Lecture 30: Modules over PIDs IV - Canonical forms for matrices

Recall:

- $M_a = \ker\left(M \xrightarrow[m \longmapsto a\cdot m]{a} M\right)$ $\qquad M_{tor} = \{x : \mathrm{Ann}(x) \neq (0)\}$
- p-Torsion elements $= \{x \in M : \mathrm{Ann}(x) = (p^k)$ for some $k \geq 0\}$.
- **Classification Thm:** If $M \neq 0$ is a fg Torsion module over a PID R, then

$$(*) \quad M = \bigoplus_{p_i \text{ prime}} M_{p_i^{n_i}} \quad \text{for } n_i \geq 1 \text{ (unique choice)}$$

Furthermore: $M_{p^n} \cong R/(p^{\nu_1}) \oplus \cdots \oplus R/(p^{\nu_s})$ with $n = \nu_1 \geq \nu_2 \geq \cdots \geq \nu_s$ $(p = p_i)$

The sequence (ν_i) is uniquely determined by M & p. (Type of M_{p^n})

TODAY:

- 2nd Classification Thm
- 2nd Structure Thm
- Smith Normal Forms of $m \times n$ matrices over PIDs

Classification Thm v2: If $0 \neq M$ is a fg torsion module over a PID R, then

$$M \simeq R/(q_1) \oplus \cdots \oplus R/(q_r)$$

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.

Proof: Write $M = \bigoplus_{i=1}^{t} M_{p_i^{n_i}}$ & $M_{p_i^{n_i}} \simeq R/(p_i^{\nu_1^{(i)}}) \oplus \cdots \oplus R/(p_i^{\nu_{s_i}^{(i)}})$ 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, $\boxed{s = \max\{s_1, \ldots, s_r\}}$
- We regroup by columns:

$$M_{p_1^{n_1}} = \boxed{R/(p_1^{\nu_1^{(1)}}) \oplus \cdots \oplus R/(p_1^{\nu_s^{(1)}})} \oplus \cdots \oplus \boxed{R/(p_t^{\nu_s^{(t)}})}$$
$$\vdots$$
$$M_{p_r^{n_r}} = \boxed{R/(p_r^{\nu_1^{(r)}}) \oplus \cdots \oplus R/(p_r^{\nu_s^{(r)}})}$$

$\simeq R/(q_1)$ $\qquad$ $\simeq R/(q_r)$

where $\boxed{q_i = \prod_{j=1}^{t} p_j^{\nu_i^{(j)}}}$

(Here $p^0 = 1$)

Claim $\dfrac{R}{(p_1^{\nu_i^{(1)}})} \oplus \cdots \oplus \dfrac{R}{(p_r^{\nu_i^{(r)}})} \cong \dfrac{R}{(q_i)}$

Pf/ Since $p_1, \ldots, p_r$ 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)

- $(q_i) = \bigcap_{j=1}^{r} (p_j^{\nu_i^{(j)}}) = \prod_{j=1}^{r} (p_j^{\nu_i^{(j)}})$

  $=$ (PID, unique factoriz.) $=$ (Lecture 23)

- Iso in claim follows from CRT (Lecture 17)

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

Uniqueness $\mathrm{Ann}(\Pi) = (q_1)$ Pick $x \in \Pi$ with $\mathrm{Ann}(x) = q$.

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

Structure Theorem

- Recall the following statement from Lecture 28:

Lemma: 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) $M = N \oplus \ker f$.

($N = (x_i : i \in I)$ $f(x_i) = x_i'$ $(\{x_i'\}_{i\in I}$ basis for $M')$

- We'll use this to prove the following statement:

Structure Thm Assume R is a PID and $M = $ fg free R-mod of rank n. Fix $0 \neq N \subseteq M$ submodule. Then $\exists$ bases $\{e_1 \dots e_n\}$ of M and $a_1, \dots, a_r \in R \setminus \{0\}$ such that

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

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

Ex: $M = \mathbb{Z}^2$

$N = \mathbb{Z}((1,0),(0,2)) = \{(n, 2m) : n, m \in \mathbb{Z}\}$

$e_1 = (1,0)$ $a_1 = 1$ $\{e_1, e_2\}$ basis for M

$e_2 = (0,1)$ $a_2 = 2$ $\{e_1, 2e_2\}$ basis for N

Pf/ $0 \neq N \subseteq M \simeq R^n$ submod $\rightsquigarrow$ To Build: $\{e_1 \dots e_n\}$ basis for M & $a_1, \dots, a_r \in R$ with $\{a_1 e_1, \dots, a_r e_r\}$ ——— N $a_i | a_{i+1}$ $\forall i$

We know N is free of rank $\leq n$. (Theorem 2, Lecture 27) (r = rank N)

- We argue by induction on n:
- Base case: $n=1$ so $M = R$ & $N = (a)$ $a \neq 0$.
- Induction Step Consider $\mathcal{F} = \{T(N) : T \in Hom_R(M, R)\}$
- Each $T(N)$ is a submodule of R (ie an ideal)
- $\mathcal{F} \neq \emptyset$ ($(0) \in \mathcal{F}$)

$\Big\}$ $\overset{R \text{ Noeth}}{\Rightarrow}$ $\exists\, m \in \mathcal{F}$ maximal element.

- Claim 1 $m = (\alpha) \neq (0)$. (R PID)

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

- $\exists\, T_0 \in Hom_R(M, R)$ & $v \in N$ with $T_0(v) = \alpha$.
- Claim 2 $\forall\, T \in Hom_R(M, R)$ $\alpha \mid T(v)$. (ie $T(v) \in (\alpha)$)

Pf/ Write $(\alpha, T(v)) = (d) \Rightarrow d = a\alpha + bT(v) = aT_0(v) + bT(v)$

$= (aT_0 + bT)(v)$, with $(d) \in \mathcal{F}$, $Hom_R(M,R)$

So $(d) \supseteq (\alpha) \Rightarrow$ by maximality for (α): $(\alpha) = (d) \ni T(v)$.

• Apply the claim to each $\pi_j \Rightarrow \alpha \mid \pi_j(v)\ \forall j$

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

$\Rightarrow \alpha = T_0(v) = \alpha T_0(w) \xRightarrow[R\text{domain}]{} T_0(w) = 1$

Claim 3: $M = (\ker T_0) \oplus Rw$ $\Rightarrow \operatorname{rank} \ker T_0 = n-1$

$N = (N \cap \ker T_0) \oplus Rv$

Pf/ Use Lemma for $T_0 : M \twoheadrightarrow R$ & $T_0|_N \; N \twoheadrightarrow R\alpha \simeq R$

$[T_0(w) = 1]$ $[T_0(v) = \alpha \; ; \; T_0(N) = (\alpha)]$

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

$\Rightarrow$ By IH $\exists \{e_2, \dots, e_n\}$ basis of $\ker T_0$ & $\alpha_2, \alpha_3, \dots, \alpha_r \in R$ with

- $\{a_2 e_2, \dots, a_r e_r\}$ basis for $N \cap \ker T_0$.
- $a_2 \mid a_3 \mid \cdots \mid a_r$.

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

• By construction • $\{e_1, e_2, \dots, e_n\}$ is basis for M, $\{\underbrace{a_1 e_1}_{=v}, a_2 e_2, \dots, a_r e_r\}$ basis for N

• $a_2 \mid \cdots \mid a_r$

Claim 4: $a_1 \mid a_2$.

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

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

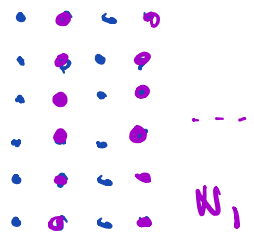
Then $\alpha = T(\alpha\omega) \in T(N)$ so $(\alpha) \subset T(N)$

By maximality of α: $T(N) = (\alpha)$

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

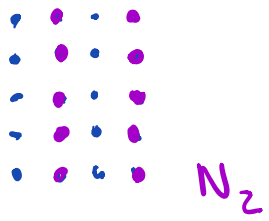
Examples: ① $M = \mathbb{Z} \times \mathbb{Z}$ $\quad N_1 = ((0,1), (2,0))$

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



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

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



Equivalence of matrices

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

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

Example: $R = \mathbb{K}$ field, then $A \sim \left[\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right]$ (r ones) $r = \mathrm{rank}(A)$ (via row & column reduction)

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

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

(d_i: 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 $\Rightarrow$ free of rank $\leq m$

- By Structure Theorem: $\exists$ basis $B' = \{e_1, \dots, e_m\}$ of R^m & $d_1 \dots d_r \in R$ s.t.
  $\{d_1 e_1, \dots, d_r e_r\}$ is a basis for $T_A(R^n)$ & $d_i \mid d_{i+1}$ $\forall i$

- Pick f_i with $T_A(f_i) = d_i e_i$ $(i = 1, \dots, r)$ & let $N = (f_1, \dots, f_r)$

- Then $R^n = N \oplus \operatorname{Ker} T_A$. $N, \operatorname{Ker} T_A$ free of complem. rank [lemma applied to $T_A : R^n \to T_A(R^n)$, free]

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

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

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

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

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

□