Lecture 40: Modules over PID IV - Smith Normal Forms

Recall: • Defined Torsion elements: $x \in M$ with $\mathrm{Ann}(x) \neq (0)$

$M_{Tor} = \{\text{torsion elements}\}$ submodule of M

• M is Torsion free module $\Leftrightarrow M_{Tor} = \{0\}$

• Pick representatives for prime elements in R $\{p_i\}_{i \in I}$

↳ $(p) \neq 0$ prime ideal

Classification Theorem I: If $(0) \neq M$ is a fg Torsion module over a PID R, then:

$$M = \bigoplus_{p_i \text{ prime}} M_{p_i^{n_i}}$$

for suitable $n_i \in \mathbb{Z}_{>0}$ with $M_{p_i^{n_i}} \neq \{0\}$.

Furthermore: $M_{p_i^{n_i}} \cong R/(p^{v_1^{(i)}}) \oplus \cdots \oplus R/(p^{v_s^{(i)}})$

with $n_i = v_1^{(i)} \geq v_2 \geq \cdots \geq v_s \geq 1$ & the sequence (v_i) is uniquely determined by M & p.

§2 Classification v2:

We can rearrange the $M_{p_i^{v_j^{(i)}}}$ factors to give an alternative classification:

Classification Thm v2: If $0 \neq M$ is a fg torsion module over a PID R, then $M \cong R/(q_1) \oplus \cdots \oplus R/(q_r)$

where $q_i \neq 0$, $q_i \notin R^\times$ $\forall i$ & $q_r \mid q_{r-1} \mid \cdots \mid q_1$.

Furthermore, the sequence of ideals $(q_1), \ldots, (q_r)$ is uniquely determined by the above conditions.

Pf/ Write $M = \bigoplus_{i=1}^{r} M_{p_i^{n_i}}$

$$M_{p_i^{n_i}} \cong R/(p_i^{\nu_1^{(i)}}) \oplus \cdots \oplus R/(p_i^{\nu_{s_i}^{(i)}}) \quad \text{with}$$

$$\nu_1^{(i)} \geq \cdots \geq \nu_{s_i}^{(i)} \geq 1$$

- We complete with $\nu_j^{(i)} = 0 \;\; \forall j > s_i$ so that all decomp have the same number of summands. $s = \max_{1 \leq i \leq r} \{s_i\}$
- We regroup by columns:

$$\begin{array}{ccccccc}
M_{p_1^{n_1}} & = & \boxed{R/(p_1^{\nu_1^{(1)}})} & \oplus & \cdots & \oplus & \boxed{R/(p_1^{\nu_s^{(1)}})} \\
\oplus & & \oplus & & & & \oplus \\
\vdots & & & & & & \\
M_{p_r^{n_r}} & = & \boxed{R/(p_r^{\nu_1^{(r)}})} & \oplus & \cdots & \oplus & \boxed{R/(p_r^{\nu_s^{(r)}})} \\
 & & \cong R/(q_1) & & & & \cong R/(q_r)
\end{array}$$

Where $q_i = \prod_{j=1}^{s} p_j^{\nu_i^{(s)}}$ (Here $p^0 = 1$)

<u>Claim</u> $R/(p_1^{\nu_i^{(1)}}) \oplus \cdots \oplus R/(p_r^{\nu_i^{(r)}}) \cong R/(q_i)$

Pf/ CRT $p_1, \ldots, p_r$ are distinct coprimes so, after ignoring the 0-summands in (LHS), we get pairwise coprime ideals $(p_1^{\nu_i^{(1)}}), \ldots, (p_r^{\nu_i^{(r)}})$ (Lecture 23)

- $(q_i) \underset{\substack{\text{PID} \\ \text{unique factoriz.}}}{=} \bigcap_{j=1}^{r} (p_j^{\nu_i^{(j)}}) \underset{\text{Lecture 23}}{=} \prod_{j=1}^{r} (p_j^{\nu_i^{(j)}})$

- Iso in claim follows from CRT (Lecture 17)

By construction $q_r \mid q_{r-1} \mid \cdots \mid q_1$ because $\nu_i^{(j)} \geq \nu_{i+1}^{(j)}$ $\forall j$

<u>Uniqueness</u> $\mathrm{Ann}(M) = (q_1)$ Pick $x \in M$ with $\mathrm{Ann}(x) = q_1$.

$\rightsquigarrow$ $\mathrm{Ann}(M/(x)) = (q_2)$ (use Lemma from page 2), etc.

§2. Structure Thm:

Recall the following statement from Lecture 28:

<u>Lemma</u>: Consider M & M' two modules over a PID R. Assume M' is free & let $f: M \to M'$ be a surjective homomorphism of R-modules. Then, there exists a free submodule N of M such that

(1) $f|_N$ induces an isomorphism $f|_N : N \xrightarrow{\sim} M'$.

(2) $M = N \oplus \operatorname{Ker} f$. $\quad$ ($N = (x_i : i \in I)$ $\quad f(x_i) = x_i'$ $\quad$)
$\{x_i'\}$ basis for M'

We'll use this to prove the following statement:

<u>Structure Thm</u> Assume R is a PID and M = f.g. free R-mod of rank n. Fix $0 \neq N \subseteq M$ submodule. Then $\exists$ basis $\{e_1, \ldots, e_n\}$ of M and $a_1, \ldots, a_r \in R \setminus \{0\}$ such that

(1) $a_1 \mid a_2 \mid \cdots \mid a_r$.

(2) $\{a_1 e_1, \ldots, a_r e_r\}$ is a basis for N

<u>Proof</u> We know N is free of rank $\leq n$. (Theorem 2, Lecture 27)

- We argue by induction on n:
- <u>Base case</u>: $n=1$ so $M = R$ & $N = (a)$ $a \neq 0$.
- <u>Induction Step</u> Consider $\mathcal{F} = \{T(N) : T \in \mathrm{Hom}_R(M,R)\}$
- Each $T(N)$ is a submodule of R (ie an ideal)
- $\mathcal{F} \neq \emptyset$ $((0) \in \mathcal{F})$
- R Noetherian $\Rightarrow \exists\, \mathcal{M} \in \mathcal{F}$ maximal element.
- <u>Claim 1</u> $\mathcal{M} \underset{R\,PID}{=} (\alpha) \neq (0)$.

Pf/ $M \simeq R^n \xrightarrow{\pi_j} R$ projection to j^{th} copy.

$N \neq (0)$ in R^n so $\exists\, (x_1 \dots x_n) \in N$ with some $x_j \neq 0$

$\Rightarrow \pi_j(N) \ni x_j \neq 0$.

- $\exists\, T_0 \in \mathrm{Hom}_R(M,R)$ & $v \in N$ with $T_0(v) = \alpha$.
- <u>Claim 2</u> $\forall\, T \in \mathrm{Hom}_R(M,R)$ $\alpha \mid T(v)$. (ie $T(v) \in (\alpha)$)

Pf/ Write $(\alpha, T(v)) = (d)$ (R is a PID)

$$d = a\alpha + bT(v) = aT_0(v) + bT(v) = \underbrace{(aT_0 + bT)}_{\in\ \mathrm{Hom}_R(M,R)}(v)$$

So $(d) = (\alpha)$ by maximality

$\Rightarrow \alpha \mid T(v)$.

- Apply the Claim to each $\pi_j \Rightarrow \alpha \mid \pi_j(v)$ $\forall j$

Thus $v = (\alpha b_1, \alpha b_2, \dots, \alpha b_m)$ for $b_1, \dots b_m \in R$

- Write $w = (b_1, b_2, \dots, b_m)$ so $v = \alpha w$.

$\Rightarrow \alpha = T_0(v) = \alpha T_0(w) \underset{R\ \text{domain}}{\Longrightarrow} T_0(w) = 1$

<u>Claim 3</u>: $M = (\mathrm{Ker}\, T_0) \oplus Rw$ $\Rightarrow$ rank $\mathrm{Ker}\, T_0 = n-1$

$N = (N \cap \mathrm{Ker}\, T_0) \oplus Rv$

Pf/ Use Lemma for $T_0 : M \twoheadrightarrow R$ $\quad T_0(w) = 1$

$T_0|_N \; N \twoheadrightarrow R\alpha \simeq R$ $\quad T_0(v) = \alpha$

• $\mathrm{rank}(\mathrm{Ker}\, T_0) = n-1$ & $N \cap \mathrm{Ker}\, T_0 \subseteq \mathrm{Ker}\, T_0$ submodule $\neq (0)$ (otherwise $r=1$ & we are done)

$\Rightarrow$ By IH $\exists \{e_2, \ldots, e_n\}$ basis of $\mathrm{Ker}\, T_0$ & $\alpha_2, \alpha_3, \ldots, \alpha_r \in R$ with $\{a_2 e_2, \ldots, a_r e_r\}$ basis for $N \cap \mathrm{Ker}\, T_0$.

$a_2 | a_3 | \cdots | a_r$.

• To finish, set $a_1 = \alpha$, $e_1 = w$

<u>Claim 4</u>: $a_1 | a_2$.

Pf/ Define $T \in \mathrm{Hom}_R(M, R)$ via $T(e_1) = 1 = T(e_2)$ &

$T(e_i) = 0 \quad \forall i > 2$.

Then $\alpha = T(\alpha w) \in T(N)$ so $(\alpha) \subset T(N)$

By maximality of α: $T(N) = (\alpha)$

But $a_2 = T(\underbrace{a_2 e_2}_{\in N})$ so $a_2 \in (\alpha)$, ie $\alpha | a_2$. $\square$

<u>Examples</u>: ① $M = \mathbb{Z} \times \mathbb{Z}$ $\quad N_1 = ((0,1), (2,0))$ $\quad e_2 = (0,1)$, $e_1 = (1,0)$, $a_1 = 1, a_2 = 2$

① $N_2 = ((0,1), (2,2))$ $\quad M = \mathbb{Z}^2$

$e_1 = (0,1)$, $e_2 = (1,1)$ $\quad a_1 = 1, a_2 = 2$.

§2. Equivalence of matrices

Def: Assume R is a commutative ring & $A, B \in Mat_{m\times n}(R)$.
We say A is *equivalent* to B (write, $A \sim B$) if $\exists\, P \in GL_n(R)$, $Q \in GL_m(R)$ with $B = QAP^{-1}$

- Clear: $\sim$ defines an equivalence relation on $Mat_{m\times n}(R)$
- Q: Can we find nice representatives for each class?

A: Depends on R.

Example: $R = \mathbb{K}$ field, then $A \sim \begin{array}{c} \overbrace{\hphantom{1\ 0}}^{r} \hphantom{\ \ 0} \\ \left[\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right] \end{array}$ $r = \text{rank}(A)$

(via row & column reduction)

Theorem: Assume R is a PID, then every matrix $A \in Mat_{m\times n}(R)$ is equivalent to a matrix

$$S = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & d_2 & & 0 \\ 0 & & \ddots\ d_r & \\ \hline & 0 & & 0 \end{array}\right) \quad \text{with } d_1 | d_2 | \cdots | d_r.$$

(invariant factors)

Name = S = Smith Normal Form of A.

Pf/ Consider the R-linear map $T_A : R^n \xrightarrow{A\cdot} R^m$

- $T_A(R^n) \subset R^m$ is a submodule of a free rank-m mod

$\Rightarrow T_A(R^n)$ is free of rank $\leq m$

- By Structure Thm $\exists$ basis $B' = \{e_1, \ldots, e_m\}$ of R^m & $d_1, \cdots d_r \in R$ s.t $\{d_1e_1, \ldots, d_re_r\}$ is a basis for $T_A(R^n)$ & $d_i | d_{i+1}\ \forall i$

- Pick f_i with $T_A(f_i) = d_ie_i$ $(i = 1, \ldots, r)$ & let $N = (f_1, \ldots, f_r)$

View $T_A : R^n \twoheadrightarrow T_A(N)$ with basis $\{d_ie_i\}_{i=1}^{r}$. By the Lemma, we get

$$\mathbb{R}^n = N \oplus \operatorname{Ker} T_A . \qquad N, \operatorname{Ker} T_A \text{ free of complem. rank}$$

- If $\{f_{r+1}, \ldots, f_n\}$ is a basis for $\operatorname{Ker} T_A$, then:

$B = \{f_1, \ldots, f_n\}$ is a basis for $\mathbb{R}^n$ &

$$[T_A]_{BB'} = \left[\begin{array}{c|c} \begin{matrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right] \qquad d_1 \cdots d_r .$$

P^{-1} = Change of basis from $\{e_1, \ldots, e_n\}$ to B

Q = ———————— B' to $\{e_1, \ldots, e_m\}$