MATH 510

Minimal polynomial.

Given linear map $T: V \to V$ where V is f.d., the subset

$$\{ Id = T^0, T, T^2, \ldots \} \subset End(V)$$

must be linearly dependent (since $\dim End(V) < \infty$)

Thus there exists a lin comb.

$$\sum_{k=0}^{N} \alpha_k T^k = 0$$

where at least one α_k is nonzero. Let $d \geq 0$ be the largest such k. Then

$$\sum_{k=0}^{d} \alpha_k T^k = 0$$

Now divide by α_d and put

$$c_k = \frac{\alpha_k}{\alpha_d}$$

We get

$$T^d + c_{d-1}T^{d-1} + \dots + c_1 T + c_0 \, Id_V = 0$$

in End(V). Put

$$f(x) = x^d + c_{d-1}x^{d-1} + \dots + c_1 x + c_0$$

Then we can write

$$f(T) = 0$$

Def

1) A pol $g(x) \in \mathbb{F}[x]$ is monic if it is nonzero and the leading coeff. is 1: $\left(\begin{array}{l} 3x^2+1 \in \mathbb{Q}[x] \text{ not monic} \\ x^2 + 1/3 \in \mathbb{Q}[x] \text{ is monic} \end{array} \right)$

2) A pol $m(x) \in \mathbb{F}[x]$ is a minimal pol for $T \in End(V)$ if
   1) $m(x)$ is monic and $m(T) = 0$
   2) If $f(x)$ is monic and $f(T) = 0$, then $\deg f(x) \geq \deg m(x)$.

Def Let $f(x), g(x) \in \mathbb{F}[x]$.
We say $f(x)$ divides $g(x)$
written $f(x) \mid g(x)$
if $\exists\, h(x) \in \mathbb{F}[x] : f(x)h(x) = g(x)$.

Theorem Let $T : V \to V$ be linear map, where V is fin. dim'l.
Let $m(x)$ be a minimal pol. for T, and let $f(x)$ be any ~~monic~~ pol such that $f(T) = 0$.
Then $m(x) \mid f(x)$.

Proof By the Division Algorithm in $\mathbb{F}[x]$,

$$f(x) = m(x)\, q(x) + r(x)$$

for some $q(x), r(x) \in \mathbb{F}[x]$ where either $r(x) = 0$, or $\deg r(x) < \deg m(x)$.
We have

$$r(T) = \underbrace{f(T)}_{=0} - \underbrace{m(T)}_{=0}\, q(T) = 0$$

If $r(x)$ were nonzero with leading coeff c then $\frac{1}{c} r(x)$ would be a monic pol annihilating T ($\frac{1}{c} r(T) = 0$) and of degree strictly less than $\deg m(x)$. This would contradict that $m(x)$ is a minimal pol. for T.

Therefore $r(x) = 0$.

So $m(x) \mid f(x)$ ∎

<u>Cor</u> Every $T \in \mathrm{End}(V)$, V fin. dim'l, has a <u>unique</u> minimal polynomial.

<u>Pf</u> If $m_1(x)$, $m_2(x)$ are both minimal pols, then $m_1(x) \mid m_2(x)$ and $m_2(x) \mid m_1(x)$ by theorem. So $m_2(x) = \lambda m_1(x)$, $\lambda \in \mathbb{F}$. But both are monic, So $\lambda = 1$. ∎

Notation The minimal pol for T is denoted

$$m_T(x).$$

If $V = \mathbb{F}^n$ and $T = T_A$ (mult. by $A \in \mathbb{F}^{n \times n}$) we put $m_A(x) = m_{T_A}(x)$.

Examples 1) The zero map $0 : V \longrightarrow V$ has $m_0(x) = x$

2) A scalar matrix

$$\lambda I_n = \begin{bmatrix} \lambda & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda \end{bmatrix}$$

has $m_{\lambda I_n}(x) = x - \lambda$

3) A diagonal matrix
$D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$
has $m_D(x) = (x - \lambda_{i_1}) \dots (x - \lambda_{i_k})$
where λ_{i_j} are the pairwise distinct λ_i's

Ex

A Jordan block of size $n \times n$:

$$J_n(\lambda) = \begin{bmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{bmatrix}$$

has min. pol. $(x-\lambda)^n$

Proof

Let $A = J_n(\lambda)$

$(A-\lambda I_n)^0 = \begin{bmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{bmatrix} = I_n$

$\cancel{A} - \lambda I_n = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ & & & 0 \end{bmatrix}$ $\quad (\cancel{A}-\lambda I)^2 = \begin{bmatrix} 0 & 0 & 1 & & 0 \\ & 0 & 0 & 1 & \\ & & 0 & 0 & 1 \\ & & & 0 & 0 & 1 \\ 0 & & & & \ddots & 0 \\ & & & & & 0 \end{bmatrix}$

$\ldots \quad (\cancel{A}-\lambda I)^{n-1} = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & 0 & & \vdots \\ & & & 0 \end{bmatrix}, \quad \underline{\underline{(A-\lambda I)^n = 0}}$

These are lin indep. &

$\{1 = (x-\lambda)^0, \ x-\lambda, (x-\lambda)^2, \ldots, (x-\lambda)^{n-1}\}$

is a basis for subspace of $\mathbb{F}[x]$ of pols of deg $\leq n-1$. So $m_A(x)$ has degree $\geq n$. But $(\cancel{A}-\lambda I)^n = 0$ so $m_A(x) = (x-\lambda)^n$ $\blacksquare$

In HW you showed:

If $m_A(x) = x^n$

(so in particular $1, A, \dots, A^{n-1}$ are lin. indep.)

then $A \sim \begin{bmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & 1 & 0 \end{bmatrix}$

~~Now~~ $m_A(x) = m_{A^T}(x)$

Reordering basis

$\Rightarrow A \sim \begin{bmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} = J_n(0)$

$\Rightarrow$ If $m_T(x) = (x-\lambda)^n$

then $[T]_{\mathcal{B}} = \begin{bmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{bmatrix} = J_n(\lambda)$

in some basis

(Note: $m_{T+\lambda Id_V}(x) = m_T(x-\lambda)$)