Finite Abelian gps.

Theorem (Naive version) Every finite abelian group is a finite direct ~~product~~ sum of finite cyclic groups.

Cyclic groups $\mathbb{Z}/n\mathbb{Z}$

Direct sum $\mathbb{Z}/n_1\mathbb{Z} \oplus \dfrac{\mathbb{Z}}{n_2\mathbb{Z}}$

$$\underset{\text{finite abelian gp}}{M} \simeq \frac{\mathbb{Z}}{n_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_k\mathbb{Z}}.$$

Cancellation problem: Suppose N, M, and M' are finite abelian groups. Suppose further that

$N \oplus M \simeq N \oplus M'$. Then $M \simeq M'$.

True or false?

Upshot: This problem reduces to the case when N is cyclic.

Assume N is a finite direct sum of finite cyclic gps.

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_k\mathbb{Z}} \oplus M$$

$$\wr$$

$$\frac{\mathbb{Z}}{n_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{n_k\mathbb{Z}} \oplus M'$$

Chinese Remainder Thm.

A comm. ring with 1.

$\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pairwise comaximal ideals

Then $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

$$\frac{A}{\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n} = \frac{A}{\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n} \simeq \frac{A}{\mathfrak{a}_1} \times \frac{A}{\mathfrak{a}_2} \times \dots \times \frac{A}{\mathfrak{a}_n}$$

Given a finite abelian grp M,

$\exists$ $d > 0$ integer s/t $dM = 0$.

Thus M is a $\frac{\mathbb{Z}}{d\mathbb{Z}}$-module

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

$$d = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

$(a, b) = 1$ Euclid's division algorithm

gcd is 1

$\mathbb{C}[x, y]$ x, y

If the gcd of a & b is 1

then $\exists\, x, y \in \mathbb{Z}$ s/t $xa + yb = 1$

M finite abelian gp; $dM = 0$

$$\mathbb{Z}/p_1^{r_1}\mathbb{Z} \times 0 \times \cdots \times 0 = S_1$$

$$\vdots$$

$$0 \times \cdots \times 0 \times \frac{\mathbb{Z}}{p_k^{r_k}\mathbb{Z}} = S_k$$

$$\frac{\mathbb{Z}}{d\mathbb{Z}} = S_1 \oplus \cdots \oplus S_k$$

$$e_1 \longleftrightarrow (1, 0, \ldots, 0)$$

$$\vdots$$

$$e_k \longleftrightarrow (0, 0, \ldots, 0, 1)$$

$e_1^2 = e_1, \ldots, \quad e_k^2 = e_k$

$e_i e_j = 0 \quad \forall\ i \neq j \qquad 1 = e_1 + e_2 + \cdots + e_k$

$$M = \underbrace{e_1 M}_{\substack{\cong \\ \mathbb{Z}/p_1^{r_1}\mathbb{Z}\text{-module}}} \oplus \cdots \oplus \underbrace{e_k M}_{\substack{\cong \\ \mathbb{Z}/p_k^{r_k}\mathbb{Z}\text{-module}}}$$

$e_1 M, \ldots, e_k M$ are called the primary components of M.

$e_i M$ is the p_i-primary component of M.

Primary Decomposition Theorem

Noetherian Module: $(0 :_M p) \subseteq (0 :_M p^2)$

Fix a prime p.

$$(0 :_M a) = \{m \in M \mid am = 0\}$$

$(0:_M p) \subseteq (0:_M p^2) \subseteq (0:_M p^3) \subseteq \cdots$ stabilises

Ex: The stable value of this is precisely p-primary component of M.

M has a non-trivial p-primary component iff $p = p_1$, or, $\ldots$, $p = p_k$.

Ex: The p-primary component of M is precisely The p-Sylow subgp of M.

Theorem (Structure of finite nilpotent gps) Any finite nilpotent gp is the direct product of its Sylow p-subgps.

For a finite abelian gp the primary decomposition is precisely the above decomposition.

Let us denote the p-primary component of M by $p(M)$.

~~Then~~ $p_1(M) = e_1 M$

$(1, 0, \ldots, 0)$

d is s/t $dM = 0$

M finite ab. gp,

$d = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

$$M = \underbrace{p_1(M)}_{\mathbb{Z}/p_1^{r_1}\mathbb{Z}} \oplus \cdots \oplus p_k(M)$$

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

p prime & $r \geq 1$

<u>Thm</u>: Given a finite $\dfrac{\mathbb{Z}}{p^r\mathbb{Z}}$ - module M.

$\exists$ non-negative integers $t_1, \dots, t_r$ s/t

$$M \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{t_1} \oplus \left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^{t_2} \oplus \dots \oplus \left(\frac{\mathbb{Z}}{p^r\mathbb{Z}}\right)^{t_r}$$

Moreover, M is uniquely determined (up to isomorphism) by $t_1, \dots, t_r$

<u>**Thm:**</u> (Finer than the naive version)
Every finite abelian gp is a finite direct sum of finite cyclic gps of prime power orders.

Proof of CRT:

$\mathfrak{a}_1, \dots, \mathfrak{a}_n$ are pairwise comaximal

To show: $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n$

Proof: $\supseteq$ ✓ always

$\subseteq$ ✓ induction on n.

$n = 2$ $\quad \mathfrak{a}_1 \cap \mathfrak{a}_2 \overset{?}{\subseteq} \mathfrak{a}_1 \mathfrak{a}_2$

$1 = a_1 + a_2 \qquad \underset{\in \mathfrak{a}_1 \cap \mathfrak{a}_2}{x} = \underset{\in \mathfrak{a}_1 \mathfrak{a}_2}{x a_1} + \overset{\in \mathfrak{a}_1 \mathfrak{a}_2}{x a_2}$

For the induction step: ~~$\mathfrak{a}$~~

$$\mathfrak{m}_1 \cap \underbrace{\mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n}_{\parallel \text{ by i.h.}} \overset{?}{=} \mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_n$$

$$\underline{\mathfrak{m}_1} \cap \underline{\mathfrak{m}_2 \cdots \mathfrak{m}_n} = $$

$n=2$ case

provided $\mathfrak{m}_1$ & $\mathfrak{m}_2 \cdots \mathfrak{m}_n$ are comaximal

$1 = a_{12} + a_2 \qquad a_j \in \mathfrak{m}_j$ for $j \geq 2$

$1 = a_{13} + a_3$

$\vdots$

$1 = a_{1n} + a_n$

$$1 = \underbrace{(a_{12} + a_2) \cdots (a_{1n} + a_n)}$$

$$1 \in \mathfrak{m}_1 + \underbrace{a_2 \cdots a_n}_{\in \mathfrak{m}_2 \cdots \mathfrak{m}_n}$$

$a_{12}, a_{13}, \ldots, a_{1n} \in \mathfrak{m}_1$

$$\frac{A}{\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n} = \frac{A}{\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n} \simeq \frac{A}{\mathfrak{a}_1}\times\cdots\times\frac{A}{\mathfrak{a}_n}$$

$$\mathfrak{a}_i \supseteq \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n \quad \forall\ 1\le i\le n$$

$$A/\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n \xrightarrow{\pi_i} A/\mathfrak{a}_i$$

$$\frac{A}{\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n} \xrightarrow{\pi_1\times\cdots\times\pi_n} \frac{A}{\mathfrak{a}_1}\times\cdots\times\frac{A}{\mathfrak{a}_n}$$

Injection: ✓

Surjection: $e_1 = (1, 0, \dots 0)$, $e_2 = (0, 1, 0 \dots, 0)$ } belong to the img etc.

$b_1 \mapsto e_1, \ldots, b_n \mapsto e_n$

$$(a_1, \ldots, a_n)$$

$$a_1 b_1 + \cdots + a_n b_n \mapsto a_1 e_1 + \cdots + a_n e_n$$

~~How~~ What is b_1?

$\mathfrak{a}_1$ ~~and~~ $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal

$$\underset{\mathfrak{a}_1}{a} + b = 1$$

$b \equiv 0 \mod \mathfrak{a}_j \quad \forall j \geq 2$

Choose b_1

~~Q~~ ED

$\mathbb{Z}/d\mathbb{Z}$ $\quad M$ $\quad dM = 0$

finite ab gp $\quad d = p_1^{r_1} \cdots p_k^{r_k}$