Lecture 33: Jordan canonical forms, Cayley-Hamilton Theorem

Recall A $\mathbb{K}[x]$-module M = a $\mathbb{K}$-vector space V $(= M \text{ as a set})$ and a $\mathbb{K}$-linear map $f : V \xrightarrow{x\cdot} V$

If $\dim_{\mathbb{K}} V < \infty$ and f is represented by a matrix A, then the $\mathbb{K}$-linear map

$$\Psi : \mathbb{K}[x] \longrightarrow \mathrm{End}_{\mathbb{K}}(V), \quad p \longmapsto p(A)$$

has $\ker(\Psi) = (q_A) \subseteq \mathbb{K}[x]$
↳ monic

Name: q_A = minimal polynomial for A. & M is a $\mathbb{K}[x]$-torsion module.

• Classification v2: $\Rightarrow$ $M \simeq \mathbb{K}[x]/(q_1) \oplus \cdots \oplus \mathbb{K}[x]/(q_r)$ with $q_r \mid q_{r-1} \mid \cdots \mid q_1$

Theorem 1: V admits a basis B over $\mathbb{K}$ 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 $q_i = \sum_{i=1}^{n_i} a_i x^i$, $a_{n_i} = 1$

$$= \begin{bmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & & \vdots \\ & & 1 & -a_{n_i-1} \end{bmatrix}$$

This is know as the rational normal form for A.
($A \sim \mathrm{RNF}(A)$ where $A \sim C$ iff $\exists\, Q \in GL_n(\mathbb{K})$ with $A = Q^{-1} C Q$)

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 $\mathbb{K}[x]$. Choose them to be monic.

• Everything is monic, so no unit is needed in the factorization.

Theorem 2: 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 $n_i = \nu_1^{(i)} \geq \cdots \geq \nu_{s_i}^{(i)}$)

§1. 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: $\mathcal{B} = \{\omega, (A-\alpha)\omega, \ldots, (A-\alpha)^{m-1}\omega\}$ 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: $(A-\alpha)^{k+1}(\omega) = (A-\alpha)\left((A-\alpha)^k(\omega)\right)$ yields

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

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.

§2 Characteristic polynomial:

Fixed V an n-dim'l $\mathbb{K}$-vector space & $A: V \longrightarrow V$ a k-linear map. We have

$$K[X] \longrightarrow K[A]$$
$$X \longmapsto A$$

Def: We define the characteristic polynomial of A as

$$\chi_A = \det(x I_n - A)$$

Obs: If $A \sim C$, meaning $C = G^{-1} A G$ for $G \in GL_n(\mathbb{K})$, then, $\chi_C = \chi_A$.

Indeed: $\chi_C = \det(x I_n - G^{-1} A G)$

$$= \det(G^{-1}(x I - A) G) = \det G^{-1} \det(x I_n - A) \det G$$

$$= \chi_A$$

Lemma: If $\varphi: \mathbb{K} \longrightarrow \mathbb{K}'$ is a homomorphism of rings between 2 fields, then: $\chi_{\varphi(M)} = \varphi(\chi_M)$

(Here, φ extends to $\varphi: \mathbb{K}[x] \longrightarrow \mathbb{K}'[x]$)

Proof: Exercise.

§3 Cayley-Hamilton:

Theorem (Cayley-Hamilton) $\chi_A(A) = 0$ (ie $q_A \mid \chi_A$)

We'll see two proofs:

1. Via Rational Normal forms
2. Show: $\chi_A(A)(v) = 0$ $\forall v \in \mathbb{K}^n \setminus \{0\}$ via $[A]_{BB} = \begin{array}{c} \\ d \end{array}\left[\begin{array}{c|c} \overset{d}{A_1} & A_2 \\ \hline 0 & A_3 \end{array}\right]$

   $B = \underbrace{\{v, Av, \ldots A^{d-1}v\}}_{\text{li (d maxl)}} \cup B'$ & use $\chi_A = \chi_{A_1} \cdot \chi_{A_3}$.

Key: $\chi_{C_q} = q$ for any $q \in \mathbb{K}[x]$ monic (C_q = companion matrix for q)

Proof 1: We'll use the Rational Normal form of A.

$$[A]_{BB} = \begin{bmatrix} C_{q_1} & & \\ & \ddots & \\ & & C_{q_r} \end{bmatrix} \qquad q_1 \mid q_2 \mid \cdots \mid q_r = q_A.$$

$$\det(xI_n - A) = \det \begin{bmatrix} xI_n - C_{q_1} & & 0 \\ & \ddots & \\ 0 & & xI_n - C_{q_r} \end{bmatrix}$$

$$\underset{\text{block decomp}}{=} \chi_{C_{q_1}} \cdots \underbrace{\chi_{C_{q_r}}}_{= q_r \text{ by Lemma below.}}$$

So $q_A \mid \chi_A$. $\square$

Lemma: $\chi_{C_f} = f$ for any monic polynomial $f \in \mathbb{K}[x]$.

Pf/ By induction on degree of f

- $\deg f = 1$: $\quad \chi_{C_{x+a_0}} = \det(x+a_0) = x+a_0 \qquad C_{x+a_0} = [-a_0]$

- $\deg f = m \rightsquigarrow f = x^m + a_{m-1}x^{m-1} + \cdots + a_0$

$$C_f = \begin{bmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 0 & \\ & & 1 & -a_{m-1} \end{bmatrix} \rightsquigarrow xI_m - C_f = \begin{bmatrix} x & 0 & \cdots & & a_0 \\ -1 & x & & & a_1 \\ & -1 & x & & a_2 \\ & & \ddots & \ddots & \vdots \\ & & & -1 & x+a_{m-1} \end{bmatrix}$$

$\det(xI_m - C_f)$ is computed by column expansion :

$$\chi_{C_f} = x \underbrace{\det \begin{bmatrix} x & & \cdots & a_0 \\ -1 & x & & a_1 \\ & \ddots & x & \vdots \\ & & -1 & x+a_{m-1} \end{bmatrix}}_{\begin{array}{c} \parallel \\ \chi_{C_{\frac{f-a_0}{x}}} \end{array}} + 1 \underbrace{\det \begin{bmatrix} 0 & 0 & \cdots & a_0 \\ -1 & x & & a_1 \\ 0 & -1 & x & \\ & & \ddots & x \\ & & -1 & x+a_{m-1} \end{bmatrix}}_{(-1)^{m-1+1} a_0 \underbrace{\det \begin{bmatrix} -1 & x & \cdots & 0 \\ 0 & -1 & x & \\ & & \ddots & x \\ & & & -1 \end{bmatrix}}_{=(-1)^{m-2}}}$$

$$= x \ \chi_{C_{\frac{f-a_0}{x}}} + (-1)^{2m-2} a_0$$

$$\underset{\text{IH}}{=} x \ \frac{f-a_0}{x} + a_0 = f(x) - a_0 + a_0 = f(x) \qquad \square$$

Proof 2: To show: $\chi_A(A)(v) = 0 \quad \forall v$ in V.

Pick any $v \in V$ & consider $V' = K[A] \cdot v$ that is, the vector space spanned by $\{v, Av, A^2v, \dots\}$.

- We know we can find d with $B' = \{v, Av, \dots, A^{d-1}v\}$ a basis for V'. Assume $\dim V = n$.
- We extend B' to a basis B of V. Then we get

$$[A]_{BB} = \begin{array}{c} \\ d \\ n-d \end{array}\left[\begin{array}{c|c} \overset{d}{A_1} & \overset{n-d}{A_2} \\ \hline 0 & A_3 \end{array}\right] \quad \text{where } A_1 = \begin{bmatrix} 0 & & 0 & -a_0 \\ 1 & 0 & & \vdots \\ & 1 & \ddots & \vdots \\ 0 & & 1 & -a_{d-1} \end{bmatrix}$$

So $A_1 = C_{q_{A|_{V'}}}$.

Then using the same block decomposition, we get.

$$\chi_A = \chi_{A_1} \cdot \chi_{A_3} \underset{\text{Lemma}}{=} q_{A|_{V'}} \cdot \chi_{A_3} = \chi_{A_3}\, q_{A|_{V'}}$$

So
$$\chi_A(A)(v) = \left(\chi_{A_3}(A) \cdot q_{A|_{V'}}(A)\right)(v)$$
$$= \chi_{A_3}(A)\Big(\underbrace{q_{A|_{V'}}(A)(v)}_{=0 \ (v \in V')}\Big) = 0$$

$\square$

Obs: The result is true for matrices over any commutative ring R.
We can show this by proving the polynomial

$$\chi_A(X) = X^n + b_{n-1}X^{n-1} + \dots + b_0 \quad \text{where } b_i \in \mathbb{Z}[a_{ij}]$$

vanishes on $A = (a_{ij})$ inside a dense open set of $\mathrm{Mat}_{n\times n}(\mathbb{R})$.
We can pick diagonalizable matrices as such set.

$\square$

- Alternative proof: Using Cofactor matrices (see HW11)