Last time

If M is a f.g & torsion free $\mathbb{Z}$-mod $\Rightarrow$ M is free.

Prop) Say M is a f.g $\mathbb{Z}$ mod
Then $M = M_{tors} \oplus M/M_{tors}$ → free

Pf) M/M_{tors} is torsion free + fin gen (as quot of f.g)
$\Rightarrow M/M_{tors}$ free.

$\therefore$
$$
\begin{tikzcd}
0 \arrow[r] & M_{tors} \arrow[r] & M \arrow[r, "\pi"] & M/M_{tors} \arrow[l, dotted, bend left, "\exists \varphi"] \arrow[r] & 0
\end{tikzcd}
$$
M/M_{tors} → free

by final lemma from last lec $\exists\ \varphi$ so $\pi \circ \varphi = id$

$\Rightarrow M = M_{tors} \oplus \operatorname{im} \varphi$, $\operatorname{im}\varphi \cong M/M_{tors}$

Rmk) M f.g $\mathbb{Z}$ mod $\Rightarrow$ M tors is finite.
M_{tors} is f.g b/c $\mathbb{Z}$ is noeth
$\therefore$ let $x_1, \dots, x_n \in M_{tors}$ gen it
$\exists N \in \mathbb{Z}$, $N \neq 0$ so $N x_i = 0$ $\forall i$ (take lcm)
$\Rightarrow N \cdot x = 0$ $\forall x \in \underline{M_{tors}}$.

So, M_{tors} is naturally a $\mathbb{Z}/N\mathbb{Z}$-mod
$x_1, \dots, x_n$ gen M_{tors} as a $\mathbb{Z}/N\mathbb{Z}$ mod
$\Rightarrow$ have surj $(\mathbb{Z}/N\mathbb{Z})^n \twoheadrightarrow \underline{M_{tors}}$. $\therefore$ finite.

To prove main thm (Every fin gen $\mathbb{Z}$-mod is $\oplus$ of cyclic mod)
it suffices to treat the case of a finite grp.

Gen obs 1 if R & S are 2 rings & M, N are R & S mod resp.

$\Rightarrow M \oplus N$ is naturally a $R \times S$ module

$(r,s)(m,n) = (rm, sn)$

And every $R \times S$ module has the form above.

let $L = R \times S$ module

put $e = (1,0)$, $f = (0,1)$ are idempotents in $R \times S$

w/ $ef = 0$ $e + f = 1$

let $M = eL$ and $N = fL$

$\Rightarrow L \cong M \oplus N$ given $x \in L$ $x = 1 \cdot x = \underbrace{ex}_{\in M} + \underbrace{fx}_{\in N}$

Say, M = finite $\mathbb{Z}$ module

$\exists\, 0 \neq N \in \mathbb{Z}$ so $Nx = 0$ $\forall x \in M$

so M is a $\mathbb{Z}/N\mathbb{Z}$ module.

factor $N = p_1^{e_1} \cdots p_r^{e_r}$ p_i dist prime.

By CRT, $\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \text{———} \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$

obs

$\Rightarrow$ $M = M_1 \oplus \text{———} \oplus M_r$

$M_i = \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ module

Now suffices to show that f.g $\mathbb{Z}/p^r\mathbb{Z}$ mods are $\oplus$ of cyclic mods.

let M be a $\mathbb{Z}/p^r\mathbb{Z}$ module f.g.

Choose r to be minimal (eg if $p^{r-1}x = 0$ $\forall x \in M$ then M is a $\mathbb{Z}/p^{r-1}\mathbb{Z}$ -mod repl w/ $r = r-1$)

$\therefore \exists\, x \in M$ so $p^{r-1}x \neq 0$

$\therefore$ Submod gen'd by x is $\cong \mathbb{Z}/p^r\mathbb{Z}$ (i.e $\operatorname{ord}(x) = p^r$) $\Leftrightarrow$ cyclic subgrp

Idea: split this off from M as a summand

Rmk| if M is a R-mod & $x \in M$
$\langle x \rangle$ submod gen'd by x
To understand this, consider
$$\varphi : R \to M \qquad \operatorname{im}\varphi = \langle x \rangle$$
$$a \longmapsto ax$$
$\langle x \rangle \cong R/\ker\varphi$ & $\ker\varphi = \{a \in R \mid ax = 0\}$
↳ $\operatorname{ann}(x)$
↳ annihilator

General| Given an R-submod $M \subset N$
$\exists$ idea of complimentary submod $M' \subset N$
so $N = M + M'$ & $M \cap M' = 0$
i.e. $N = M \oplus M'$

We say a SES is split
$$0 \to M \xrightarrow{i} N \xrightarrow{\pi} L \to 0$$
if $\exists$ compl submod M' to M
(rmk $\pi|_{M'} : M' \to L$ is isom)

TFAE
1. The SES is split
2. $\exists\, \varphi : L \to N$ so $\pi \circ \varphi = \mathrm{id}_L$ [$M' = \operatorname{im}\varphi$]
3. $\exists\, \psi : N \to M$ so $\psi \circ i = \mathrm{id}_M$ [$M' = \ker\psi$]

Lemma| (last time)
If L is free then any SES as above is split
↳ using crit 2

In fact L is projective $\iff$ any such SES splits

Defn) M is an injective module if any SES as above splits

Rmk) M is inj iff whenever if $M \subset N$ $\exists$ compl submod to M.

Eg) $2\mathbb{Z} \subset \mathbb{Z}$ has no compl submod.

$$\begin{array}{c} 2\mathbb{Z} \\ \cong \\ \mathbb{Z} \end{array}$$

so $\mathbb{Z}$ is not injective as a $\mathbb{Z}$ mod

The SES $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ not split.

WTS) $\mathbb{Z}/p\mathbb{Z}$ is injective as a module over itself.

Why) let M - f.g $\mathbb{Z}/p^r\mathbb{Z}$ with r minimal

Pick $x \in M$ s.t $p^{r-1}x \neq 0$

$$\begin{array}{c} \langle x \rangle \subset M \\ \cong \\ \mathbb{Z}/p^r\mathbb{Z} \end{array}$$

if $\langle x \rangle$ inj then $\exists$ compl mod to $\langle x \rangle$ so

$M = \langle x \rangle \oplus (?)$ smaller (as finite) cont pf by ind.

(need minimality as $\mathbb{Z}/p\mathbb{Z}$ not inj as a $\mathbb{Z}/p^2\mathbb{Z}$-mod)

$$0 \to \underbrace{p\mathbb{Z}/p^2\mathbb{Z}}_{\cong \mathbb{Z}/p\mathbb{Z}} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

This doesn't split $\Rightarrow$ $\mathbb{Z}/p\mathbb{Z}$ not inj as $\mathbb{Z}/p^2\mathbb{Z}$ mod.

E.g) $M = \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ as $\mathbb{Z}/p^2\mathbb{Z}$ mod

$x = (p, 0)$ & $\langle x \rangle = p\mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$ not inj & no split