Lecture 31: Rational normal forms, Jordan canonical forms

Last 2 lectures: Saw Classification theorems for fg Torsion modules over PIDs

Fix: $M \neq (0)$ a fg Torsion module over a PID R

Classification Theorem 1: $M = \bigoplus_{p_i \text{ prime}} M_{p_i^{n_i}}$ for suitable $n_i \in \mathbb{Z}_{>0}$ (n_i minimal) with $M_{p_i^{n_i}} \neq \{0\}$.

Furthermore: $M_{p_i^{n_i}} \simeq R/(p_i^{v_1^{(i)}}) \oplus \cdots \oplus R/(p_i^{v_{s_i}^{(i)}})$

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_i.

Classification Thm v2: $M \simeq R/(q_1) \oplus \cdots \oplus R/(q_r)$ where $q_i \neq 0$, $q_i \notin R^\times$ $\forall i$.

& $q_1 | q_2 | \cdots | q_r$. Furthermore, the sequence of ideals $(q_1), \ldots, (q_r)$ is unique.

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))

Main results: Rational normal form decomposition for $\mathrm{Mat}_{n\times n}(\mathbb{K})$

Jordan canonical form for $\mathrm{Mat}_{n\times n}(\overline{\mathbb{K}})$ eg $\overline{\mathbb{K}} = \mathbb{C}$.

$\mathbb{K}[x]$- 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)

Def $A, C \in \mathrm{Mat}_{n\times n}(\mathbb{K})$: $A \sim C \iff \exists\, G \in GL_n(\mathbb{K})$ st $A = G^{-1} C\, G$

The minimal polynomial of A

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

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

- 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. + $\mathbb{K}$-linear
- $\mathrm{Im}\,\Psi$ = subring of $\mathrm{End}_{\mathbb{K}}(V)$ generated by A & $\mathbb{K}$.
- $\mathrm{Ker}\,\Psi = ?$ Ideal of $\mathbb{K}[X]$ = PID so $\mathrm{Ker}\,\Psi = (f)$

Lemma: $\mathrm{Ker}\,\Psi \neq (0)$ ($\rightsquigarrow q_A$ = monic gen of $\mathrm{Ker}\,\Psi$ = minimal polynomial)

Pf/. $\mathrm{Im}\,\Psi = \mathbb{K}[A] \subseteq \mathrm{End}_{\mathbb{K}}(V) \simeq \underbrace{\mathrm{Mat}_{n\times n}(\mathbb{K})}_{\text{f. dim'l}} \Rightarrow \dim_{\mathbb{K}} \mathbb{K}[A] < \infty$

- Ψ $\mathbb{K}$-linear & $\dim_{\mathbb{K}} \mathbb{K}[X]$ infinite $\Longrightarrow \mathrm{Ker}\,\Psi \neq (0)$

$\square$

Cyclic case

Def V is <u>cyclic</u> (as $K[x]$-mod) if $\exists\, v \in V$ st $\{v, Av, A^2v, \dots\}$ spans V.

Proposition Assume $V \neq 0$ is cyclic. Then:

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

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

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

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

(2) Pick d minimal $A^d v \in \operatorname{Span}(\underbrace{\{v, Av, \dots, A^{d-1}v\}}_{li})$ & by induction on $k \geq 0$ $A^{d+k} v \in \operatorname{Span}(\{v, Av, \dots, A^{d-1}v\})$ $\Rightarrow$ $V \subseteq \operatorname{Sp}\{v, Av, \dots, A^{d-1}v\}$

$\Rightarrow$ Basis claim follows

(1) Write a nontrivial l.d relation:

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

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

Claim: $h = q_A$

Pf/ (1) $h \in \operatorname{Ker} \Psi$ ($h(A)_{(v)} = 0$, $h(A)(Av) \overset{A \,\&\, h(A) \text{ commute}}{=} A\underbrace{h(A)_{(v)}}_{=0} = 0$,

$\ldots\ h(A)(A^\ell v) \overset{A^\ell \,\&\, h(A) \text{ commute}}{=} A^\ell \underbrace{h(A)(v)}_{=0} = 0. \rightsquigarrow h(A)\big|_V = 0$)

$\{A^\ell v\}_{\ell \geq 0}$ spans V

$\Rightarrow h = q_A\, g$ 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!

Conclude: $\deg q_A = \deg h$, $q_A \mid h$ & both are monic $\Rightarrow q_A = h$. $\square$

Corollary 1: If V is cyclic and $q_A = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then in the basis $B = \{v, Av, \ldots A^{d-1}v\}$ we have

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

(Characteristic poly $= q_A$)

Corollary 2: 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 & $\operatorname{Ker}\varphi = (q_A(x))$)
$f(x) \longmapsto f(v)$

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

(**Reason:** -Problem 6 HW10 $\mathbb{K}[x]/(f) \simeq \mathbb{K}[x]/(g) \iff \deg f = \deg g$ (same dim!))

Q: What happens in the non-cyclic case?

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

Why? $q_A(A) = 0 \in \operatorname{End}_{\mathbb{K}}(V)$, meaning $q_A(A)(w) = 0 \ \forall w \in V$

$\Rightarrow \operatorname{Ann}(V) \supseteq (q_A(x)) \neq (0)$.

A: Classification Theorems for fg Torsion modules / $\mathbb{K}[x]$.

Rational normal forms

Theorem 1: V $\mathbb{K}$-vector space & $A \in \mathrm{End}_{\mathbb{K}}(V)$ $A \neq 0$. Then,
V admits a direct sum decomposition:

$$V = V_1 \oplus \cdots \oplus V_r$$

where each V_i is a cyclic $\mathbb{K}[x]$-module with invariants $q_i \neq 0$, satisfying $q_1 \mid q_2 \mid \cdots \mid q_r$

Furthermore, the sequence $(q_1, \ldots, q_r)$ 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) $\square$

Corollary: V admits a basis $\mathcal{B}$ with

$$[A]_{\mathcal{B}\mathcal{B}} = \begin{bmatrix} C_{q_1} & & 0 \\ & \ddots & \\ 0 & & C_{q_r} \end{bmatrix} \qquad C_{q_i} = \text{companion matrix for } q_i$$

This is known as the rational normal form for A. ($A \sim RNF(A)$)

Pf/ Pick v_i generator for V_i $\leadsto$ $\mathcal{B}_i = \{v, Av, \ldots, A^{d_i-1}v\}$ with $d_i = \deg q_i$. Then, take $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_r$. $\square$

Q: What about alternative Classification Thm?

We factor $q_A(x) = p_1^{n_1}(x) \cdots p_s^{n_s}(x)$ into distinct monic prime powers (Everything is monic, so no unit is needed in the factorization)

Theorem $V = V_{p_1^{n_1}} \oplus \cdots \oplus V_{p_r^{n_r}}$ & each $V_{p_i^{n_i}}$ decomposes further as

$$V_{p_i^{n_i}} \cong \bigoplus_{j=1}^{s_i} \mathbb{K}[x] / (p_i^{\nu_j^{(i)}}) \qquad n_i = \nu_1^{(i)} \geq \cdots \geq \nu_{s_i}^{(i)} \qquad (\text{sequence } \nu_j^{(i)} \text{ is unique})$$

Jordan canonical form

Assume $\mathbb{K} = \overline{\mathbb{K}}$, char 0 (Eg $\mathbb{K} = \mathbb{C}$) Then $p_i \in \mathbb{K}_{[x]}$ irred & monic $\Rightarrow p_i = (x-\alpha)$

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

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

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

Pf/

- Claim $B = \{w, (A-\alpha)w, \ldots, (A-\alpha)^{m-1}w\}$ is a basis for $W_{p_i,m}$
  - LI: $(x-\alpha)^m$ is the minimal polynomial of W_{p_i}s. $(*)$
    (Any dependency will yield a polynomial g with $g(A)|_{W_{p_i m}} = 0$.)
  - $\dim W_{p_i,m} = m = |B|$.

- Note: $(A-\alpha)^{k+1}(w) = (A-\alpha)((A-\alpha)^k(w))$ yields
  $A(A-\alpha)^{k+1}(w) = (A-\alpha)^{k+1}(w) + \alpha(A-\alpha)^k(w)$
  $(A-\alpha)^m(w) = 0$ by $(*)$
  $\Rightarrow [A|_{W_{p_i,m}}]_B = J(\alpha, m)$. $\square$

Corollary: Given V & A with $q_A = p_1^{n_1} \cdots p_r^{n_r}$, $\exists$ B basis for V s.t.

$$[A]_B = \begin{bmatrix} \boxed{A_1} & & 0 \\ & \ddots & \\ 0 & & \boxed{A_r} \end{bmatrix}$$

block diagonal decomp.

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

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

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

- This block decomposition is the Jordan canonical form of A