Lecture 34: Nakayama’s Lemma, Basics in Linear Algebra
Recall: Last time we discussed Cayley–Hamilton for $A \in \text{Mat}_{n \times n}(\mathbb{R})$ meaning

**Theorem (Cayley–Hamilton)** $\chi_A(A) = 0$ i.e. $\text{tr} \chi_A = 0$

**51 Consequences of Cayley–Hamilton**:

**Corollary 1.** Given $A \in \text{Mat}_{n \times n}(K)$, $F \in \text{Mat}_{n \times n}(K)$ with $AC = CA = \det(A)I_n$. Then

$$\begin{align*}
\exists \theta = \chi_A(0) = \det(-A) = (-1)^n \det A
\end{align*}$$

CH gives $\chi_A(A) = A^n + a_{n-1}A^{n-1} + \ldots + a_1I_n = 0$

$$\Rightarrow -a_0I_n = A\left( A^{n-1} + a_{n-1}A^{n-2} + \ldots + a_1I_n \right) = C'A
$$

$(-1)^n \det A I_n$

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

**Obs:** $C^T = \text{Cof}(A) = \text{cofactor matrix of } A$ with $(\text{Cof}(A))_{ij} = (-1)^{i+j} \det(A^{(i,j)})$

(We’ll see this in a future lecture) $\Rightarrow A$ with row $i$ and col $j$ removed.

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

$$\chi_A = \det \begin{pmatrix} x-a & -b \\ -c & x-d \end{pmatrix} = (x-a)(x-d) + bc
$$

$$\chi_A(A) = A^2 - (a+d)A + (ad-bc)I_2
$$

$$= \begin{bmatrix} a^2 + bc & b(a+d) \\ c(a+d) & c(b+d) \end{bmatrix} - \begin{bmatrix} (a+d)a & (a+d)b \\ (a+d)c & (a+d)d \end{bmatrix} + \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$$
Next: Fix \( R \) a commutative ring. 

**Corollary 2:** Given \( A \in \text{Mat}_{n \times n}(R) \), \( \exists \ C \in \text{Mat}_{n \times n}(R) \) with 
\[
AC = CA = \det(A)I_n.
\]

**Proof:** If \( C \) is the cofactor matrix of \( A \), then \( AC = CA = \det(A)I_n \). This yields a polynomial identity on \( \mathbb{Z}[a_{i,j}] \). So it's valid over any commutative ring! 

This corollary gives the general version of CH (see HW11)

**Theorem 2 (CH):** For any commutative ring \( R \) and \( A \in \text{Mat}_{n \times n}(R) \), we have \( \chi_A(A) = 0 \).

**Proof:** Show \( \chi_A(A) = 0 \) by using cofactor identity \( m \)
\[
B = XI_n - A \text{ and setting } x = A(B) \text{ cof } B = C \text{ cof } B \text{ det } B \text{ cof } I_n = \chi_A(0)I_n \)

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

**Proof:** 
(\( \Rightarrow \)) is clear \( \det(AB) = \det A \det B \). \( \det I_n = 1 \).
(\( \Leftarrow \)) Use \( AC = CA = (\det A)I_n \) from Corollary 2

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

**Nakayama's Lemma:** Fix \( (R, M) \) local commutative ring and let \( M \) be a finitely generated \( R \)-module. If \( M M = M \), then \( M = 0 \).
Write $M = \langle x_1, \ldots, x_n \rangle$. Then, $MN = \{ \sum_{j=1}^{n} c_j x_j : c_j \in M \}$.

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

Then $A = I_n - (c_{ij}) \in \text{Mat}_{nxn}(\mathbb{R})$ satisfies

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

Pick $F$ with $FA = AF = (\det A) I_n$. (e.g. $F = (A^T)^{-1}$) Then:

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

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

$\Rightarrow$ conclude: $x_1 = \ldots = x_n = 0 \Rightarrow M = \{0\}$.

(See H111 for other versions of Nakayama's Lemma.)

§ 2. Linear Algebra Basics:

Fix $K$ a field. Next, we review the basic operations in vector spaces over $K$: Direct sums, Hom, Dual Vector Spaces

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

§ 2.1 Vector Spaces, Linear Maps:

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

$$+: V \times V \rightarrow V, \quad (v_1, v_2) \mapsto v_1 + v_2$$
$$-: V \rightarrow V, \quad v \mapsto -v$$

\{ abelian group with 0 as the identity element \}

$1K \times V \rightarrow V, \quad (1, v) \mapsto v$ (scalar multiplication)
satisfying: \[ \begin{align*}
& z (v_1 + v_2) = zv_1 + zv_2 \\
& (z_1 + z_2) v = z_1 v + z_2 v \\
& z_1 (z_2 v) = (z_1 z_2) v \\
& 1_{K} v = v.
\end{align*} \]

\[ \forall z, z_1, z_2 \in K, \forall v, v_1, v_2 \in V. \]

**Obs:** \( V \) is a \( K \)-module.

**Def:** A \( K \)-linear map between \( 2 \) vector spaces is a group homomorphism \( f: V \rightarrow W \) s.t. \( f(z \cdot v) = z f(v) \) \( \forall z \in K \).

**Obs:** Same definition as homomorphism of \( K \)-modules.

\[ \text{Hom}_K(V, W) = \text{set of all linear maps from } V \text{ to } W \]

**Prop:** \( \text{Hom}_K(V, W) \) is a \( K \)-vector space:

1. \( \forall f_1, f_2 \in \text{Hom}_K(V, W), f_1 + f_2 \) is defined as:
\[ (f_1 + f_2)(v) = f_1(v) + f_2(v) \quad \forall v \in V \]
(\text{Easy to check: this new map } f_1 + f_2: V \rightarrow W \text{ is } K\text{-linear})

2. \( \forall v \in V, 0 \in \text{Hom}_K(V, W), 0 \cdot v = 0 \text{ for all } v \in V. \)

3. \( \forall z \in K, \forall f \in \text{Hom}_K(V, W), (zf)(v) = z f(v). \)
(\text{Easy to check: this new map } zf: V \rightarrow W \text{ is } K\text{-linear})

Distributive and Associative Laws follow from these in \( W \); \( f \cdot 1 = f \) is clear \( \Box \).

**Note:** We never really used the vector space structure of \( V \) in the definition of the vector space structure on \( \text{Hom}_K(V, W) \). The same would work to make \( \text{Hom}_K(X, W) \), a vector space when \( X \) is any set & \( W \) is a \( K \)-vector space.
Remark: If \( V \) & \( W \) are finite-dimensional, with \( \dim V = n \), \( \dim W = m \), then \( \text{Hom}_K(V, W) \) can be identified with \( \text{Mat}_{m \times n}(K) \). This involves choosing bases \( B_V = \{ v_i \}_{i=1}^n \) & \( B_W = \{ w_j \}_{j=1}^m \) for \( V \) & \( W \), respectively. Then \( f \in \text{Hom}_K(V, W) \) can be expressed as \( f(v_i) = \sum_{j=1}^m a_{ji} w_j \). \( A = (a_{ji})_{i=1}^n_{j=1}^m \in \text{Mat}_{m \times n}(K) \).

Furthermore \( [f(v)]_{B_W} = A [v]_{B_V} \). \( A = [f]_{B_VB_W} \).

§ 2.3 Bases:

We use the same definition as free-modules.

**Def**: \( B \) is a basis for \( V \) if \( V \cong \bigoplus_{v \in B} K \).

\[
\begin{align*}
\cdot \ & B \text{ is linearly independent} \\
\cdot \ & B \text{ spans } V
\end{align*}
\]

Equivalently: every \( v \in V \) can be written uniquely as a linear combination of elements in \( B \).

Equivalently: \( B \) is maximal linearly independent set (HWII).

Obs: By HW10-Problem 6, any 2 maximal linearly independent sets have the same cardinality. So \( \dim V = \text{size of any basis for } V \).

The usual technique to find a basis in a spanning set, & a basis for \( V \) by extending a linearly independent set, hold in any dimension (see HWII). The proof uses Zorn's Lemma.
**Theorem 3:** Let $V$ be a vector space over a field $K$ with $V \neq 0$.  

1. Let $S$ be a linear subset of $V$. Then there exists a basis $B$ in $V$ with $S \subseteq B$.  
2. Let $\Gamma$ be a generating set for $V$ (i.e., a spanning set). Then there exists a basis $B$ of $V$ with $B \supseteq \Gamma$.

---

**§2.2 Direct Sums:**

Let $V_1$ and $V_2$ 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:

1. $(v_1, v_2) + (v'_1, v'_2) = (v_1 + v'_1, v_2 + v'_2)$ (same as for $\mathbb{Z}$)
2. $- (v_1, v_2) = (-v_1, -v_2)$
3. $z (v_1, v_2) = (zv_1, zv_2)$

This is the same definition as the one for modules / $\mathbb{R}$.

---

**Linear Maps and Direct Sums:**

If $f_1 : V_1 \to W_1$, $f_2 : V_2 \to W_2$ are $K$-linear maps, then we build a new map $f = f_1 \oplus f_2 \in \text{Hom}_K (V_1 \oplus V_2, W_1 \oplus W_2)$ via $f (v_1, v_2) = (f_1 (v_1), f_2 (v_2))$.

If $v_1, v_2, w_1, w_2$ are defined dimensions ($\dim V_i = n_i$, $\dim W_i = m_i$),

- $B_V = \{e_1 \times \{0\} \cup \{0\} \times e_2 \}$ is a basis for $V_1 \oplus V_2$,
- $B_W = \{e_1 \times \{0\} \cup \{0\} \times e_2 \}$ is a basis for $W_1 \oplus W_2$. 

---

(Continued text on the next page.)
Let \( V \) be a \( k \)-vector space.

**Def.** The dual of \( V \), denoted by \( V^* \), is defined as:

\[
V^* = \text{Hom}_k(V, k)
\]

\( \hat{V} \) is a \( k \)-dim vector space.

**Theorem.** If \( V \) is finite-dimensional, then \( \dim V^* = \dim V \).

**Proof.** Let \( \{v_i\}_{i=1}^m \) be a basis for \( V \). Define \( v_i^* \in V^* \) by

\[
v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \quad (v_i^* \left( \sum_{j=1}^m a_j v_j \right) = a_i \in k)
\]

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

**1.** \( v^* \) spans:

Given \( f: V \to k \) linear, it's determined uniquely by its values at \( \mathcal{B} \):

\[
f \left( \sum_{i=1}^m a_i v_i \right) = \sum_{i=1}^m a_i f(v_i) = \sum_{i=1}^m a_i v_i^* = b_i
\]

Then:

\[
f = \sum_{i=1}^m b_i v_i^*
\]

\[
\left[ f(v_j) = \sum_{i=1}^m b_i v_i^*(v_j) = \sum_{i=1}^m b_i \delta_{ij} = b_j \right]
\]
Lemma: If \( f : V \to W \) is a linear map, then \( f^* : W^* \to V^* \) defined by \( f^*(\xi) = \xi \circ f : V \to W \to K \) for all \( \xi \in W^* \) is \( K \)-linear. More precisely: \( f^*(\xi)(v) = \xi(f(v)) \) for all \( v \in V \), \( \xi \in W^* \).

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