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:

① via Rational Normal form

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

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

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)

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

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

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

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

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 $M = 0$.

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. $f(z \cdot v) = z f(v) \quad \forall z \in \mathbb{K}$. (Hmm of $\mathbb{K}$-modules!)

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

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

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 $B \subset \Gamma$.

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 $f = f_1 \oplus f_2 : V_1 \oplus V_2 \longrightarrow W_1 \oplus W_2$

Dual Vector Spaces

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

Def The dual of V, denoted by V^*, is defined as: $V^* = \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K})$

($\mathbb{K}$: 1-dim'l vector space.)

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

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

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

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

$$V^* = \left\{ \sum_{i \in I} a_i v_i^* \right\} \geq \left\{ \sum_{i \in I} a_i v_i^* \quad a_i = 0 \text{ for all but fin many } i\text{'s} \right\}$$

$\neq$ if $|B| = \infty$.

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!