *recognition theorem for direct products*, we have that $PQ \cong P \times Q$. Also:

   $$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{p^\alpha q^\beta}{1} = |G|,$$

   so that $PQ = G$, and the result follows. □

   (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

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

   Proof. Let $H_i = P_1 P_2 \cdots P_i$. We show that $H_i \cong P_1 \times \cdots \times P_i$ by induction. The base case is part (b) (in fact, the base case where $i = 1$ is trivial). For the induction step, notice that:

   $$H_i = P_1 P_2 \cdots P_{i-1} P_i = H_{i-1} P_i.$$

   By induction,

   $$|H_{i-1}| = |P_1 \times P_2 \cdots \times P_{i-1}| = |P_1||P_2| \cdots |P_{i-1}| = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{i-1}^{\alpha_{i-1}}$$

and the order of $P_i = p_i^{\alpha_i}$. Since all the p_i are distinct, these are coprime, so that by Lagrange's theorem, $H_{i-1} \cap P_i = 1$. They are both normal in G since G is abelian so that:

$$H_i = H_{i-1}P_i \cong H_{i-1} \times P_i \cong P_1 \times \cdots \times P_{i-1} \times P_i,$$

where the last step follows by induction. Therefore we see that:

$$|H_t| = |P_1 \times \cdots \times P_t| = p_1^{\alpha_1} \cdots p_t^{\alpha_t} = |G|,$$

so that $H_t = G$ and the result follows. □

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

Proof. If each P_i is the product of cyclic groups, and G is the product of the P_i, then G is the product of the all the cyclic groups corresponding to each P_i. □

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.

Proof. This amounts to showing that $(xy)^p = x^p y^p$. A priori:

$$(xy)^p = \underbrace{(xy)(xy)\cdots(xy)}_{p \text{ times}},$$

Nevertheless, since A is abelian, we can pass all of the x's to the left, and the y's to the right. Since there are p of each of them, this gives the result. □

(b) Let $A_p = \ker \varphi = \{a : a^p = 1\} \trianglelefteq A$. Show that A_p is an elementary abelian p-group.

Proof. Recall that an elementary abelian p-group is an abelian p-group where every element has order $\leq p$. By Lagrange's theorem $|A_p|$ divides $|A| = p^\alpha$, so that $|A_p|$ is a power of p and so A_p is a p-group. Furthermore, A_p is a subgroup of an abelian group, hence abelian. Finally, fix any $x \in A_p$. Then x is p-torsion so that $x^p = 1$. Therefore $|x| \leq p$. Thus A_p satisfies the definition of being 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).

Proof. We first show A/A^p is an elementary abelian p group. Since it is the quotient of a p-group it is a p-group by Lagrange's theorem. Similarly, quotients are of abelian groups are abelian. Finally, fix $\overline{x} \in A/A^p$, the coset corresponding to $x \in A$. Then $\overline{x}^p = \overline{x^p}$. But since A^p is precisely the p powers of elements in A, we have $x^p \in A^p$. Therefore $\overline{x^p} = \overline{1}$ so that $|\overline{x}| \leq p$. All together this shows that that A/A^p is an elementary abelian p group.

The first isomorphism theorem implies that $\operatorname{im}\varphi \cong A/\ker\varphi$. That is, $A^p \cong A/A_p$. Numerically this means:

$$|A^p| = |A/A_p| = |A|/|A_p|.$$

Cross multiplying,

$$|A_p| = |A|/|A^p| = |A/A^p|.$$

Since A_p and A/A^p are both elementary abelian p groups of the same order (say p^r) then by Definition/Proposition 4, they are both isomorphic to:

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

Therefore they are isomorphic to eachother. □

(d) Conclude $|A^p| < |A|$. This will be a crucial ingredient for our induction step.

Proof. Since A is nontrivial, there is some $1 \neq x \in A$. Then $|x| = p^\ell$ for some ℓ. Notice that $x^{p^{\ell-1}} \neq 1$ and $(x^{p^{\ell-1}})^p = x^{p^\ell} = 1$, so that $x^{p^{\ell-1}}$ is p-torsion. Thus we have a nontrivial element of A_p, so that $|A_p| > 1$. By part (c) this shows that $|A/A^p| > 1$, which implies that A^p cannot be all of A. Since A is finite, the result follows. (We remark that this implies that not every element of a p-group is a p-power.) □

3. We will now prove Proposition 3 by induction on $|A|$.

(a) First the base case: show that Proposition 3 is true if $|A| = p$.

Proof. If $|A| = p$ then $A \cong Z_p$ is cyclic (by TH1 Problem 4(a)), and thus a product of a single cyclic group. □

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).

Proof. We proceed by induction, and therefore assume that Proposition 3 is true for all groups smaller than A. By 2(d), we know $|A^p| < |A|$, hence we apply the inductive hypothesis and are done. $\square$

(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.)

Proof. We first notice that $A^p \cap A_p = \{a \in A^p : a^p = 1\}$, so that it consists precisely of the p-torsion of A^p, (in slighly unweildy notation, it is $(A^p)_p$). Therefore it is an elementary abelian p-group by 2(b). Combining this observation with 3(b), we see that we are studying the p-torsion of a product of cyclic p-groups, so let's begin with the special case of studying the p-torsion of a cyclic p-group.

Lemma 5. *Let $G = \langle x \rangle$ be a cyclic group of order p^ℓ. Then the p-torsion of G is:*

$$G_p = \langle x^{p^{\ell-1}} \rangle.$$

Proof. As any subgroup of a cyclic group is cyclic, the p-torsion of G must be cyclic. The only cyclic groups where the p-power of every element is 1 are the trivial group and Z_p, so that G_p isomorphic to one of these. Arguing as in 2(d), we know that $x^{p^{\ell-1}}$ is a nontrivial p-torsion element of G, so that G_p is nontrivial. Therefore G_p it is a cyclic group of order p, and it contains $\langle x^{p^{\ell-1}} \rangle$, which is also order p. The result follows. $\square$

From this special case, the general case is rather straightforward. All we need to know is how p-torsion works with respect to direct prodcuts.

Lemma 6. *The p-torsion of a product is the product of the p-torsion. That is, let $G = G_1 \times \cdots \times G_n$ be a product of (abelian) groups. Then:*

$$G_p \cong (G_1)_p \times \cdots \times (G_n)_p.$$

Proof. Let $g = (g_1, \cdots, g_n) \in G$. Then $g^p = 1$ if and only if $g_i^p = 1$ for all $i = 1, \cdots, n$, and the result follows. $\square$

To complete the proof we consider the decomposition

$$A^p = \langle x_1 \rangle \times \cdots \times \langle x_t \rangle,$$

from 3(b). Since A^p is a p group, Lagrange's theorem implies each x_i has p-power order, say $|x_i| = p^{\ell_i}$. Putting this together with Lemmas 5 and 6 gives:

$$\begin{aligned} A^p \cap A_p &= (A^p)_p \\ &\cong (\langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle)_p \\ &\cong \langle x_1 \rangle_p \times \langle x_2 \rangle_p \times \cdots \times \langle x_t \rangle_p \\ &\cong \langle x_1^{p^{\ell_1 - 1}} \rangle \times \langle x_2^{p^{\ell_2 - 1}} \rangle \times \cdots \times \langle x_t^{p^{\ell_t - 1}} \rangle. \end{aligned}$$

This exhibits $A^p \cap A_p$ as a product of t copies of Z_p, proving the result. $\square$

(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 $y_i^p = x_i$.

Proof. This is immediate from the definition of A^p. □

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).

Proof. We will make use of the following lemma.

Lemma 7. *Let G be a group, and M, N subgroups. If MN is a subgroup of G, then $MN = \langle M, N \rangle$.*

Proof. Certainly $MN \leq \langle M, N \rangle$. Conversely, we know M and N are in MN, so the subgroup the generate is too since MN is a subgroup. □

We first remark that if $|x_i| = p^{\ell_i}$ like in 3(c), then $|y_i| = p^{\ell_i+1}$. With this in mind, let $H_i = \langle y_1, \cdots, y_i \rangle$ be the subgroup generated by the first i generators, and notice that $H_t = A_0$. We proceed by induction on i. The base case where $i = 1$ is trivial. For the general case, we notice that $H_i = \langle H_{i-1}, y_i \rangle = H_{i-1}\langle y_i \rangle$ by Lemma 7 (noticing that the product is a subgroup since everything in sight is normal). By induction, we know $H_{i-1} \cong \langle y_1 \rangle \times \cdots \times \langle y_{i-1} \rangle$ so it suffices to show that $H_{i-1} \cap \langle y_i \rangle = 1$ so that we can apply the *recognition theorem for direct products*. Fix:

$$a = (y_1^{\alpha_1}, y_2^{\alpha_2}, \cdots, y_{i-1}^{\alpha_{i-1}}) \in H_{i-1},$$

and suppose that $a = y_i^{\alpha_i}$ as well, so that a is in the intersection. Since for all j we have $x_j = y_j^p$, we see that,

$$a^p = (x_1^{\alpha_1}, \cdots, x_{i-1}^{\alpha_{i-1}}) \in \langle x_1 \rangle \times \cdots \times \langle x_{i-1} \rangle,$$

and also $a^p = x_i^{\alpha_i} \in \langle x_i \rangle$. Thus a^p is in the intersection

$$(\langle x_1 \rangle \times \cdots \times \langle x_{i-1} \rangle) \bigcap \langle x_i \rangle, \tag{1}$$

of distinct factors of the product group:

$$(\langle x_1 \rangle \times \cdots \times \langle x_{i-1} \rangle) \times \langle x_i \rangle,$$

so that $a^p = 1$. Therefore for each $j = 1, \cdots, i$, we have $\left(y_j^{\alpha_j}\right)^p = 1$, so that by Lemma 5, we know that $y_j^{\alpha_j}$ is a power of

$$y_j^{p^{\ell_j+1-1}} = y_j^{p^{\ell_j}} = x_j^{p^{\ell_j-1}}.$$

In particular, each $y_j^{\alpha_j}$ is a power of x_j, so that we also know a is in the intersection in Equation 1 above, so that it must be 1 as well. Putting this all together:

$$\begin{aligned} \langle H_{i-1}, \langle y_i \rangle \rangle &= H_{i-1}\langle y_i \rangle \\ &\cong H_{i-1} \times \langle y_i \rangle \\ &\cong \langle y_1 \rangle \times \cdots \times \langle y_{i-1} \rangle \times \langle y_i \rangle. \end{aligned}$$

Letting $i = t$ completes the proof. □

iii. Show that $A^p \trianglelefteq A_0$ and that A_0/A^p is an elementary abelian group of order p^t.

Proof. That $A^p \trianglelefteq A_0$ is immediate since A_0 is abelian. The second statement follows immediately from the following more general lemma (which is essentially HW8 Problem 8(a)).

Lemma 8. *Let $G = G_1 \times \cdots \times G_n$, and let $H_i \trianglelefteq G_i$. Then under the usual identifications $(H_1 \times \cdots \times H_n) \trianglelefteq G$ and*

$$G/(H_1 \times \cdots \times H_n) \cong \frac{G_1}{H_1} \times \cdots \times \frac{G_n}{H_n}.$$

Proof. Build a homomorphism

$$\varphi : G \to \frac{G_1}{H_1} \times \cdots \times \frac{G_n}{H_n},$$

by the rule $\varphi(g_1, \cdots, g_n) = (\overline{g}_1, \cdots, \overline{g}_n)$. This is plainly surjective, and it's kernel consists of elements whose coordinates g_i are in H_i for each i, which is precisely $H_1 \times \cdots \times H_n$. The result follows via the first isomorphism theorem. □

The result follows by Lemma 8 with $G = A_0$ and $H_i = \langle x_i \rangle = \langle y_i^p \rangle$, noticing that $\langle y_i \rangle / \langle y_i^p \rangle \cong Z_p$. □

iv. Use part (c) and (d)(iii) to show that $|A_0| = |A|$. Conclude that Proposition 3 holds for A.

Proof. Since $A_0 \leq A$, we know (by the fourth isomorphism theorem) that

$$A_0/A^p \leq A/A^p \cong A_p,$$

where the isomorphism on the right is 2(c). The left hand side is elementary of order p^t by 3(d)(iii). On the other hand, since we are assuming $A_p \leq A^p$, the right hand side is equal to $A_p \cap A^p$ which is also elementary of order p^t (by 3(c)). Thus we have that $A_0/A^p = A/A^p$, so that counting orders we have $A_0 = A$. By 3(d)(ii), $A = A_0$ is a product of cyclic groups, so we are done. □

(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 $|x| = |\overline{x}| = p$.

Proof. Since $x \in A_p$, we know the order of x is 1 or p. But since $x \notin A^p$, we know $x \neq 1$. So $|x| = p$. We also know $\overline{x}^p = 1$, so that its order is 1 or p. But $x \notin A^p$ so that $\overline{x} \neq \overline{1}$. Thus $|\overline{x}| = p$. □

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 Definition/Proposition 4 in Lecture 18).

Proof. By 2(c), $\overline{A}$ is elementary, say of order p^r. Let $\overline{E} = \overline{A}/\langle \overline{x} \rangle$, and let $\varpi : \overline{A} \to \overline{E}$ be the natural projection. Since $\overline{x}$ has order p, then $\overline{E}$ is elementary of order p^{r-1} (indeed, arguing as in 2(c), the quotient of an elementary abelian p-group is an abelian p-group for free, and then the order of elements condition is inherited by virtue of being a quotient of $\overline{A}$). So $\overline{E} = \langle e_1 \rangle \times \cdots \langle e_{r-1} \rangle$ (by HW8 Problem 5). Let $a_i \in \varpi^{-1}(\overline{e}_i)$, and build a map:

$$\psi : \langle x \rangle \times \overline{E} \to \overline{A},$$

via the rule $\psi(\overline{x}) = \overline{x}$ and $\psi(e_i) = a_i$. Since the two groups have the same order, it suffices to prove surjectivity of ψ. We argue is in our solution to HW8 Problem 5. Fix $a \in A$, and consider:

$$\varpi(a) = (e_1^{j_1}, \cdots, e_{r-1}^{j_{r-1}}).$$

Then $a \cdot a_1^{-j_1} \cdots a_{r-1}^{-j_{r-1}} \in \ker \varpi = \langle \overline{x} \rangle$, say it's x^k. Therefore:

$$a = x^k a_1^{j_1} \cdots a_{r-1}^{j_{r-1}} = \psi(x^k, e_1^{j_1}, \cdots, e_{r-1}^{j_{r-1}}),$$

proving surjectivity and completing the proof. □

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.

Proof. Notice first that $\langle x \rangle E = A$. Indeed, fix any $a \in A$. By 3(e)(ii) we know that $\pi(a) = (\overline{x}^k, \overline{e})$. Then $\pi(x^{-k}a) \in \overline{E}$, so that $a = x^k(x^{-k}a) \in \langle x \rangle E$, proving the claim. Since $|x| = p$, by Lagranges theorem $\langle x \rangle \cap E$ is either 1 or all of $\langle x \rangle$, but $x \notin E$ (since $\overline{x} \notin \overline{E}$), so the intersection is trivial. By the recognition theorem:

$$A \cong \langle x \rangle \times E.$$

But $|E| < |A|$, so that by induction, E is a product of cyclic groups. The result follows. □

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 9. *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.

Proof. We write

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t} \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle,$$

so that the generator of the ith component is x_i with order n_i. Suppose $m|n_1$. Let $k = n_1/m$. Then $|x_1^k| = m$ as an element of Z_{n_1}, and therefore $(x_1^k, 1, \cdots, 1) \in G$ has order m as well.

Conversely, suppose $y \in G$ with $|y| = m$. In coordinates we have $y = (y_1, y_2, \cdots, y_t)$. Then $y^{n_1} = (y_1^{n_1}, y_2^{n_1}, \cdots, y_t^{n_1})$. Each $n_i|n_1$, so call $k_i = n_1/n_i$. Then:

$$y_i^{n_1} = (y_i^{n_i})^{k_i} = 1^{k_i} = 1,$$

because anything in Z_{n_i} to the n_ith power is 1 (by TH2 Problem 3). Thus $y^{n_1} = 1$, so that the order of y divides n_1. This completes the proof.

Since anything to the power n_1 is 1, we know that n_1 is less than or equal to the exponenent of G. But $(x_1, 1, \cdots, 1)$ has order n_1, so the exponent could be no smaller that 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.

Proof. By part (a), the exponent of G is both n_1 and m_1, so $n_1 = m_1$. By HW8 Problem 8, we can cancel Z_{n_1} from each side so that:

$$G_1 = Z_{n_2} \times \cdots \times Z_{n_s} \cong Z_{m_2} \times \cdots \times Z_{m_t}.$$

We still have $n_i, m_i \geq 2$ and $n_{i+1}|n_i$ and $m_{i+1}|m_i$, so these are two invariant factor decompositions of G_1. Again by part (a), we see that $n_2 = m_2$ is the exponent of G_1. Again cancelling with HW8 Problem 8 and continuing in this fashion gives the result. □