Structure Theory for finite abelian groups.

Let M be a finite abelian gp.

What is the structure of M?

M is a finite direct sum of finite cyclic groups of prime power order

Ex:

$$(\mathbb{Z}/2\mathbb{Z})^5 \oplus \left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^0 \oplus \left(\frac{\mathbb{Z}}{2^3\mathbb{Z}}\right)^3 \oplus$$

$$(\mathbb{Z}/3\mathbb{Z})^0 \oplus (\mathbb{Z}/3^2\mathbb{Z})^5 \oplus$$

$$(\mathbb{Z}/23\mathbb{Z})^{15} \oplus \left(\frac{\mathbb{Z}}{41\mathbb{Z}}\right)^{2021}$$

.

$p_1 = 2$ $\quad (\mathbb{Z}/p_1\mathbb{Z})^{\boxed{\ }} \oplus (\mathbb{Z}/p_1^2\mathbb{Z})^{\boxed{\ }} \cdots \oplus \left(\frac{\mathbb{Z}}{p_1^{k_1}\mathbb{Z}}\right)^{\boxed{\ }}$

$p_2 = 3$

$\vdots$

$$(\mathbb{Z}/2^3\mathbb{Z})^3 \oplus \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^5$$

$$\oplus (\mathbb{Z}/3^2\mathbb{Z})^5$$

$$\oplus \left(\frac{\mathbb{Z}}{23\mathbb{Z}}\right)^{15}$$

$$\oplus \left(\frac{\mathbb{Z}}{41\mathbb{Z}}\right)^{2021}$$

$$\underbrace{\left(\mathbb{Z}/41\mathbb{Z}\right) \oplus \cdots}_{}\quad (2021) \text{ times}$$

$$\underbrace{\left(\mathbb{Z}/23\mathbb{Z}\right) \oplus \cdots}_{15 \text{ times}}$$

$$\vdots$$

$$\underbrace{\left(\mathbb{Z}/3^2\mathbb{Z}\right) \oplus \cdots}_{5 \text{ times}}$$

$$\mathbb{Z}/2^3\mathbb{Z} \oplus \frac{\mathbb{Z}}{2^3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2^3\mathbb{Z}} \oplus \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots}_{5 \text{ times}}$$

$\underline{41 \cdot 23 \cdot 3^2 \cdot 2^3}$ repeats 3 times

$41 \cdot 23 \cdot 3^2 \cdot 2$ repeats 2 times

$41 \cdot 23 \cdot 2$ repeats 3 times

$41 \cdot 23$ repeats 7 times

41 repeats 2006 times

direct sum of 2021 cyclic gps.

$$\left[\frac{\mathbb{Z}}{(41\cdot 23\cdot 3^2\, 2^3)\mathbb{Z}}\right]^{\oplus 3} \oplus \left(\frac{\mathbb{Z}}{41\cdot 23\cdot 3^2\cdot 2\,\mathbb{Z}}\right)^{\oplus 2} \oplus$$

$$\left(\frac{\mathbb{Z}}{41\cdot 23\cdot 2\,\mathbb{Z}}\right)^{\oplus 3} \oplus \left(\frac{\mathbb{Z}}{41\cdot 23}\right)^{\oplus 7} \oplus \left(\frac{\mathbb{Z}}{41\mathbb{Z}}\right)^{2006}$$

Thm: Given a finite abelian gp M, $\exists$ positive integers $d_1, d_2, \ldots, d_k \geq 2$ s/t

$d_k \mid d_{k-1} \mid d_{k-2} \mid \cdots \mid d_1$ &

$$M = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{d_2\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_k\mathbb{Z}}.$$

Moreover these $d_1, \ldots, d_k$ are unique.

In the above example, $k=2021$

$$\underbrace{d_1 \mid \cdots \mid d_{2006}}_{41} \mid \underset{41\cdot 23}{\underset{\shortparallel}{d_{2007}}} \mid \cdots \mid \underbrace{d_{2013}}_{41\cdot 23} \mid$$

$$\underbrace{d_{2014} = d_{2015} = d_{2016}}_{41\cdot 23\cdot 2} \mid \underbrace{d_{2017} = d_{2018}}_{41\cdot 23\cdot 3^2\cdot 2} \mid$$

$$\underbrace{d_{2019} = d_{2020} = d_{2021}}_{41\cdot 23\cdot 3^2\cdot 2^3}$$

$$\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Chinese Remainder Theorem

$\Downarrow$ Primary Decomposition.

$$M = \bigoplus p_i(M)$$

p_i prime; $p_i \in \{2, 3, 5, 7, \dots\}$

finite sum

Let d be s/t $dM = 0$. Write $d = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

$$\mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{r_k}\mathbb{Z}$$

$\Downarrow$

$e_1, \dots, e_k$; $e_i^2 = e_i \quad e_i e_j = 0$

$1 = e_1 + e_2 + \dots + e_k$

$p_i(M) = e_i M.$ = Sylow p_i-subgp of M

The structure of $\underbrace{p_i(M)}$.

Module over $\dfrac{\mathbb{Z}}{p_i^{r_i}\mathbb{Z}}$

What is the structure of a finite $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$-module? $\boxed{p_i = p}$ $\boxed{r_i = r}$

$\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ ⊕

$\mathbb{Z}/p_i\mathbb{Z}$, $\dfrac{\mathbb{Z}}{p_i^2\mathbb{Z}}$, ...,

$\mathbb{Z}/p\mathbb{Z}$, $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$, ..., $\dfrac{\mathbb{Z}}{p^r\mathbb{Z}}$.

$(\mathbb{Z}/p\mathbb{Z})^{l_1} \oplus \left(\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^{l_2} \oplus \cdots \oplus \left(\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^{l_r}$

Claim: Isomorphism classes of finite $\frac{\mathbb{Z}}{p^r\mathbb{Z}}$-modules are indexed by tuples $(\underbrace{l_1, \ldots, l_r})$ of non-negative integers.

Given a finite $\frac{\mathbb{Z}}{p^r\mathbb{Z}}$-module M, how do we get $l_1, \ldots, l_r$?

$p = 5$ $\quad \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^3 \oplus \left(\frac{\mathbb{Z}}{5^2\mathbb{Z}}\right)^2 = M$

$5^2 M = 0$

$\cap\!\mid$

$5M$

$\cap\!\mid$

M

$M/5M$

$5M/5^2M$

~~Modules~~ vector spaces over $\frac{\mathbb{Z}}{5\mathbb{Z}} = k$

$\dim_k \underbrace{\frac{M}{5M}}$ $= 5$ $\dim_k \frac{5M}{5^2M} = 2$

5

$l_1 + \dots + l_r, \dots, l_r + l_{r-1}, l_r$

$\dim \frac{M}{pM}$ $\dim \frac{pM}{p^2M}$ $= \dim \frac{p^{r-1}M}{p^rM}$

$$\dim \frac{p^{i-1}M}{p^iM} \leq \dim \frac{p^{i-2}M}{p^{i-1}M}$$

Why?

Proof: Suppose $m_1, \dots, m_s \in M$ are s/t $p^{i-1}m_1, \dots, p^{i-1}m_s \in p^{i-1}M/p^iM$ form a $\frac{\mathbb{Z}}{p\mathbb{Z}}$-basis of $p^{i-1}M/p^iM$.

Then $p^{i-2}m_1, \dots, p^{i-2}m_s \in p^{i-2}M/p^{i-1}M$ are l.i. (claim) Pf of claim:

Suppose $\lambda_1 p^{i-2}m_1 + \dots + \lambda_s p^{i-2}m_s = 0$

Multiply by p to get ~~@~~the following:

$$\lambda_1 p^{i-1} m_1 + \dots + \lambda_s p^{i-1} m_s = 0 \in \frac{p^{i-1}M}{p^{i}M}$$

$$\frac{p^{i-2}M}{p^{i-1}M} \xrightarrow[\text{by } p]{\text{multiply}} \frac{p^{i-1}M}{p^{i}M} \qquad \mathbb{Z}/p\mathbb{Z}\text{-linear}$$

onto

$$\begin{array}{ccccccc}
\dim \frac{M}{pM} & & \dim \frac{pM}{p^2M} & & \dots & & \dim \frac{p^{r-1}M}{p^{r}M} \\
\| & & \| & & & & \| \\
q_1 & \geq & q_2 & \geq & \dots & \geq & q_r \\
 & & & & \| & & \| \\
 & & & & l_{r-1}+l_r & & l_r
\end{array}$$

$$\begin{aligned}
\text{Set } l_{r-1} &:= q_{r-1} - q_r \\
l_{r-2} &:= q_{r-2} - q_{r-1} \\
&\vdots \\
l_1 &:= q_1 - q_2
\end{aligned}$$

Given M, we have produced

$l_1, \ldots, l_r$.

$$l_i := \dim \frac{p^{i-1}M}{p^iM} - \dim \frac{p^iM}{p^{i+1}M}$$

$$M \overset{?}{\cong} \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{l_1} \oplus \cdots \oplus \left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^{l_r}$$

$$l_r = \dim \frac{p^{r-1}M}{p^rM} - \cancel{\dim \frac{p^rM}{p^{r+1}M}} = 0$$

$m_1, \ldots, m_{l_r}$ s/t $p^{r-1}m_1, \ldots, p^{r-1}m_{l_r}$ are a basis of $p^{r-1}M/p^rM$

$$\left(\frac{\mathbb{Z}}{p^r M}\right)^{l_r} \longrightarrow M$$

$$e_1, \ldots, e_{l_r} \longmapsto m_1, \ldots, m_{l_r}$$

$$m_{l_r+1}, \ldots, m_{l_r+l_{r-1}} \qquad \left(\frac{\mathbb{Z}}{p^{r-1}\mathbb{Z}}\right)^{l_{r-1}}$$

s/t $p^{r-2} m_{l_r+1}, \ldots, p^{r-2} m_{l_r+l_{r-1}},$

$p^{r-2} m_{l_r}, \ldots, p^{r-2} m_1$

form a basis for $\dfrac{p^{r-2}M}{p^{r-1}M}$

Can further arrange s/t $p^{r-1} m_{l_r+l_{r-1}} = 0$

$p^{r-1} m_{l_r+1}, \ldots,$

$$M \xleftarrow{\varphi} N = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{l_1} \oplus \cdots \oplus \left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^{l_r}$$

$$\frac{M}{pM} \xleftarrow{\bar{\varphi}} \frac{N}{pN}, \quad \frac{pM}{p^2M} \xleftarrow{\sim} \frac{pN}{p^2N}, \quad \cdots$$

$$\cdots \frac{p^{i-1}M}{p^iM} \xleftarrow{\varphi} \frac{p^{i-1}N}{p^iN}, \quad \cdots$$