

## Takehome 3

Due Monday, April 27th

This assignment will walk you through a proof of the structure theorem for finite abelian groups. 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  $(n_1, n_2, \dots, n_s)$  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 1.** *Every finite abelian group is the direct product of cyclic groups.*

1. Step one is to reduce the problem to  $p$ -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  $i = 1, \dots, t$ , then

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

- (d) Explain why if we prove Proposition 1 for each of the  $P_i$ , then we have proved Proposition 1 for  $G$ .

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

**Proposition 2.** *Let  $A$  be an abelian  $p$ -group i.e., one of prime power order  $p^\alpha$ . Then  $A$  is a product of cyclic groups.*

We will do this by induction on  $\alpha$  but first we must develop an auxiliary tool.

2. Let  $A$  be a nontrivial abelian  $p$ -group. Define the  $p$ -power map  $\varphi : A \rightarrow A$  by the rule  $\varphi(x) = x^p$ .
  - (a) Show that  $\varphi$  is a homomorphism.
  - (b) Let  $A_p = \ker \varphi = \{a : a^p = 1\} \leq A$  be the  $p$ -torsion of  $A$  (first studied in HW4 Problem 2). Show that  $A_p$  is an elementary abelian  $p$ -group (recall the definition from HW8 Problem 5).
  - (c) Let  $A^p = \text{im } \varphi = \{a^p : a \in A\} \leq A$ . Show that  $A/A^p \cong A_p$ . (Hint, show they are elementary abelian  $p$ -groups of the same order, then apply HW8 Problem 5).
  - (d) Conclude  $|A^p| < |A|$ . This will be a crucial ingredient for our induction step.

3. We will now prove Proposition 2 by induction on  $|A|$ .

- (a) First the base case: show that Proposition 2 is true if  $|A| = p$ .
- (b) The induction step is more involved, begin by showing 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 2(d)).
- (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  $A^p$ , show that there is some  $y_i \in A$  with  $y_i^p = x_i$ .
  - ii. Let  $A_0 = \langle y_1, \dots, y_t \rangle$ . 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  $A^p \leq A_0$  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 2 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  $\bar{A} = A/A^p$ , and let  $\pi : A \rightarrow \bar{A}$  be the natural projection. Let  $\bar{x} = \pi(x)$ . Show that  $|x| = |\bar{x}| = p$ .
  - ii. Show that  $\bar{A} \cong \langle \bar{x} \rangle \times \bar{E}$  for some subgroup  $\bar{E} \leq \bar{A}$ . (Hint: first notice  $\bar{A}$  is elementary abelian (why?). Now this should look a lot like the induction step of proof of HW8 Problem 5, in particular, it may be useful to consider the fibers of the projection  $\bar{A} \rightarrow \bar{A}/\langle \bar{x} \rangle$ ).
  - iii. Let  $E = \pi^{-1}(\bar{E}) \leq A$ . Show that  $A \cong E \times \langle x \rangle$ . Conclude that Proposition 2 holds true for  $A$ .

We have now proved Proposition 2, which by 1(d) immediately implies Proposition 1. In class 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. As a useful tool, we provide you with the following lemma which you may use without proof.

**Lemma 1** (Cancellation Property for Products of Finite Groups). *Let  $M, N, K$  be finite groups and suppose  $K \times M \cong K \times N$ . Then  $M \cong N$ .*

**Remark.** *This lemma is more subtle than one might think, and it is not true without assuming the groups are finite. There is a lot to explore here that is beyond the scope of this assignment. For now feel free to use the lemma as a black box, and we will study this problem more deeply in a future assignment.*

Finally, we remind ourselves of the following definition.

**Definition 1.** *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. Let  $G$  be a group, and suppose it has 2 invariant factor decompositions. That is:

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

Where each  $n_i, m_i \geq 2$ , and  $n_{i+1} | n_i$  and  $m_{i+1} | m_i$ . Use HW10 Problem 5 and Lemma 1 in descending induction to show that  $s = t$  and  $n_i = m_i$  for every  $i$ .