Lecture 34: Nakayama's Lemma, Basics on Linear Algebra

Recall: Last time we discussed Cayley-Hamilton for $A \in Mat_{n\times n}(R)$ R any comm ring

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

§1 Consequences of Cayley-Hamilton:

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

Pf/ $a_0 = \chi_A(0) = \det(-A) = (-1)^n \det A$

CH gives $\chi_A(A) = A^n + a_{n-1}A^{n-1} + \dots + a_0 I_n = 0$

$$\Rightarrow \underset{\substack{\| \\ (-1)^{n+1}\det A\, I_n}}{-a_0 I_n} = A\big(\underbrace{A^{n-1} + a_{n-1}A^{n-2} + \dots + a_1 I_n}_{C'}\big) = C'A$$

A commutes with C'!

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

Obs: $C^T = Cof(A)$ = cofactor matrix of A with
$$(Cof(A))_{ij} = (-1)^{i+j}\det(A^{(i,j)})$$
↳ A with row i & col j removed.

(We'll see this in a future lecture)

Ex: $n=2$ $\quad A = \begin{bmatrix} a & b \\ c & d\end{bmatrix}$

$$\chi_A = \det\begin{pmatrix} x-a & -b \\ -c & x-d\end{pmatrix} = (x-a)(x-d) - bc$$
$$= x^2 - \underbrace{(a+d)}_{tr(A)}x + \underbrace{ad-bc}_{\det A}$$

$$\chi_A(A) = A^2 - (a+d)A + (ad-bc)I_2$$
$$= \begin{bmatrix} a^2+bc & b(a+d) \\ c(a+d) & cb+d^2\end{bmatrix} - \begin{bmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d\end{bmatrix} + \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc\end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad ✓$$

$$C = (-1)^3 (A - (a+d) I_2) = -\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a+d & 0 \\ 0 & a+d \end{bmatrix}$$
$$= \begin{bmatrix} +d & -b \\ -c & +a \end{bmatrix} = \mathrm{Cof}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)^T$$

Next: 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 $AC = CA = \det(A) I_n$
This yields a polynomial identity on $\mathbb{Z}[a_{ij}]$. So it's valid over any commutative ring! $\square$

- This Corollary gives the general version of CH (see HW11)

Theorem 2 (CH) For any R comm ring & $A \in \mathrm{Mat}_{n\times n}(R)$, we have $\chi_A(A) = 0$.

Proof: Show $\chi_A(A) = 0$ by using cofactor identity on $B = xI_n - A$ & setting $x = A$ ($B\,\mathrm{Cof}^T B = \mathrm{Cof}^T B \cdot B = \det B\, I = \chi_A(x) I_n$) $\square$

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 using $\det(AB) = \det A \det B$ & $\det I_n = 1$.
($\Leftarrow$) 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 $M = \langle x_1, \ldots, x_n \rangle$. Then, $\mathfrak{m} M = \{ \sum_{j=1}^{n} c_j x_j \quad c_j \in \mathfrak{m} \}$

In particular $x_i \in M = \mathfrak{m} M$ so:

$$x_i = \sum_{j=1}^{n} c_{ij} x_j \qquad \text{with } c_{ij} \in \mathfrak{m}.$$

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 $FA = AF = (\det A) I_n$. (eg $F = \mathrm{Cof}(A)^T$) Then:

$$(\det A) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = FA \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = F \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \Rightarrow \begin{cases} (\det A)\, x_1 = 0 \\ \quad \vdots \\ (\det A)\, x_n = 0 \end{cases}$$

But $\det A = \det(I_n - \underbrace{(c_{ij})}_{\in \mathfrak{m}}) \in 1 + \mathfrak{m}$, so it's a unit.

$\Rightarrow$ Conclude: $x_1 = \cdots = x_n = 0$ so $M = \{0\}$. $\square$

(See HW11 for other versions of Nakayama's Lemma.)

§2. Linear Algebra Basics:

Fix $\mathbb{K}$ a field. Next, we review the basic operations on vector spaces over $\mathbb{K}$: Direct sums, Homs, Dual Vector Spaces

Next Time: Tensor products, Symmetric & Alternating (or Exterior) products

§2.1 Vector Spaces, Linear Maps:

Definition: A vector space over $\mathbb{K}$ is a set V together with 3 operations

$$\left.\begin{array}{ll} + : V \times V \longrightarrow V, & V \longrightarrow V \\ \quad (v_1, v_2) \longmapsto v_1 + v_2 & v \longmapsto -v \end{array}\right\} \text{abelian gp with 0 as the identity element}$$

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

satisfying:
- $z(v_1+v_2) = zv_1 + zv_2$
- $(z_1+z_2)v = z_1 v + z_2 v$

$\Big\}$ (Distributive)

- $z_1(z_2 v) = (z_1 z_2) v$ (Associative)
- $1_{\mathbb{K}} \cdot v = v$.

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

Obs: V is a $\mathbb{K}$-module

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

Obs: Same definition as homomorphism 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; $1\cdot f = f$ 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 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 $\mathrm{Mat}_{m\times n}(\mathbb{K})$. This involves choosing 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 $f(v_i) = \sum_{j=1}^{m} a_{ji} w_j \rightsquigarrow A = (a_{ji})_{\substack{j=1,\ldots,m \\ i=1,\ldots,n}} \in \mathrm{Mat}_{m\times n}(\mathbb{K})$

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

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

§2.3 Bases:

We use the same definition as free-modules

Def: B is a basis for V if $V \simeq \bigoplus_{v\in B} \mathbb{K}$.

$\begin{cases} \bullet\ B \text{ is linearly independent} \\ \bullet\ B \text{ spans } V \end{cases}$

- Equivalently: every v in V can be written uniquely as a linear comb. of elements in B
- Equivalently: B is maximal linearly independent set (HW11)

Obs: By HW10 - Problem 6, any 2 maximal linearly indep sets have the same cardinality. So $\dim V$ = size of any basis for V.

The usual techniques to find a basis in a spanning set, & a basis for V by extending a linearly independent set hold in any dimension (see HW11.). The proof uses Zorn's Lemma:

Theorem 3: 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 $B \subset \Gamma$.

§2.2 Direct Sums:

Let V_1 & V_2 be two vector spaces.

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

$$\left.\begin{array}{l} ① \ (v_1, v_2) + (v_1', v_2') = (v_1 + v_1', v_2 + v_2') \\ ② \ -(v_1, v_2) = (-v_1, -v_2) \end{array}\right\} \text{same as for groups}$$

$$③ \ z(v_1, z_2) = (zv_1, zv_2)$$

This is the same definition as the one for modules / R.

• Linear maps & direct sums:

If $\begin{array}{l} f_1 : V_1 \longrightarrow W_1 \\ f_2 : V_2 \longrightarrow W_2 \end{array}$ are $\mathbb{K}$-linear maps, then we build a new map

$$f = f_1 \oplus f_2 \in \operatorname{Hom}_{\mathbb{K}}(V_1 \oplus V_2, W_1 \oplus W_2) \text{ via } f_{(v_1, v_2)} = (f_{1(v_1)}, f_{2(v_2)})$$

If V_1, V_2, W_1, W_2 are define dimensions ($\dim V_i = n_i$, $\dim W_i = m_i$)

• $B_V = (B_{V_1} \times \{0\}) \cup (\{0\} \times B_{V_2})$ is a basis for $V_1 \oplus V_2$

• $B_W = (B_{W_1} \times \{0\}) \cup (\{0\} \times B_{W_2})$ ——— $W_1 \oplus W_2$

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

Obs: Same will work for free modules over a comm ring with finite rank.

§2.3 Dual Vector Spaces:

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

Def The dual of V, denoted by V^*, is defined as:

$$V^* = \mathrm{Hom}_{\mathbb{K}}(V, \underbrace{\mathbb{K}}_{\text{1-dim'l vector space.}})$$

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

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

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

$\mathbb{K}$-linear.

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

① B^* spans:

Given $f: V \longrightarrow \mathbb{K}$ linear, it's determined uniquely by its values at B:

$$f\Big(\sum_{i=1}^m a_i v_i\Big) = \sum_{i=1}^m a_i \underbrace{f(v_i)}_{=b_i}$$

Then: $f = \sum_{i=1}^m b_i v_i^*$

$$\Big[\ f(v_j) = \sum_{i=1}^m b_i v_i^*(v_j) = \sum_{i=1}^m b_i \delta_{ij} = b_j\ \Big]$$

② B^* is l.i.:

$$\sum_{i=1}^{m} \underbrace{a_i}_{\text{scalars in } \mathbb{K}} v_i^* = 0 : V \longrightarrow \mathbb{K} \Rightarrow 0 = \Big(\sum_{i=1}^{m} a_i v_i^*\Big)_{(v_j)} = a_j \quad \forall j$$

□

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

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 $f \notin \operatorname{Span}(e_k^* : k \in \mathbb{N})$. □

Obs: Similarly if R is a commutative ring, and M is a free R-mod, we can define $M^* = \operatorname{Hom}_R(M, R)$. It turns out that M^* need not be free if $\operatorname{rk}(M)$ is infinite. (Eg $M = \mathbb{Z}^{\oplus \mathbb{N}}$, $M^* = \prod_{\mathbb{N}} \mathbb{Z}$ not free)
. If $\operatorname{rk}(M) < \infty$, M^* is free $\operatorname{rk}(M^*) = \operatorname{rk}(M) < \infty$ (Same proof works!)

Q: How to dualize a map?

Lemma: If $f : V \longrightarrow W$ is a linear map, then $f^* : W^* \longrightarrow V^*$ defined by $f^*(\xi) = \xi \circ f : V \longrightarrow W \longrightarrow \mathbb{K}$ $\forall \xi \in W^*$ is $\mathbb{K}$-linear

More precisely: $f^*(\xi)(v) = \xi(f(v)) \quad \forall v \in V, \ \forall \xi \in W^*$

Prop (HW 11): If $\dim V = n$, $\dim W = m$ then $[f^*]_{B_{W^*} B_{V^*}} = [f]^T_{B_V B_W}$.