Lecture XXI: Classification of finite abelian groups II

§22.1 Classification of finite abelian p-groups:

Last time we discussed the following result.

Theorem 2: Let G be an abelian p-group, say $|G| = p^n$ for $n \geq 1$. Then, there exist $a_1, \ldots, a_k$ with $a_1 \leq a_2 \leq \cdots a_k$ such that $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$ (so, $a_1 + \cdots + a_k = n$) Moreover, k and $a_1 \ldots a_k$ are uniquely determined by G

Proof of Existence:

We used induction to prove the existence. Define

$$a := \max_{g \in G} \{ s \mid \operatorname{ord}(g) = p^s \} = a_k$$

and pick $\sigma = \sigma_k$ any element of G of order p^a.

CASE 1: $a = n$ is clear.

CASE 2: $a < n$

Set $H_k = \langle \sigma_k \rangle$ & use (IH) to decompose
$$G/H_k \underset{\varphi}{\overset{\longleftarrow}{\simeq}} \underset{\langle \bar{y}_1 \rangle}{\overset{\mathbb{Z}/p^{a_1}\mathbb{Z}}{\shortparallel}} \times \cdots \times \underset{\langle \bar{y}_{k-1} \rangle}{\overset{\mathbb{Z}/p^{a_{k-1}}\mathbb{Z}}{\shortparallel}}$$

with $a_1 \leq a_2 \leq \cdots \leq a_{k-1}$ & $a_1 + \cdots + a_{k-1} = n - a$

Notation: $\bar{y}_i \in G/H_k$ of order p^{a_i} with $\bar{y}_i = \varphi((0, \ldots, 0, \underset{i^{\text{th}}\text{ spot}}{1}, 0, \ldots 0))$, so $\operatorname{ord}(\bar{y}_i) = p^{a_i}$ for $i = 1, \ldots, k-1$

We used the following claim to lift the decomposition from G/H_k to G.

Claim 1: For every $i = 1, \ldots, k-1$, we can find $\sigma_i \in G$ such that $\bar{y}_i = \sigma_i H$ $\forall i$
$\operatorname{ord}(\sigma_i) = p^{a_i}$ (in G)

Proof of Claim 1: We want to find $\sigma_i \in G$ such that $\begin{cases} \bullet\ \bar{y}_i = \sigma_i H_k & \forall i = 1, \ldots, k-1 \\ \bullet\ \operatorname{ord}(\sigma_i) = p^{a_i} \text{ (in } G) \end{cases}$

This problem can be handled individually for each i. It is a consequence of the following Lemma, applied to $H = \pi^{-1}(\langle \bar{y}_i \rangle)$ $G_1 = H_k$, $l_1 = a_k$, and $G_2 = \langle \bar{y}_i \rangle$

where $\pi : G \longrightarrow G/H_k$. ($G_2 \simeq H/H_k$ by the First Iso Theorem)

Lemma: Let H be an abelian group of order $|H| = p^\ell$. Let

$\ell_1 = \max\{s \mid \mathrm{ord}(\sigma) = p^s \text{ for some } \sigma \in H\}$

Assume that there exists $G_1 \trianglelefteq H$ with $G_1 \simeq \mathbb{Z}/p^{\ell_1}\mathbb{Z}$ such that

$G_2 := H/G_1 \simeq \mathbb{Z}/p^{\ell_2}\mathbb{Z}$ (in particular, $\ell_1 + \ell_2 = \ell$)

Let $y \in G_2$ be a generator of G_2. Then, we can find $\sigma_2 \in H$ such that

$y = \sigma_2 G_1$ and $\mathrm{ord}(\sigma_2) = \mathrm{ord}(y) = p^{\ell_2}$.

Proof: Let us choose $\sigma_1 \in G_1$ a generator of G_1. Pick $x \in H$ such that

$xG_1 = y \in H/G_1 \cong G_2$ is a generator of G_2.

Then, $p^{\ell_2} y = 0$ in G_2 implies $p^{\ell_2} x \in G_1 = \{j \cdot \sigma_1 : 0 \leq j \leq p^{\ell_1} - 1\}$

Writing the corresponding j in terms of p as $j = p^s m$ for some $0 \leq m$, $0 \leq s < \ell$,

with $(m,p) = 1$, we get $p^{\ell_2} x = p^s \boxed{m\sigma_1}$.

Key: H is a p-group & $p \nmid m$, so $m\sigma_1$ has order p^{ℓ_1} (same as σ_1).

$\Rightarrow \mathrm{ord}(p^{\ell_2} x) = p^{\ell_1 - s}$, so $\mathrm{ord}(x) = p^{\ell_1 + \ell_2 - s} = p^{\ell - s} \leq p^{\ell_1}$

because p^{ℓ_1} was the largest order of any element in H.

Thus, $s \geq \ell - \ell_1 = \ell_2$.

Conclusion: $p^{\ell_2} x = p^{s - \ell_2 + \ell_2} m\sigma_1 \Longrightarrow p^{\ell_2}(x - p^{s-\ell_2} m\sigma_1) = 0$ (*)

Take $\sigma_2 := x - p^{s-\ell_2} m\sigma_1$

Claim: $\mathrm{ord}(\sigma_2) = p^{\ell_2}$ and $y = \sigma_2 G_1$

Pf/ • $\sigma_2 G_1 = (x - \underbrace{p^{s-\ell_2} m\sigma_1}_{\in G_1}) G_1 = xG_1 = y$ ✓

• $\mathrm{ord}(\sigma_2) \leq p^{\ell_2}$ by (*)

• If $\mathrm{ord}(\sigma_2) < p^{\ell_2} \Rightarrow p^r \sigma_2 G_1 = p^r y = 0$ for some $r < \ell_2$, so

$\mathrm{ord}(y) \leq p^r < p^{\ell_2}$ Contra!

∎

This finishes the proof of existence from Lecture 20.

Proof of Uniqueness:

Assume we have a second decomposition, ie an isomorphism

$$\Psi : G \longrightarrow \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_\ell}\mathbb{Z} \qquad \text{with } b_1 \leq \cdots \leq b_\ell, \; b_1 + \cdots + b_\ell = n$$

Then: $b_\ell = \max\{ s : \operatorname{ord}(x) = p^s \text{ for } x \in \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_\ell}\mathbb{Z} \}$

- Since Ψ is an iso, order of elements are preserved. Thus, $\boxed{b_\ell = a_k}$
- Fix $\sigma \in G$ of order p^{a_k}. Then, $\Psi(\sigma)$ has order p^{b_ℓ}.

If $\Psi(\sigma) = (x_1, \ldots, x_\ell)$ the order condition forces $\operatorname{ord}(x_\ell) = p^{b_\ell}$ so x_ℓ generates $\mathbb{Z}/p^{b_\ell}\mathbb{Z}$.

$$\Rightarrow \underbrace{\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_{k-1}}\mathbb{Z}}_{\text{order } p^{n-a}} \simeq G/\langle\sigma\rangle$$

$$\begin{tikzcd}
G/\langle\sigma\rangle \arrow[r, "\overline{\Psi}", "\sim"'] & \left(\mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_\ell}\mathbb{Z}\right)/\langle\Psi(\sigma)\rangle \\
& \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_{\ell-1}}\mathbb{Z} \arrow[u, "\exists g"]
\end{tikzcd}$$

- $g = \pi_{\langle\Psi(\sigma)\rangle} \circ i$ where $i : \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_{\ell-1}}\mathbb{Z} \hookrightarrow \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_\ell}\mathbb{Z}$

$$(z_1, \ldots, z_{\ell-1}) \longmapsto (z_1, \ldots, z_{\ell-1}, 0)$$

Claim: g is an isomorphism

Pf/ g is a group homomorphism because it is a composition of group homomorphisms.
- The source and target groups of g have the same order, namely p^{n-a}.

So to prove g is an isomorphism, we need only show it is injective.

Pick $\underline{z} \in \operatorname{Ker}(g)$, so $\underline{z} = (z_1, \ldots z_{\ell-1})$ satisfies $(z_1, \ldots z_{\ell-1}, 0) \in \langle\Psi(\sigma)\rangle$

Since $\Psi(\sigma) = (x_1 \ldots x_\ell)$ has order p^{b_ℓ}, we can find $! c \in \{0, \ldots, p^{b_\ell - 1}\}$ st. $(z_1, \ldots, z_{\ell-1}, 0) = c(x_1, \ldots, x_\ell) = (cx_1, \ldots, cx_\ell)$

In particular, $0 = c x_\ell$. Since $\operatorname{ord}(x_\ell) = p^{b_\ell}$, we get $c = 0$

Thus $\underline{z} = 0$, as we wanted. $\square$

- Using the Claim we obtain 2 decompositions for the group $G/\langle\sigma\rangle$, which has order p^{n-a}

$$\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_{k-1}}\mathbb{Z} \overset{\pi}{\simeq} G/\langle\sigma\rangle \xrightarrow{g^{-1}\circ\overline{\Psi}} \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_{\ell-1}}\mathbb{Z}$$

By the inductive hypothesis, we get $k-1 = \ell-1$ & $a_1 = b_1$
$\vdots$
$a_{k-1} = b_{k-1}$

Since $a_k = b_\ell$, uniqueness has been proven. $\square$

Q: How to find the "structure constants" $a_1, \dots, a_k$ for abelian p-groups?

A: Given an abelian p-group G with $|G| = p^n$, we consider the group homomorphism.

$$\sigma: G \longrightarrow G$$
$$g \longmapsto p\cdot g = \underbrace{g + \cdots + g}_{p \text{ times}}$$

Theorem 3: $\underset{id}{\mathrm{Ker}(\sigma^0)} = \{e\} \subseteq \mathrm{Ker}(\sigma) \subseteq \mathrm{Ker}(\sigma^2) \subseteq \cdots \subseteq \mathrm{Ker}(\sigma^n) = G$

Then the values $a_1, \dots, a_k$ are obtained as the indices j when the size of the successive quotients $\mathrm{Ker}(\sigma^{j+1})/\mathrm{Ker}(\sigma^j)$ jump.

Proof: Prove this for $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$. In particular.

$$a_k = \min\{j : \mathrm{Ker}(\sigma^j) = G\}$$

Example: $G = \mathbb{Z}/8\mathbb{Z}$

$$\sigma: \mathbb{Z}/8\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z}$$
$$\bar{x} \longmapsto 2\cdot\bar{x}$$

$\mathrm{Ker}\,\sigma = 4\mathbb{Z}/8\mathbb{Z}$

$\mathrm{Ker}\,\sigma^2 = 2\mathbb{Z}/8\mathbb{Z}$

$\mathrm{Ker}\,\sigma^3 = \mathbb{Z}/8\mathbb{Z} = \mathrm{Ker}\,\sigma^4 = \cdots$

$\Rightarrow \dfrac{\mathrm{Ker}\,\sigma^2}{\mathrm{Ker}\,\sigma} = \dfrac{2\mathbb{Z}/8\mathbb{Z}}{4\mathbb{Z}/8\mathbb{Z}} \simeq 2\mathbb{Z}/4\mathbb{Z}$ by 3rd Iso Thm order $=2$

$\dfrac{\mathrm{Ker}\,\sigma^3}{\mathrm{Ker}\,\sigma^2} = \dfrac{\mathbb{Z}/8\mathbb{Z}}{2\mathbb{Z}/8\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}$ order 2 $\quad \dfrac{\mathrm{Ker}\,\sigma^4}{\mathrm{Ker}\,\sigma^3} = \dfrac{G}{G} = \{0\} \Rightarrow \boxed{a_1 = 3}$

<u>Remark:</u> A similar result works for finitely generated abelian group. The difference will be $G \simeq \mathbb{Z}^{\ell} \times G'$, where

- G' is a finite abelian group (the torsion of G), which can be decomposed further using Theorems 1 and 2 from §20.1 & §20.2.
- ℓ is uniquely determined ($\mathbb{Z}^{\ell}$ is the "torsion-free" part of G)

You will see a proof of this for more general structures, namely finitely generated modules over PIDs, in Algebra II (Math 5112 - 5991H)

§ 21.2 Classification of finite abelian groups:

Combining Theorems 1 & 2 from Lecture 20, we get a complete classification of finite abelian groups as direct product of cyclic p-groups for all p prime numbers dividing the order of the group. The powers $a^1_1, \ldots, a^1_{k_1}, a^2_1, \ldots, a^2_{k_2}, \ldots, a^s_1, \ldots, a^s_{k_s}$ with $n = p_1^{b_1} \cdots p_s^{b_s}$ $\quad a^i_1 \leq \cdots \leq a^i_{k_i}$ $\quad a^i_1 + \cdots + a^i_{k_i} = b_i$ $\quad \forall i = 1, \ldots, s$.

Here is an alternative decomposition of finite ab groups.

<u>Theorem 4:</u> Let G be a finite abelian group of order n. Then, there exists unique integers $d_1, \ldots, d_s$ with $d_1 | d_2, d_2 | d_3, \ldots, d_{s-1} | d_s$ such that

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

<u>Proof:</u> Consider the prime decomposition of n, ie $n = p_1^{a_1} \cdots p_k^{a_k}$ $\left(\begin{array}{l} p_i \text{ distinct primes} \\ a_i \geq 1 \ \forall i \end{array}\right)$

By Theorem 2 $G \simeq G_{p_1} \times \cdots \times G_{p_k}$ with $|G_{p_i}| = p_i^{a_i}$.

In turn, by Theorem 3, we write

$$\begin{array}{lll} G_{p_1} \cong \mathbb{Z}/p_1^{a^1_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{a^1_{s_1}}\mathbb{Z} & & a^1_1 \leq \cdots \leq a^1_{s_1} \\ G_{p_2} \simeq \mathbb{Z}/p_2^{a^2_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_2^{a^2_{s_2}}\mathbb{Z} & & a^2_1 \leq \cdots \leq a^2_{s_2} \\ \vdots \qquad\qquad \vdots & & \qquad\qquad (*) \\ G_{p_k} \simeq \mathbb{Z}/p_k^{a^k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a^k_{s_k}}\mathbb{Z} & & a^k_1 \leq \cdots \leq a^k_{s_k} \end{array}$$

After reordering the primes, we may assume $s_1 \geq \cdots \geq s_k$.

By completing will 0's at the beginning of each sequence, $a^i_1 \le \dots \le a^i_{s_i}$ (which will give $\mathbb{Z}/p_i^0\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{0\}$), we may assume $\boxed{s_1 = \dots = s_k}$ (ie we have the same number of summands for each G_{p_i}). Call this number s & keep the notation a^i_j.

We take the direct sum of the terms on each "column" of $(*)$ with this "extension by 0's". We get:

$$H_1 := \mathbb{Z}/p_1^{a^1_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{a^k_1}\mathbb{Z}$$

$$\vdots$$

$$H_s := \mathbb{Z}/p_1^{a^1_s}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{a^k_s}\mathbb{Z}$$

Define $d_i = \prod_{j=1}^{s} p_j^{a^j_i}$. Since $a^j_i \le a^j_{i+1}$ $\forall j$ we get $d_i \mid d_{i+1}$.

<u>Claim:</u> $H_i \simeq \mathbb{Z}/d_i\mathbb{Z}$ $\forall i$

Pf/ $\mathbb{Z}/d_i\mathbb{Z}$ is cyclic, so its Sylow p-subgroups are also cyclic. Their sizes are $p_j^{a^j_i}$ if $p_j \mid d_i$. Theorem 2 shows $\mathbb{Z}/d_i\mathbb{Z} \simeq \prod_{\substack{1\le j\le k \\ a^j_i \ge 1}} \mathbb{Z}/p_j^{a^j_i}$

Completing the (RHS) with 0's gives the isomorphism claimed above. □

Since $G \simeq H_1 \times \dots \times H_s$ by mere regrouping of the $\mathbb{Z}/p_i^{a^i_j}\mathbb{Z}$ factors, the claim establishes the existence of the decomposition.

For the uniqueness, it suffices to undo the process. Namely, decompose each $\mathbb{Z}/d_i\mathbb{Z}$ Theorem 2 and notice that since $\mathbb{Z}/d_i\mathbb{Z}$ is cyclic all its subgroups are also cyclic. In particular, it's Sylow p-subgroups are cyclic as well.

From this calculation, we can recover the original structure constants $a^1_1, \dots, a^k_s$ since the divisibility condition ensures that $a^i_j \le a^i_{j+1}$ $\forall i$ $\forall j$

The uniqueness of the structure constants ensures that the d_i's are unique as well. □

Example 1: Decompose $G = \mathbb{Z}/300\mathbb{Z}$

Solution: Write $300 = 2^2\cdot 3\cdot 5^2$

$$\Rightarrow \quad G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$

(subgroups of a cyclic group are cyclic, so Sylow p-subgroups of G are cyclic)

$$\begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \hookrightarrow & \mathbb{Z}/300\mathbb{Z} \\ \bar{1} & \longmapsto & \overline{75} \end{array} \quad , \quad \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} & \hookrightarrow & \mathbb{Z}/300\mathbb{Z} \\ \bar{1} & \longmapsto & \overline{100} \end{array} \quad , \quad \begin{array}{ccc} \mathbb{Z}/5\mathbb{Z} & \hookrightarrow & \mathbb{Z}/300\mathbb{Z} \\ \bar{1} & \longmapsto & \overline{60} \end{array}$$

Example: Decompose $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/144\mathbb{Z}$

Solution: Note $3 \mid 48$ & $48 \mid 144$.

$$3 = 3 \quad \rightsquigarrow \quad \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}$$

$\cdot 16$

$$48 = 2^4\cdot 3 \quad \rightsquigarrow \quad \mathbb{Z}/48\mathbb{Z} \simeq \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$\cdot 3$

$$144 = 2^4\cdot 3^2 \quad \rightsquigarrow \quad \mathbb{Z}/144\mathbb{Z} \simeq \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}$$

$$\rightsquigarrow \quad G \simeq \underbrace{\mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/2^4\mathbb{Z}}_{\text{Sylow 2-subgroup of } G} \times \underbrace{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z}}_{= \text{ Sylow 3-subgroup of } G}$$

Conversely, starting from the (RHS), we recover the original iso by regrouping by columns, after adding 0's. We get $4 \le 4$ for $p=2$, $1 \le 1 \le 2$ for $p=3$, so $s=3$

and

$$\underbrace{\boxed{\begin{array}{c} 0 \\ \mathbb{Z}/3\mathbb{Z} \end{array}}}_{= H_1} \begin{array}{c} \times \\ \times \end{array} \underbrace{\boxed{\begin{array}{c} \mathbb{Z}/2^4\mathbb{Z} \\ \mathbb{Z}/3\mathbb{Z} \end{array}}}_{= H_2} \begin{array}{c} \times \\ \times \end{array} \underbrace{\boxed{\begin{array}{c} \mathbb{Z}/2^4\mathbb{Z} \\ \mathbb{Z}/3^2\mathbb{Z} \end{array}}}_{= H_3}$$

$H_1 = \mathbb{Z}/3\mathbb{Z}$

$$H_2 = \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/48\mathbb{Z}$$
$$(\bar{3}, \underbrace{\overline{16}}_{=\bar{1}}) \longleftarrow \bar{1}$$

$$H_3 = \mathbb{Z}/2^4\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \simeq \mathbb{Z}/144\mathbb{Z}$$
$$(\bar{9}, \underbrace{\overline{16}}_{=\bar{7}}) \longleftarrow \bar{1}$$