Lecture 32: Rational normal forms & Jordan canonical forms

In the last lecture, we saw 2 ways to classify non-zero finitely generated torsion modules over a PID R:

Classification Theorem 1: If $(0) \neq M$ is a fg torsion module over a PID R, then:

$$M = \bigoplus_{p_i \text{ prime}} M_{p_i^{n_i}} \quad \text{for suitable } n_i \in \mathbb{Z}_{\geq 0} \ (n_i \text{ minimal}) \quad \text{with } M_{p_i^{n_i}} \neq \{0\}.$$

Furthermore: $M_{p_i^{n_i}} \simeq R/(p_i^{\nu_1^{(i)}}) \oplus \cdots \oplus R/(p_i^{\nu_{s_i}^{(i)}})$

with $n_i = \nu_1^{(i)} \geq \nu_2 \geq \cdots \geq \nu_s \geq 1$ & the sequence (ν_i) is uniquely determined by M & p_i.

Classification Thm v2: If $M \neq (0)$ 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.

TODAY'S GOAL: Focus on the case of $\mathbb{K}[x]$-modules, where $\mathbb{K}$ is a field of characteristic 0 (in char p, perfect fields will be needed (see Math 6112))

§1. $\mathbb{K}[x]$-modules:

Q: What is a $\mathbb{K}[x]$-module?

A. a $\mathbb{K}$-vector space V

- multiplication by X defines a map $x\cdot : V \longrightarrow V$, $m \longmapsto x\cdot m$
- $x\cdot$ is $\mathbb{K}$-linear since $\mathbb{K}[x]$- is commutative.

$$x\cdot(a\cdot m) \underset{\text{Assoc.}}{=} (x\cdot a)\,m \underset{\mathbb{K}[x]\text{ comm}}{=} (a\cdot x)\,m \underset{\text{Assoc}}{=} a\cdot(x\cdot m)$$

Conclude: $\mathbb{K}[x]$-module $\longleftrightarrow$ a $\mathbb{K}$-vector space V + $\varphi \in \mathrm{End}_{\mathbb{K}}(V)$.

From now on, we assume V has $\dim_{\mathbb{K}} V = n < \infty$.

So $\varphi \longleftrightarrow A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$ (matrix of the linear transf w.r.t a fixed basis)

$\rightsquigarrow$ Define a map Ψ $\mathbb{K}[x] \longrightarrow \mathbb{K}[A] \subset \mathrm{End}_{\mathbb{K}}(V)$

$$P(X) \longmapsto P(A)$$

- What is $P(A)$? If $v \in V$, then:

$$P = \sum_{i=0}^{N} a_i x^i \rightsquigarrow P(A)(v) = \sum_{i=0}^{N} a_i \, (A^i)(v).$$
$$A^i = \underbrace{A\circ\cdots\circ A}_{i \text{ times}}$$

- Ψ is a ring homomorphism.
- $\mathrm{Im}\,\Psi$ = subring of $\mathrm{End}_{\mathbb{K}}(V)$ generated by A & $\mathbb{K}$.
- $\mathrm{Ker}\,\Psi = ?$ Ideal of $\mathbb{K}[x]$ = PID so

$\rightsquigarrow \mathrm{Ker}\,\Psi = (f)$ for some $f \in \mathbb{K}[x]$

Lemma: $\mathrm{Ker}\,\Psi \neq (0)$:

Pf/ $\mathbb{K}[A] \underset{\text{subspace}}{\subseteq} \mathrm{End}_{\mathbb{K}}(V) \cong \underset{\text{f.dim }\mathbb{K}\text{-VS}}{\mathrm{Mat}_{n\times n}(\mathbb{K})} \Rightarrow \dim_{\mathbb{K}} \mathbb{K}[A] < \infty$

Ψ is also $\mathbb{K}$-linear map. If $\mathrm{Ker}\,\Psi = (0)$, then

$\underset{\text{inf dim'l}}{\mathbb{K}[x]} \subseteq \underset{\text{fin dim'l}}{\mathbb{K}[A]}$ Contr! $\square$

Name: $f \neq 0 \rightsquigarrow$ take $q_A(x) = \frac{1}{LT(f)} f$ (monic)

$q_A(x) =$ minimal polynomial of A over k.

§2. Cyclic case:

Proposition Assume we have $v \in V$ s.t. $V = k[x] \cdot v$, ie V is generated by $\{v, Av, A^2v, \ldots\}$ (over $\mathbb{K}$) (V is cyclic). Then,

(1) $\deg(q_A)$ is minimal integer $d \geq 0$ s.t $\{v, Av, \ldots, A^d v\}$ is ld, ie:

- $\{v, Av, \ldots, A^{d-1}v\}$ is li
- $\{v, Av, \ldots, A^d v\}$ is ld.

(2) Furthermore, in this situation $\{v, Av, \ldots, A^{d-1}v\}$ is a basis for V.

Pf/ Since V is f.dim'l we have $\{v, Av, \ldots, A^d v\}$ ld for some d

(2) If d is minimal, then $\{v, Av, \ldots, A^{d-1}v\}$ is li.

We claim $A^d v \in \operatorname{Span}(v, Av, \ldots, A^{d-1}v)$ & by induction on $k \geq 0$ $A^{d+k}v \in$ ____________________.

So $\{v, Av, \ldots, A^{d-1}v\}$ is a basis for V.

(1) Write a nontrivial l.d relation:

$$a_0 v + a_1 Av + a_2 A^2 v + \cdots + a_{d-1} A^{d-1} v + a_d A^d v = 0$$

Since $a_d \neq 0$, we can assume $a_d = 1$. Call: $h_{(x)} = \sum_{i=0}^{d} a_i x^i$

We claim $h = q_A$

(1) $h \in \operatorname{Ker} \Psi$ ($h(A)_{(v)} = 0$, $h(A)(Av) = A\underbrace{h(A)_{(v)}}_{=0} = 0$, $\ldots$ $h(A)(A^\ell v) = A^\ell \underbrace{h(A)(v)}_{=0} = 0$. $\rightsquigarrow h(A)_{|V} = 0$)

$\Rightarrow h = q_A\, g$ for $g \in \mathbb{K}[x]$

(2) If $\deg q_A < \deg h = d \Rightarrow$ We would have a dependency relation for $\{v, Av, A^2v, \ldots, A^{d-1}v\}$ Contr!

<u>Conclude</u>: $\deg q_A = \deg h$, $q_A \mid h$ & both are monic $\Rightarrow q_A = h$ $\square$

<u>Corollary 1</u>: If V is cyclic as a $\mathbb{K}[x]$-module and

$q_A = x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0$, then in the basis

$\mathcal{B} = \{v, Av, \dots A^{d-1}v\}$ we have

$$[A]_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} 0 & & & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & & 1 & -a_{d-1} \end{bmatrix} = \underset{C_{q_A}}{\text{Companion matrix}} \text{ for the polynomial } q_A.$$

(Characteristic poly $= q_A$)

<u>Corollary 2</u>: If V is cyclic, then: $V \simeq \mathbb{K}[x]/q_A(x)$ (as $\mathbb{K}$-v.s.)

(Why? $\mathbb{K}[x] \xrightarrow{\varphi} V$ is surj & $\ker\varphi = (q_A(x))$)

$f(x) \longmapsto f(v)$

Moreover $q_A(x)$ is independent of the choice of generator v for V
$=$ an invariant of V.

(<u>Reason</u> (HW10): $\mathbb{K}[x]/(f) \simeq \mathbb{K}[x]/(g) \iff \deg f = \deg g$ (same dim!))

§3 Non-cyclic case:

<u>Q</u>: What happens in the non-cyclic case?

<u>A</u>: Classification Theorems for f.g. Torsion modules / $\mathbb{K}[x]$.

<u>Obs</u>: $\dim_{\mathbb{K}} V < \infty$, then V is a Torsion module over $\mathbb{K}[x]$.

($q_A(A) = 0$ endomorphism, meaning $q_A(A)(w) = 0$ $\forall w \in V$)

<u>Theorem 1</u>: V $\mathbb{K}$-vector space & $A \in \mathrm{End}_{\mathbb{K}}(V)$ $A \neq 0$. Then, V admits a direct sum decomposition: $V = V_1 \oplus \dots \oplus V_r$
where each V_i is a cyclic $\mathbb{K}[x]$-module with invariants $q_i \neq 0$ satisfying
$q_1 \mid q_2 \mid \dots \mid q_r$. Furthermore, the sequence $(q_1, \dots, q_r)$ is uniquely determined by V & A, & $q_r = q_A$.

Pf/ Classification Theorem v2 gives the q_i's. Uniqueness also follows.

To finish: $\mathrm{Ann}(V) = (q_A) \ni q_r$ since $q_i \mid q_r \ \forall i$

But $q_r \mid q_A$ since $q_A(x) \cdot V_r = 0$ so $q_r = q_A$ (both monic) □

<u>Corollary</u>: V admits a basis B with

$$[A]_{BB} = \begin{bmatrix} \boxed{C_{q_1}} & & 0 \\ & \ddots & \\ 0 & & \boxed{C_{q_r}} \end{bmatrix}$$

C_{q_i} = companion matrix for each q_i

This is known as the <u>rational normal form for A</u>.

($A \sim RNF(A)$ where $A \sim C$ iff $\exists\, Q \in GL_n(\mathbb{K})$ with $A = Q^{-1} C Q$)

Pf/ Pick v_i generator for V_i $\rightsquigarrow B_i = \{v, Av, \ldots, A^{d_i - 1} v\}$ with $d_i = \deg q_i$. Then, take $B = B_1 \cup \cdots \cup B_r$. □

Q: What about alternative Classification Thm?

We factor $q_A(x) = p_1^{n_1}(x) \cdots p_s^{n_s}(x)$ into distinct prime powers ($p_i(x)$ = monic & irreducible)

- The p_i's are the representatives of prime elements in $\mathbb{K}[x]$
- Everything is monic, so no unit is needed in the factorization

<u>Theorem 2</u>: V $\mathbb{k}$-vector space & $A \in \mathrm{End}_{\mathbb{k}}(V)$ $A \neq 0$. Then, V admits a direct sum decomposition: $V = V_{p_1^{n_1}} \oplus \cdots \oplus V_{p_r^{n_r}}$

Furthermore, each $V_{p_i^{n_i}}$ can be express as a direct sum of submodules isomorphic to $\mathbb{k}[x] / (p_i^{\nu_j^{(i)}})$ (with $n_i = \nu_1^{(i)} \geq \cdots \geq \nu_{s_i}^{(i)}$)

§ 4. Jordan canonical form:

In the special case when $\mathbb{K} = \overline{\mathbb{K}}$, char 0 (Eg $\mathbb{K}=\mathbb{C}$) then write $p_i = (x-\alpha)$ for some $\alpha \in \mathbb{K}$.

Each $\dfrac{\mathbb{K}[x]}{(p_i)^m}$ piece gives a cyclic submodule $W_{p_i,m} \neq (0)$ of V of dimension m

Theorem 3: $W_{p_i,m}$ has a basis B over $\mathbb{K}$ such that

$$[A|_{W_{p_i,m}}]_B = \begin{bmatrix} \alpha_i & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \alpha_i \end{bmatrix} \quad \begin{array}{l} (m\times m \text{ matrix}) \\ = J(\alpha, m) \end{array}$$

Pf/ $W_{p_i,m}$ is generated by some $\omega \in V$.

Claim: $B = \{\omega, (A-\alpha)\omega, \ldots, (A-\alpha)^{m-1}\omega\}$ is a basis.

- LI: $(x-\alpha)^m$ is the minimal polynomial of $W_{p_i,m}$.
  Any dependency will yield a polynomial g with $g(A)|_{W_{p_i,m}}=0$.
- Span: Proposition from early on + binomial Theorem.
  (Alternative $|B| = \dim W_{p_i,m}$.)
- Note: $(A-\alpha)^{k+1}(\omega) = (A-\alpha)((A-\alpha)^k(\omega))$ yields

$$A(A-\alpha)^{k+1}(\omega) = (A-\alpha)^{k+1}(\omega) + \alpha(A-\alpha)^k(\omega)$$

Also $(A-\alpha)^m(\omega) = 0$ since $q_{A|_{W_{p_i,m}}} = (x-\alpha)^m$.

So $[A|_{W_{p_i,m}}]_B$ has the desired shape. $\square$

Corollary: Given V & A with $q_A = p_1^{n_1}\cdots p_r^{n_r}$, $\exists B$ basis for V with $[A]_B = \begin{bmatrix} \boxed{A_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_r} \end{bmatrix}$ block diagonal decomp

Furthermore for $p_i = (x-\alpha_i)$, we have.

$$A_i = \begin{bmatrix} J(\alpha_i, m_1^{(i)}) & & 0 \\ & \ddots & \\ 0 & & J(\alpha_i, m_{s_i}^{(i)}) \end{bmatrix}$$

with $n_i = m_1^{(i)} \geq \dots \geq m_{s_i}^{(i)}$

- This block decomposition is the Jordan canonical form of the matrix A.