Lecture XX: Classification of finite abelian groups I

§20.1 Classification of finite abelian groups:

Last time, we took the first step to classify finite abelian groups:

Theorem 1: Let G be a finite abelian group. If $|G| = n$ is written into its prime factors $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ (p_i all distinct primes, $a_i \in \mathbb{Z}$ $\forall i$) then $\exists$ $P_i \trianglelefteq G$ of order $p_i^{a_i}$ such that $G \simeq P_1 \times \cdots \times P_k$.
Furthermore, this decomposition is unique.

(G is the direct product of its Sylow p-subgroups: $P_1 \times \cdots \times P_k \longrightarrow P_1 \cdots P_k = G$)
$(n_1, \ldots, n_k) \longmapsto n_1 \cdots n_k$

Definition G is the direct product of subgroups $H_1, \ldots H_k$ if

(0) $H_i \trianglelefteq G$ $\forall i = 1, \ldots, k$

(1) G is generated by $H_1 \cup \cdots \cup H_k$

(2) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) = \{e\}$ $\forall i = 1, \ldots, k$

Key: (2) & $H_i \trianglelefteq G$ so $ab = ba$ $\forall a \in H_i$, $b \in H_j$ $i \neq j$. In particular words in $H_1 \cup \cdots \cup H_k$ can be expressed as $a_1 \cdots a_k$ with $a_i \in H_i$.

Remark: The same proof will work if G is not abelian but every Sylow p-subgroup of G is normal $\forall p$ (ie $n_p = 1$ $\forall p$ dividing $|G|$). Nilpotent groups (to be defined in a future lecture) will have this property.

To finish our classification, we need to classify abelian p-groups (ie $P_1, \ldots P_k$ in Thm 1)

§20.1 Classification of finite abelian p-groups:

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

Remark 1: For notational convenience, we think of $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$ as additive,

ie $\underline{0} = (0, \ldots, 0)$ is the neutral element

$\underline{x} + \underline{y}$ coordinatewise is the group operation

$m \cdot \underline{x} = \underbrace{\underline{x} + \cdots + \underline{x}}_{m \text{ times}}$ for $m \in \mathbb{Z}_{\geq 1}$.

<u>Remark 2</u>: Say $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$. What are the properties of $a_1, \dots, a_k$?

Note $\operatorname{ord}(g) \leq p^{a_k}$ for all $g \in G$ because $a_1 \leq \dots \leq a_k$ and

$c(g_1, \dots, g_k) = (cg_1, \dots, cg_k)$ so $\bullet\, cg_1 = 0 \Rightarrow c = p^{l_1}$ with $0 \leq l_1 \leq a_1$

$\vdots$

$\bullet\, cg_k = 0 \Rightarrow c = p^{l_k}$ with $0 \leq l_k \leq a_k$

Furthermore: $g = (0, \dots, 0, 1)$ has order p^{a_k}.

In particular, we know the value of a_k if $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_k}\mathbb{Z}$ because isomorphisms preserve the order of elements.

<u>Proof</u>: We prove the statement (existence & uniqueness) by complete induction on n.

<u>Base case</u>: $n = 1$ is trivial $|G| = p \Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$ because it is cyclic of order p.

In particular $k = a_1 = 1$ are unique.

<u>Inductive Step</u>: We assume the statement is true for any abelian p-group of order p^m with $m < n$.

- Let $a := \max\{ s$ such that $\operatorname{ord}(\sigma) = p^s$ for some $\sigma \in G\}$ (ie p^a is the largest order of an element of G)

Note that $a \geq 1$ because $G \neq \{e\}$ so $\exists\, g \in G$ with $\operatorname{ord}(g) \neq 1$

Fix $\sigma \in G$ with $\operatorname{ord}(\sigma) = p^a$. Let $H = \langle \sigma \rangle \simeq \mathbb{Z}/p^a\mathbb{Z}$

Since G is abelian $H \trianglelefteq G$ & $\left| G/H \right| = p^{n-a}$ with $n - a < n$.

- <u>If $a = n$</u>, we have $G \simeq \mathbb{Z}/p^a\mathbb{Z}$ with $k = 1$ and $a_1 = n$.
  Uniqueness follows because $a_k = \max\{ s : \operatorname{ord}(\sigma) = p^s$ for $\sigma \in \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_k}\mathbb{Z}\}$ because $a_1 \leq \dots \leq a_k$. This forces $a_k = a = n$ thus $k = 1$.
- <u>If $a < n$</u>, by inductive hypothesis applied to G/H we have $G/H \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_{k-1}}\mathbb{Z}$ for $k-1 \geq 1$, $1 \leq a_1 \leq \dots \leq a_{k-1}$ with $a_1 + \dots + a_{k-1} = n - a$.
  In particular, we can find $\bar{y}_1, \dots, \bar{y}_{k-1} \in G/H$ of orders $p^{a_1}, \dots, p^{a_{k-1}}$ respectively such that $\bullet\, \{\bar{y}_1, \dots, \bar{y}_{k-1}\}$ generates G/H

  $\bullet\, \langle \bar{y}_i \rangle \cap \langle \bar{y}_j : j \neq i \rangle = \{e\}$ $\forall i \neq j$ $1 \leq i, j \leq k-1$.

⚠ We would like to have a way to recover G from H and G/H. However, for general groups G, we don't have $G \simeq H \times G/H$ (we don't have a normal subgroup $N \trianglelefteq G$ with $N \simeq G/H$)

However, we can in general lift $\bar{y}_i \in G/H$ to some $\sigma_i \in \pi^{-1}(\bar{y}_i)$ with $\pi(\sigma_i) = \sigma_i H = \bar{y}_i$ for $i = 1, \dots, k-1$. In particular $\mathrm{ord}(\bar{y}_i) = p^{a_i} = \mathrm{ord}(\sigma_i H)$

⚠ $\mathrm{ord}(\bar{y}_i) = p^{a_i} \Rightarrow (\sigma_i)^{p^{a_i}} \in H$, but not necessarily $(\sigma_i)^{p^{a_i}} = 1$.

The next claim ensures <u>some</u> $\sigma_i \in \pi^{-1}(\bar{y}_i)$ will have the right order.

<u>Claim 1:</u> For every $i = 1, \dots, k-1$, we can find $\sigma_i \in G$ such that $\bar{y}_i = \sigma_i H$ $\forall i$

$\mathrm{ord}(\sigma_i) = p^{a_i}$ (in G)

Assuming the claim, we finish proving the result. We'll discuss the proof next time.

Set $\sigma_k := \sigma$ & $a_k := a$.

Set $H_i := \langle \sigma_i \rangle$ $\forall i = 1, \dots, k$. We have

- $H_i \trianglelefteq G$ (because G is abelian)
- $H_i \simeq \mathbb{Z}/p^{a_i}\mathbb{Z}$ since $\mathrm{ord}(\sigma_i) = p^{a_i}$

<u>Claim 2:</u> $H_1 \cdots H_k$ satisfy conditions (1) and (2) of Proposition §19.2

Pf/. (1) holds because $\sigma_1, \dots, \sigma_k$ generate G This is a consequence of a general fact "given G group and $H \trianglelefteq G$, then the union of a generating set of H and any lifts of a generating set of G/H under $\pi : G \twoheadrightarrow G/H$ generates G")

- We need to show (2) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) = \{e\}$ $\forall i = 1, \dots k$.

We start by proving the statement for $\boxed{i=k}$. Note that:

$$\begin{array}{ccc} H_1 \cdots H_{k-1} & \trianglelefteq & G \\ \downarrow & & \downarrow \pi \text{ natural projection} \\ \pi(H_1 \cdots H_{k-1}) & \subseteq & G/H_k \end{array}$$

$\pi(H_1 \cdots H_{k-1}) = \langle y_1 \rangle \cdots \langle y_{k-1} \rangle$ has size p^{n-a}, same as $|G/H_k|$.

so $\pi|_{H_1 \cdots H_{k-1}} : H_1 \cdots H_{k-1} \twoheadrightarrow G/H_k$

Since $|H_1 \cdots H_{k-1}| \leq |H_1| \cdots |H_{k-1}| = p^{a_1} \cdots p^{a_{k-1}} = p^{a_1+\cdots+a_{k-1}} = p^{n-a} = |G/H_k|$
we conclude it is an isomorphism by the 1st Isomorphism Theorem.

Thus: $\underset{H_k}{\overset{\|}{\ker \pi}} \cap H_1 \cdots H_{k-1} = \{e\}$

- Next, we discuss $\boxed{i = 1, \ldots, k-1}$.

Note $\Psi : H_1 \times \cdots \times H_{k-1} \xrightarrow{\simeq} G/H_k$
$(\sigma_1^{b_1}, \ldots, \sigma_{k-1}^{b_{k-1}}) \longmapsto (\bar{y}_1^{b_1} \cdots \bar{y}_{k-1}^{b_{k-1}})$

If $x \in H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_k$

$\operatorname{ord}(\sigma_j) = p_j^{a_j}$

then $x = x_i = x_1 \cdots x_{i-1} x_{i+1} \cdots x_k$ with $x_j = \sigma_j^{b_j} \in H_j$ $\forall j$ for some $0 \leq b_j < a_j$

$\Rightarrow x_i H_k = x_1 H_k \, x_2 H_k \cdots x_{i-1} H_k \, x_{i+1} H_k \cdots x_{k-1} H_k$ yields
$\bar{y}_i^{b_i} = \bar{y}_1^{b_1} \cdot \bar{y}_1^{b_2} \cdots \bar{y}_{i-1}^{b_{i-1}} \cdot \bar{y}_{i+1}^{b_{i+1}} \cdots \bar{y}_{k-1}^{b_{k-1}} \in G/H_k$.

$\Rightarrow \bar{y}_1^{b_1} \cdots \bar{y}_{i-1}^{b_{i-1}} \bar{y}_i^{-b_i} \bar{y}_{i+1}^{b_{i+1}} \cdots \bar{y}_{k-1}^{b_{k-1}} = \bar{e} \in G/H_k$.

Since Ψ is an isomorphism, we conclude $b_1 = \cdots = b_{i-1} = -b_i = b_{i+1} = \cdots = b_{k-1} = 0$
Thus $x = x_i = \sigma_i^{b_i} = e$, as we wanted to show. $\square$

- Combining Claim 2 and Proposition §19.1, we get $G \simeq H_1 \times \cdots \times H_k$, so the decomposition exists.

It remains to prove Claim 1 & show uniqueness. We will do this next time.