Ejemplo: Sea $A = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{R})$. Entonces $P_A(X) = \begin{vmatrix} X & -1 \\ -2 & X-3 \end{vmatrix} = X^2 - 3X - 2$.

Cayley-Hamilton: $A^2 - 3A - 2I_2 = 0$. En efecto, $A^2 = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 6 & 11 \end{pmatrix}$

$\Rightarrow A^2 - 3A - 2I_2 = \begin{pmatrix} 2 & 3 \\ 6 & 11 \end{pmatrix} - 3\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ✓

Usos típicos de Cayley-Hamilton: Como $A^2 - 3A - 2I_2 = 0$ (✱)

$\Rightarrow A^2 = 3A + 2I_2$, $A^3 = 3A^2 + 2A \overset{(✱)}{=} 3(3A + 2I_2) + 2A = 11A + 6I_2$, etc.

Notar que $\det(A) = \begin{vmatrix} 0 & 1 \\ 2 & 3 \end{vmatrix} = 0 - 2 \neq 0$, ie, $A \in GL_2(\mathbb{R})$.

Multiplicando (✱) por A^{-1}: $A - 3I_2 - 2A^{-1} = 0 \Rightarrow A^{-1} = \dfrac{A - 3I_2}{2} = \begin{pmatrix} -3/2 & 1/2 \\ 1 & 0 \end{pmatrix}$.

§20. Polinomio minimal

Sea V un k-e.v. de dimensión finita y $u: V \to V$ un endomorfismo.
Sabemos que siempre $\exists P \in k[X]$ no-nulo tq $P(u) = 0$ en $\mathrm{End}_k(V)$.

Prop: Sea $u: V \to V$ un endomorfismo. Entonces, existe un único polinomio unitario $m_u \in k[X]$ tq para todo polinomio $P \in k[X]$ se cumple que:

$$P(u) = 0 \iff m_u \text{ divide a } P.$$

Diremos que m_u es el polinomio minimal de u.

Dem: El sub-conjunto $I = \{P \in k[X] \text{ tq } P(u) = 0\} \subseteq k[X]$ es un ideal:

(i) Si $\lambda \in k$ y $P, Q \in I \Rightarrow \lambda P + Q \in I$ pues $(\lambda P + Q)(u) = \lambda P(u) + Q(u) = 0$
Luego, I es un sub-e.v. de $k[X]$.

(ii) Si $P \in I$ y $Q \in k[X] \Rightarrow PQ \in I$ pues $(PQ)(u) = \underbrace{P(u)}_{=0} Q(u) = 0$.

Más aún, $I \neq \{0\}$ (ver §7) $\overset{(§18)}{\Longrightarrow} \exists! \, m_u \in k[X]$ polinomio unitario tq
$I = \langle m_u \rangle$, ie, $\forall P \in k[X]$ se tiene que $P(u) = 0 \iff P \in I = \langle m_u \rangle$
$\iff P = m_u Q$ para cierto $Q \in k[X]$ ■

Terminología: Si $A \in M_n(k)$, definimos el polinomio minimal de A como el polinomio minimal $m_A \in k[X]$ del endomorfismo $u_A: k^n \to k^n$, $x \mapsto Ax$ asociado.

$\boxed{\text{Ejercicio importante}}$ Sea $u: V \to V$ un endomorfismo. Probar que:
$gr(m_u) = 1$, ie, $m_u(X) = X - \lambda$ para cierto $\lambda \in k \iff u = \lambda \, id_V$ (homotecia).
En part, $m_u(X) = X \iff u = 0$.

Teorema de Cayley-Hamilton (reformulación): Sea $u: V \to V$ un endomorfismo, entonces el polinomio minimal m_u divide al polinomio característico P_u.

Ejemplos: ① $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(k)$ verifica $A^2 = 0$. Luego m_A divide $P(X) = X^2$.
Dado que $A \neq 0$, $m_A(X) \neq X$ y luego $m_A(X) = X^2$.

② $A = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \in M_2(\mathbb{R})$ verifica $P_A(X) = X^2 - 3X - 2$. Como A no es una homotecia, $gr(m_A) \geq 2 \underset{\text{Cayley-Hamilton}}{\Longrightarrow} m_A(X) = P_A(X)$.

Dado que m_u divide P_u, y las raíces de P_u son los valores propios de u, tenemos que toda raíz de m_u es un valor propio de u. El recíproco es cierto:

Teorema: Sea $u: V \to V$ un endomorfismo. Entonces, todo valor propio de u es raíz del polinomio minimal $m_u \in k[X]$.

Dem: Sea $\lambda \in k$ un valor propio de u y sea $v \neq 0$ un vector propio asociado, ie, $u(v) = \lambda v$. La división euclideana de m_u por $(X-\lambda)$ nos da:

$$m_u(X) = Q(X)(X-\lambda) + c \quad , \text{ donde } c \text{ polinomio de grado} < 1 \text{, ie, } c \in k$$

$\Rightarrow 0 = m_u(u) = Q(u)(u - \lambda \mathrm{Id}_V) + c\,\mathrm{Id}_V$ en $\mathrm{End}_k(V)$. Aplicándolo a v:

$$0 = Q(u)(\underbrace{(u-\lambda \mathrm{Id}_V)(v)}_{=0}) + c\,\underbrace{\mathrm{Id}_V(v)}_{=v} = \underbrace{Q(u)(0)}_{=0} + cv = cv \underset{v \neq 0}{\Longrightarrow} c = 0$$

Luego, $m_u(X) = Q(X)(X-\lambda)$, ie, $\lambda \in k$ es una raíz de m_u. ∎

Ejemplo: Sup. que $\dim_k(V) = n$, entonces para todo endomorfismo $u: V \to V$ se tiene $\mathrm{gr}(P_u) = n$. Cayley-Hamilton: m_u divide $P_u \Rightarrow \mathrm{gr}(m_u) \leq n$.
En part, si $u: V \to V$ tiene n valores propios distintos entonces el Teorema anterior implica que todos ellos son raíces de $m_u \Rightarrow \mathrm{gr}(m_u) \geq n$. Luego, en ese caso tenemos que $m_u = P_u$.

Ejemplo: Sea $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(k)$ y $B = A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(k)$.

$\Rightarrow P_A(X) = P_B(X) = X^3$. Como A y B no son homotecias, $\mathrm{gr}(m_A) \geq 2$ y $\mathrm{gr}(m_B) \geq 2$.
Como $B^2 = A^3 = 0$ tenemos que $m_A(X) = P_A(X) = X^3$ y $m_B(X) = X^2 \ (\neq P_B(X))$.

§21. Reducción de endomorfismos y Descomposición de Dunford:

Comencemos por probar el siguiente resultado útil:

Lema de los kernel: Sea $u: V \to V$ un endomorfismo y $P \in k[X]$ un polinomio. Entonces:

1. El sub-e.v. $\ker(P(u))$ es estable por u, ie,
$$u(\ker P(u)) \subseteq \ker P(u).$$
2. Si $P = AB$ con A y B primos entre sí (ie, $\mathrm{mcd}(A,B) = 1$) entonces
$$\ker P(u) = \ker A(u) \oplus \ker B(u).$$

Dem: ① Notar que u y $P(u)$ conmutan: $u \circ P(u) = P(u) \circ u$.
Si $v \in \ker(P(u))$, ie, $P(u)(v) = 0$, entonces $P(u)(u(v)) = u(P(u))(v)$
$\Rightarrow u(v) \in \ker P(u)$ ✓ $\qquad = u(\underbrace{P(u)(v)}_{=0}) = 0$

② Teorema de Bézout $\Rightarrow \exists\, \mathcal{U}, \mathcal{V} \in k[X]$ tq $A\mathcal{U} + B\mathcal{V} = 1$.
$\Rightarrow A(u)\mathcal{U}(u) + B(u)\mathcal{V}(u) = \mathrm{id}_V$. Si $v \in \ker A(u)$ y $v \in \ker B(u)$
$\Rightarrow v = \mathrm{id}_V(v) = (A(u)\mathcal{U}(u))(v) + (B(u)\mathcal{V}(u))(v) = \mathcal{U}(u)(\underbrace{A(u)(v)}_{=0}) + \mathcal{V}(u)(\underbrace{B(u)(v)}_{=0}) = 0$