Finite Abelian Groups: their structure

Abelian groups are precisely $\mathbb{Z}$-modules

$\mathbb{Z}$:= ring of integers.

given an abelian gp M

$m \in M$ $\quad n \in \mathbb{Z}$

$nm = ?$ $\quad \underbrace{m + \cdots + m}_{n \text{ times}}$

if $n \geq 0$

If $n < 0$, then $nm = \underbrace{(-m) + \cdots + (-m)}_{|n| \text{ times}}$

where $-m$ is s/t $m + (-m) = 0$

ring A, with 1

A-module M

M abelian gp.

$A \times M \to M$

$(a, m) \mapsto am$

$(a + a')m = am + a'm$

$a(m + m') = am + am'$

$1 . m = m$

Notion of a finitely generated Module (over a commutative ring, say)

A-module M is f.g if $\exists\, m_1, \ldots, m_n$ finitely many elements of M s/t

$Am_1 + \cdots + Am_n = M$

Given any $m \in M$ we can choose $a_1, \dots, a_n \in A$ s/t

$$m = a_1 m_1 + \dots + a_n m_n.$$

<u>Ex:</u> $\mathbb{Q}$ is <u>not</u> f.g. as a $\mathbb{Z}$-module

Structure Theory of f.g. module over a $\underbrace{\text{PID}}_{\text{principal ideal domain}}$ (e.g. $\mathbb{Z}$)

Ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \geq 0$.

Finite $\mathbb{Z}$-modules. Finite abelian gps.

Finite abelian group: abelian group whose underlying set is finite

Finite abelian gps: Abelian gps whose underlying set is finite.

Examples: $\mathbb{Z}/n\mathbb{Z}$ Cyclic gp of order n
$(\mathbb{Z}_n)$

$$|\mathbb{Z}/n\mathbb{Z}| = n$$

Construction: If M & M' are finite abelian gp, so is $M \oplus M' \simeq M \times M'$

$$(m, m') + (m_1, m_1') = (m + m_1, m' + m_1')$$

A naive of the STRUCTURE Theorem: Every finite abelian gp is a direct sum of finitely many cyclic groups.

Given M (finite abelian gp)

$\exists$ integers $m_1, \dots, m_k \geq 2$

s/t $M \simeq \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{m_k\mathbb{Z}}$

Are $m_1, \dots, m_k$ unique? No!

$$\mathbb{Z}/6\mathbb{Z} \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$$

Some basic facts about finite abelian gps.

- given an element $m \in M$ (finite ab gp), $\exists$ non-zero positive integer $a \in \mathbb{Z}$ s/t

$$am = 0 \qquad \left[\begin{array}{l} m \\ 2m = m+m \\ 3m = m+m+m \\ \vdots \end{array}\right]$$

$$km = jm \text{ for } j > k$$

$$\underbrace{(j-k)}_{= a} m = 0$$

- $\exists$ non-zero positive integer $b \in \mathbb{Z}$ s/t $bM = 0$. $M = \{m_1, \dots, m_n\}$

Choose $a_1, \dots, a_n$ positive integers s/t

$$a_1 m_1 = a_2 m_2 = \dots = a_n m_n = 0$$

$b = a_1 a_2 \cdots a_n$. Then

$bm_1 = \cdots = bm_n = 0$. Thus $bM = 0$

Given a finite abelian grp M,

it is a module over $\dfrac{\mathbb{Z}}{b\mathbb{Z}}$.

Chinese Remainder Theorem

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

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

Chinese Remainder Theorem:

A commutative ring with 1.

Ideals $\mathfrak{a}$ & $\mathfrak{b}$ are <u>comaximal</u> if $\mathfrak{a}+\mathfrak{b} := \{a+b \mid a\in\mathfrak{a}, b\in\mathfrak{b}\}$ is the whole of A

Obs: Ideals $\mathfrak{a}$ & $\mathfrak{b}$ are comaximal iff $\exists\, a\in\mathfrak{a}$ & $b\in\mathfrak{b}$ s/t $a+b=1$

$a+b=1$, $\quad x\in A \quad \underbrace{xa}_{\in\,\mathfrak{a}}+\underbrace{xb}_{\in\,\mathfrak{b}}=x$

When are two ideals in $\mathbb{Z}$ comaximal?

$m_1\mathbb{Z}$ & $m_2\mathbb{Z}$ $\quad m_1\mathbb{Z}+m_2\mathbb{Z}=(m_1,m_2)\mathbb{Z}$

$m_1\mathbb{Z}$ & $m_2\mathbb{Z}$ are comaximal iff

$(m_1, m_2) = 1$.

Suppose $\mathfrak{a}$ & $\mathfrak{b}$ are comaximal.

Then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

<u>Proof</u>: $\mathfrak{a} \cap \mathfrak{b} \supseteq \underbrace{\mathfrak{a}\mathfrak{b}}_{\text{``}\{ab \mid a\in\mathfrak{a}, b\in\mathfrak{b}\}\text{''}}$ ✓ in general

$\subseteq$: $x \in \mathfrak{a} \cap \mathfrak{b}$.

$\exists\, a \in \mathfrak{a}$ & $b \in \mathfrak{b}$ s/t $a + b = 1$

$x = \underbrace{xa}_{\in \mathfrak{a}\mathfrak{b}} + \underbrace{xb}_{\in \mathfrak{a}\mathfrak{b}} \implies x \in \mathfrak{a}\mathfrak{b}$.

$\blacksquare$

If $\mathfrak{a}$ & $\mathfrak{b}$ are comaximal
and $\mathfrak{a}$ & $\mathfrak{c}$ are comaximal
Then $\mathfrak{a}$ & $\mathfrak{b}\mathfrak{c}$ are comaximal

$$a + b = 1 \qquad a' + c = 1$$

$$(a+b)(a'+c) = 1$$

$$\underbrace{aa' + ac + a'b}_{\in\, \mathfrak{a}} + bc = 1$$

(a) If $\mathfrak{a}$ & $\mathfrak{b}$ are comaximal
Then so are $\mathfrak{a}^k$ & $\mathfrak{b}^l$ for
any integers $k, l \geq 1$.

$1 = (a+b)$ Choose $n \geq k+l-1$

$1 = \underbrace{(a+b)^n}$ $a^i b^{n-i}$

when you expand using the binomial theorem, every term is either in $\mathfrak{a}^k$ or $\mathfrak{b}^l$.

CRT. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise comaximal ideals in a comm. ring A with identity. Then $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$

and $\dfrac{A}{\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n} \underbrace{\simeq}_{\text{as rings}} \dfrac{A}{\mathfrak{a}_1} \times \dfrac{A}{\mathfrak{a}_2} \times \cdots \times \dfrac{A}{\mathfrak{a}_n}$

M finite abelian gp. $\mathbb{Z}/b\mathbb{Z}$

$b = p_1^{r_1} \cdots p_k^{r_k}$

$b\mathbb{Z} = \left(p_1^{r_1}\mathbb{Z}\right) \cdots \left(p_k^{r_k}\mathbb{Z}\right)$

$p_1^{r_1}\mathbb{Z}, \ldots, p_k^{r_k}\mathbb{Z}$ are pairwise comaximal

$\dfrac{\mathbb{Z}}{b\mathbb{Z}} \simeq \dfrac{\mathbb{Z}}{p_1^{r_1}\mathbb{Z}} \times \cdots \times \dfrac{\mathbb{Z}}{p_k^{r_k}\mathbb{Z}}$

ideal ideal

$$M = \frac{\mathbb{Z}}{b\mathbb{Z}} M$$

$$\simeq \underbrace{\frac{\mathbb{Z}}{p_1^{r_1}\mathbb{Z}} M} \times \dots \times \underbrace{\frac{\mathbb{Z}}{p_k^{r_k}\mathbb{Z}} M}$$

Chinese Remainder Theorem (general version)