Lecture 33: More on Cayley-Hamilton, Basics in Linear Algebra

Recall: Last time we discussed Cayley-Hamilton for $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$

Theorem (Cayley-Hamilton) $\chi_A(A) = 0$ (i.e. $q_A \mid \chi_A$)

We saw two proof:

$\chi_A = \det(xI_n - A) \in \mathbb{K}[x]$. monic, degree n.

① via Rational Normal form

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

$B = \{\underbrace{v, Av, \dots A^{d-1}v}_{\text{li (} d \text{ max)}}\} \cup B'$ & 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)

TODAY: ① Consequences of Cayley-Hamilton.

② Basics in Linear Algebra ($\oplus$, Hom's, duals).

Consequences of Cayley-Hamilton

Corollary 1: Given $A \in \mathrm{Mat}_{n\times n}(\mathbb{K})$, $\exists\, C \in \mathrm{Mat}_{n\times n}(\mathbb{K})$ with $AC = CA = \det(A)\, I_n$.

If $q_0 = \chi_A(0) = \det(-A) = (-1)^n \det A$

Cayley-Hamilton gives $\chi_A(A) = A^n + q_{n-1}A^{n-1} + \cdots + q_0 I_n = 0$

$$\Rightarrow \underbrace{-q_0 I_n}_{(-1)^{n+1}\det A\, I_n} = A\underbrace{\left(A^{n-1} + q_{n-1}A^{n-2} + \cdots + q_1 I_n\right)}_{C'} = C'A$$

(A commutes with C'.)

So $C = (-1)^{n+1} C'$ works.

Obs: $C^T = \mathrm{Cof}(A) =$ **cofactor matrix of A** also works (We'll see this in a future lecture)

Here: $(\mathrm{Cof}(A))_{ij} = (-1)^{i+j} \det\left(A^{(i,j)}\right)$

↳ A with row i & col j removed.

(If $\det(A) \neq 0$, $\mathrm{Cof}(A) = C^T$ in Corollary 1)

Ex: Verify Corollary 1 for $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Fix R a commutative ring.

Corollary 2: Given $A \in \mathrm{Mat}_{n\times n}(R)$, $\exists\, C \in \mathrm{Mat}_{n\times n}(R)$ with

$$AC = CA = \det(A)\, I_n.$$

PF/ If C^T is the cofactor matrix of A, then $AC = CA = \det(A)$

This becomes a polynomial identity on $\mathbb{Z}[a_{ij}]$. So it's valid over any commutative ring (ie $\forall$ any $A \in \mathrm{Mat}_{n\times n}(R)$).

Remark: CH works over $\mathrm{Mat}_{n\times n}(R)$, (HW 11, Problem 18)

Proof uses the cofactor identity on $B = xI_n - A$.

Corollary 3: $A \in \mathrm{Mat}_{n\times n}(R)$ is invertible if and only if $\det A \in R^\times$

PF/ ($\Rightarrow$) Is clear since $\det(AB) = \det A \det B$ & $\det I_n = 1$.

($\Leftarrow$) Use $AC = CA = (\det A) I_n$ from Corollary 2

Then $A^{-1} = (\det A)^{-1} C$. $\square$

Nakayama's Lemma Fix $(R, \mathfrak{m})$ local commutative ring and let M be a finitely generated R-module. If $\mathfrak{m}M = M$, then $M = 0$.

Pf/ Write $M = \langle x_1, \dots, x_n \rangle$ Then $\mathfrak{m}M = \left\{ \sum_{j=1}^{n} c_j x_j \;\; c_j \in \mathfrak{m} \right\}$

In particular $x_i \in M = \mathfrak{m}M \Rightarrow$: $x_i = \sum_{j=1}^{n} c_{ij} x_j$ with $c_{ij} \in \mathfrak{m}$.

Then $A = I_n - (c_{ij}) \in \mathrm{Mat}_{n\times n}(R)$ satisfies

$$A \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} - (c_{ij}) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} - \begin{bmatrix} \sum_{j=1}^{n} c_{1j} x_j \\ \vdots \\ \sum_{j=1}^{n} c_{nj} x_j \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Pick F with $FA = AF = (\det A) I_n$. Then:

$$\left.\begin{array}{l} FA \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = F \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \\ \| \\ (\det A) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \end{array}\right\} \Rightarrow \begin{array}{l} (\det A)\, x_1 = 0 \\ \vdots \\ (\det A)\, x_n = 0 \end{array} \left.\begin{array}{l} \\ \\ \Rightarrow \det A \in R^\times \end{array}\right\} \Rightarrow x_1 = \cdots = x_n = 0 \Rightarrow M = 0$$

But $\det A = \det\left(I_n - \overbrace{(c_{ij})}^{\in \mathfrak{m}\,\mathrm{Mat}_{n\times n}(R)}\right) \in 1 + \mathfrak{m}$ □

(See HW12 #2 for other versions of Nakayama's Lemma.)

Linear Algebra Basics

$\mathbb{K}$ = field

TODAY: Review basis, direct sums, Hms & duals

NEXT TIME: Tensor products, symmetric & alternating (or exterior) products

Definition: A vector space over $\mathbb{K}$ is a (free) $\mathbb{K}$-module, that is

- A set V with 3 operations

$$+ : V \times V \longrightarrow V, \quad (v_1, v_2) \longmapsto v_1 + v_2$$

$$V \longrightarrow V, \quad v \longmapsto -v$$

} V becomes an abelian gp with 0 as the identity element

&

$$\mathbb{K} \times V \longrightarrow V \quad \text{(scalar multiplication)}$$
$$(z, v) \longmapsto zv$$

satisfying:

- $z(v_1 + v_2) = zv_1 + zv_2$
- $(z_1 + z_2)v = z_1 v + z_2 v$ } (Distributive)
- $z_1(z_2 v) = (z_1 z_2)v$ (Associative)
- $1_{\mathbb{K}} \cdot v = v$.

$\forall\, z, z_1, z_2 \in \mathbb{K}$, $\forall\, v, v_1, v_2 \in V$.

Hom-spaces

Def: A $\mathbb{K}$-linear map between 2 vector spaces is a group homomorphism $f: V \longrightarrow W$ s.t. $f(z \cdot v) = z f(v)$ $\forall z \in \mathbb{K}$. (Hmm of $\mathbb{K}$-modules!)

$\boxed{\mathrm{Hom}_{\mathbb{K}}(V, W)}$ = set of all linear maps from V to W

Prop: $\mathrm{Hom}_{\mathbb{K}}(V, W)$ is a $\mathbb{K}$-vector space:

PF/ ① $\forall f_1, f_2 \in \mathrm{Hom}_{\mathbb{K}}(V, W)$, $f_1 + f_2$ is defined as

$$(f_1 + f_2)_{(v)} = f_1(v) + f_2(v) \qquad \forall v \in V$$

(Easy to check: this new map $f_1 + f_2 : V \longrightarrow W$ is $\mathbb{K}$-linear)

② Zero map: $0 \in \mathrm{Hom}_{\mathbb{K}}(V, W)$ $\quad 0 : v \longmapsto 0 \quad \forall v \in V$.

③ Scalar multiplication: $\forall z \in \mathbb{K}$, $f \in \mathrm{Hom}_{\mathbb{K}}(V, W)$:

$(zf) : V \longrightarrow W \qquad (zf)_{(v)} = z f(v)$.

(Easy to check: this new map $z \cdot f : V \longrightarrow W$ is $\mathbb{K}$-linear)

Distributive & Associative Laws follow from Those on W; $1 \cdot f =$ is clear $\square$

Note: We never really used the vector space structure of V in the definition of the vector space structure on $\mathrm{Hom}_{\mathbb{K}}(V,W)$. The same idea would work to make $\mathrm{Hom}_{\mathrm{set}}(X,W)$ a vector space when X is any set & W is a $\mathbb{K}$-vector space.

Remark: If V & W are finite-dimensional, with $\dim V = n$, $\dim W = m$, then $\mathrm{Hom}_{\mathbb{K}}(V,W)$ can be identified with $\mathrm{Mat}_{m\times n}(\mathbb{K})$

- Choose bases (ordered!) $B_V = \{v_i\}_{i=1}^n$ & $B_W = \{w_j\}_{j=1}^m$ for V & W, respectively. Then, $f \in \mathrm{Hom}_{\mathbb{K}}(V,W)$ can be expressed as $f(v_i) = \sum_{j=1}^{m} a_{ji} w_j$ $\rightsquigarrow A = (a_{ji})_{\substack{j=1,\dots,m \\ i=1,\dots,n}} \in \mathrm{Mat}_{m\times n}(\mathbb{K})$

Furthermore $[f(v)]_{B_W} = A\,[v]_{B_V}$ ($[\,]_{B_W} \in \mathbb{K}^m$, $[\,]_{B_V} \in \mathbb{K}^n$)

Notation $A = [f]_{B_V B_W}$.

Bases for vector spaces

Def: B is a basis for V if $\begin{cases} \cdot\ B \text{ is linearly independent} \\ \cdot\ B \text{ spans } V \end{cases}$

$\rightsquigarrow V \cong \bigoplus_{v \in B} \mathbb{K}$.

- Equivalently every v in V can be written uniquely as a linear comb. of elements in B
- Equivalently: B is maximal linearly independent set (HW12)

Obs: By HW10 - Problem 2, any 2 maximal linearly indep sets have the same cardinality. So $\dim V$ = size of any basis for V.

Theorem: Let V be a vector space over a field $\mathbb{K}$ with $V \neq \{0\}$.

① Let S be a li subset of V. Then there exists a basis B for V with $S \subset B$

② Let Γ be a generating set for V (ie a spanning set). Then, there exists a basis B of V with $B \subset \Gamma$.

Pf / $\dim V = n < \infty$, use induction on n / $|\Gamma|$; $\dim V$ infinite, use Zorn's Lemma (HW12)

Direct Sums

(Same works for free modules over a commutative ring (use rank!))

Let V_1 & V_2 be two vector spaces. ($V_1 \oplus V_2$ = same def as for R-modules)

Def: $V_1 \oplus V_2$ denotes the vector space with underlying set the cartesian product $V_1 \times V_2$ & the following structure:

① $(v_1, v_2) + (v_1', v_2') = (v_1 + v_1', v_2 + v_2')$
② $-(v_1, v_2) = (-v_1, -v_2)$
③ $z(v_1, z_2) = (zv_1, zv_2)$

} same as for groups

Def If $f_1 : V_1 \longrightarrow W_1$, $f_2 : V_2 \longrightarrow W_2$ we set $f = f_1 \oplus f_2 : V_1 \oplus V_2 \longrightarrow W_1 \oplus W_2$
$(v_1, v_2) \longmapsto (f_1(v_1), f_2(v_2))$

Obs: If $\dim V_i = n_i < \infty$ & $\dim W_i = m_i < \infty$

- $B_V = (B_{V_1} \times \{0\}) \cup (\{0\} \times B_{V_2})$ is a basis for $V_1 \oplus V_2$
- $B_W = (B_{W_1} \times \{0\}) \cup (\{0\} \times B_{W_2})$ ——— $W_1 \oplus W_2$

& $[f]_{B_V B_W} = \left[\begin{array}{c|c} [f_1]_{B_{V_1} B_{W_1}} & 0 \\ \hline 0 & [f_2]_{B_{V_2} B_{W_2}} \end{array}\right] \in \mathrm{Mat}_{(m_1+m_2)\times(n_1+n_2)}(\mathbb{K})$

(n_1 columns, n_2 columns; m_1 rows, m_2 rows)

Dual Vector Spaces

V = $\mathbb{K}$-vector space

Def The dual of V, denoted by V^*, is defined as: $V^* = \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$ (1-dim'l vector space.)

Theorem 4: If V is finite-dimensional, then $\dim V^* = \dim V$.

Pf/ Let $\{v_i\}_{1 \le i \le m}$ be a basis for V. Define $v_i^* \in V^*$ by

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \qquad \left(v_i^*\left(\sum_{j=1}^m a_j v_j\right) = a_i \in \mathbb{K} \text{ is } \mathbb{K}\text{-linear} \checkmark \right)$$

Claim: $\mathcal{B}^* = \{v_i^*\}_{1 \le i \le m}$ is a basis for V^* (dual basis)

① **$\mathcal{B}^*$ is li:** $\sum_{i=1}^m a_i v_i^* = 0 : V \to \mathbb{K} \Rightarrow 0 = \left(\sum_{i=1}^m a_i v_i^*\right)_{(v_j)} = a_j \ \forall j$

(a_i: scalars in $\mathbb{K}$)

② **$\mathcal{B}^*$ spans:** Given $f : V \to \mathbb{K}$ linear, it's uniquely determined by its values at $\mathcal{B}$: $f\left(\sum_{i=1}^m a_i v_i\right) = \sum_{i=1}^m a_i \underbrace{f(v_i)}_{= b_i}$

Then: $f = \sum_{i=1}^m b_i v_i^*$ $\left[f(v_j) = \sum_{i=1}^m b_i v_i^*(v_j) = \sum_{i=1}^m b_i \delta_{ij} = b_j \ \forall j \right]$ □

⚠ Claim fails when V is infinite-dimensional. (① holds, ② fails)

Example: Pick $V = \mathbb{K}^{\oplus \mathbb{N}}$ $\mathbb{K}$-v.space with basis $\{e_k : k \in \mathbb{N}\}$

$\exists\ f: V \longrightarrow \mathbb{K}$ linear map with $f(e_k) = 1\ \forall k$.

$$f\Big(\sum_{\substack{i\in\mathbb{N}\\ \text{finite}}} a_i e_i\Big) = \sum_{\substack{i\in\mathbb{N}\\ \text{finite}}} a_i$$

But $f \notin \mathrm{Span}\{e_k^* : k \in \mathbb{N}\}$

Obs 1: If V has a basis $B = \{v_i : i \in I\}$, then:

$$V = \Big\{\sum_{i\in I} a_i v_i : a_i = 0 \text{ for all but finitely many } i\Big\}$$

$$V^* = \Big\{\sum_{i\in I} a_i v_i^*\Big\} \supseteq \Big\{\sum_{i\in I} a_i v_i^* \ : a_i = 0 \text{ for all but fin many } i\text{'s}\Big\}$$

$V^* = \prod_I \mathbb{K}$; $\supseteq$ is $\neq$ if $|B| = \infty$. ; $\cong \bigoplus_I \mathbb{K}$

Obs 2 Similarly if R is a commutative ring, and M is a free R-mod, we can define $M^* = \mathrm{Hom}_R(M, R)$. It turns out that M^* is also a free module over R if $\mathrm{rank}(M) < \infty$ Moreover, $\mathrm{rk}(M^*) = \mathrm{rk}(M) < \infty$ (Same proof works!)

If $\mathrm{rank}(M)$ is infinite, M^* need not be free! ($M = \mathbb{Z}^{\oplus \mathbb{N}}$, $M^* = \prod_{n\in\mathbb{Z}} \mathbb{Z}$.)