

Tema 2

Triangularización y forma canónica de Jordan

[Nota: estos apuntes se basan en el libro de Álgebra Lineal y Geometría de Manuel Castellet e Irene Llerena.]

VIII.1 Vectores propios y valores propios. Polinomio Característico.

Definición:

Sea $f \in \text{End}_k(E)$. Diremos que $v \in E$, $v \neq \vec{0}$ es un vector propio de f si $\exists k \in k$ tal que:

$$f(v) = kv$$

Diremos que k es un valor propio de f .

Ejemplo:

$\forall v \in \ker(f)$, $v \neq \vec{0}$ ($\dim(\ker(f)) \geq 1$). Se da que:

$f(v) = 0_v = 0_{\mathbb{K}}v \Rightarrow v$ es un vector propio asociado al valor propio $0 \in \mathbb{K}$.

Observación:

$v \neq \vec{0}$ es vector propio de f de valor propio $k \Leftrightarrow$

$$f(v) = kv \Rightarrow f(v) - kv = \vec{0} \quad (1)$$

Tomemos $g \in \text{End}_{\mathbb{K}}(V)$, $g(v) = f(v) - kv$. Entonces, por (1)

Si v es vector propio de $f \Rightarrow v \in \ker(g) \Rightarrow$

$\Rightarrow v \in \ker(f - k \cdot \text{id}) \Rightarrow v \in \ker(M_B(f) - k \cdot I_n)$.

Esto nos motiva a deducir: pasó a matrices (Además: Si k es valor propio, $\ker(g) \neq \{\vec{0}\}$.)

Multiplicidad de k = $\dim(\ker(g))$.

Proposición 1.1:

$k \in \mathbb{K}$ es un valor propio de $f \Leftrightarrow \det(f - k \cdot \text{id}) \neq \{\vec{0}\}$

dem:

k valor propio de $f \Leftrightarrow \ker(f - k \cdot \text{id}) \neq \{\vec{0}\} \Leftrightarrow$

$\Leftrightarrow \det(f - k \cdot \text{id}) \neq 0$

↓
por VI.3.4 (referencia del libro a otro capítulo).

Idea: $\ker(f) = \{v \in E : f(v) = \vec{0}\} \Rightarrow M_B(f) \cdot v = \vec{0} \rightsquigarrow A \cdot X = \vec{B}$

Si existe una única solución, esta ha de ser la trivial que siempre existe
y por Rouché-Frobenius $\Rightarrow \det(A) = 0$. Si no, aplicando el mismo criterio,
 $\det(A) \neq 0$. (Idea más o menos precaria para entender el concepto).

Definición:

Sea $M_{\mathcal{B}}(g) = A = (a_{ij}^g)$. Observamos que: k valor propio

$$\det(g - k \cdot \text{Id}) = \begin{vmatrix} a_{1,1} - k & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} - k & \cdots & a_{2,n} \\ \vdots & & \ddots & \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} - k \end{vmatrix} = 0 \quad (2)$$

Es una expresión de grado n en la incógnita k . Nos define un polinomio $P_A(k)$ que denominaremos **polinomio característico** de A o asociado a g .

Este es porque si B es $M_{\mathcal{B}}(g) = B \rightarrow$

$$\det(g - k \cdot \text{Id}) = \det(B - k \cdot I_n) \quad \text{y como} \quad \det(g - k \cdot \text{Id}) = \det(A - k I_n)$$

$$\Rightarrow P_A(k) = P_B(k).$$

(Matrices equivalentes, $B = P^{-1}AP$, asociadas al mismo endomorfismo, tienen el mismo polinomio característico).

Observemos que las soluciones de $P_g(k) = 0$ son los valores propios asociados a g por (2).

La **traza** de una matriz es la suma de los elementos de su diagonal, y toda la fórmula explícita de $P_g(x)$ y su invención repeta de matrices equivalentes:

$$\text{tr}(g) = \text{tr}(A) = \text{tr}(B)$$

VIII.2 Diagonalización de matrices

Definición:

Sea $f \in \text{End}(E)$. Si $\exists \beta$ base de E tal que $M_{\beta}(\mathbf{f}) = D$, decimos que f es diagonalizable y que D es diagonal.

$$M_{\beta}(\mathbf{f}) = D = \begin{pmatrix} k_1 & 0 & \cdots & 0 \\ 0 & k_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & k_n \end{pmatrix}$$

(Observar, buscamos β formada por vectores propios de manera que $\forall i \in \{1, \dots, n\}$ si $v_i \in \beta$, $\mathbf{f}(v_i) = k_i \cdot v_i$).

Observar, que del apartado anterior sabemos encontrar los valores propios y para calcular los vectores propios basta resolver el sistema de ecuaciones que nos genera $M_{\beta}(\mathbf{f}) \cdot V = k \cdot V$. Por tanto, si conseguimos ver cuándo hay $n = \dim(E)$ vectores propios linealmente independientes, ya seremos capaz de hallar β y por tanto D .

Proposición 2.1:

Vectores propios asociados a valores propios distintos son linealmente independientes.

dem -:

Por inducción sobre el número de valores propios.

Si $m = 1$.

Tendremos un único vector v_1 propio, y es linealmente independiente //

Si $m=2$.

Tomemos v_1 asociado a k_1 y v_2 asociado a k_2 . Entonces:

Suponemos una \mathbb{K} -c.l. igualada a 0 . Es:

$$\lambda_1 v_1 + \lambda_2 v_2 = \bar{0} \Rightarrow$$

$$\circ (\gamma - k_1 \text{Id})(\bar{0}) = \bar{0} \quad (\text{por ser } \gamma - k_1 \text{Id un endomorfismo}).$$

$$\circ (\gamma - k_1 \text{Id})(\lambda_1 v_1 + \lambda_2 v_2) = \downarrow \gamma(\lambda_1 v_1 + \lambda_2 v_2) - k_1 \text{Id}(\lambda_1 v_1 + \lambda_2 v_2)$$

composición de
endomorfismos

γ lineal

$$= \gamma(\lambda_1 v_1) - k_1 \text{Id}(\lambda_1 v_1) + \gamma(\lambda_2 v_2) - k_1 \text{Id}(\lambda_2 v_2) =$$

$$= (\cancel{k_1 \lambda_1 v_1} - k_1 \lambda_1 v_1) + k_2 \lambda_2 v_2 - k_1 \lambda_2 v_2$$

$$= (k_2 - k_1) \lambda_2 v_2$$

$\circ \neq$ por hip.

$$\Rightarrow (k_2 - k_1) \lambda_2 v_2 = 0 \Rightarrow \lambda_2 = 0$$

$\begin{matrix} \neq \\ 0 \end{matrix}$ $\begin{matrix} \neq \\ 0 \end{matrix}$

$$\text{y como } \lambda_1 v_1 + \lambda_2 v_2 = \bar{0} \Rightarrow \lambda_1 = 0 \Rightarrow \lambda_1 = \lambda_2 = 0$$

y v_1 y v_2 son linealmente independientes.

Supongamos el resultado cierto para m valores propios y veamos que se cumple para $m+1$.

Tomemos v_i asociado a $k_i \quad \forall i \in \{1, \dots, m+1\}$. Suponemos que

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_m v_m + \lambda_{m+1} v_{m+1} = \bar{0} \quad (\text{IK-c.l. igual a } 0)$$

con $\lambda_i \in \mathbb{K}$.

Ecuación (1)

5

Entonces: (V es la \mathbb{K} -c.l. y $\bar{v} = \bar{0}$)
 (por ser vectores propios)

$$\cdot (f - k_{m+1} \text{Id})(\bar{v}) = \bar{0} \quad (1) \quad k_i z_i v_i$$

$$\cdot (f - k_{m+1} \text{Id})(v) = \sum_{i=1}^{m+1} f(z_i v_i) - k_{m+1} \sum_{i=1}^{m+1} z_i v_i =$$

$$= \sum_{i=1}^{m+1} (k_i - k_{m+1}) z_i v_i = \sum_{i=1}^m (k_i - k_{m+1}) z_i v_i = \bar{0} \quad (2)$$

$$\begin{matrix} \# \\ \# \\ \# \\ \# \\ \# \end{matrix} \quad \begin{matrix} \downarrow \\ \downarrow \\ \downarrow \\ \downarrow \\ \downarrow \end{matrix} \quad \begin{matrix} \text{Para } i = m+1, \\ (k_{m+1} - k_{m+1}) = 0 \end{matrix}$$

Tenemos (2), una \mathbb{K} -c.l. de m vectores propios asociados a vectores propios distintos. Por hip. inducción $\Rightarrow (k_i - k_{m+1}) z_i = 0 \quad \forall i \in \{1, \dots, m\}$

$$\Rightarrow z_i = 0 \quad \forall i \in I.$$

Volviendo a (1)

Como v_{m+1} es vector propio $\Rightarrow v_{m+1} \neq \bar{0}$

$$\Rightarrow 0 + 0 + \dots + 0 + z_{m+1} v_{m+1} = \bar{0} \Rightarrow z_{m+1} = 0$$

$\Rightarrow \forall i \in I, z_i = 0$ y son linealmente independientes, lo que completa la prueba. \square

Corolario 2.2

El número de valores propios es $\leq n$ (Si hubiera $n+1$, tomamos $n+1$ vectores propios asociados a valores propios distintos y serían \mathbb{K} -libre de $n+1$, que contradice $\dim(E) = n$).

Si hay exactamente n valores propios distintos entonces f es diagonalizable.

(Tomando v_i asociado a z_i , $\{v_i\}_{i \in I}$ sería \mathbb{K} -libre maximal, base formada por vectores propios).

Proposición 2.3

- Si r es la multiplicidad del valor propio k , es decir:
 $r = \dim(\ker(f - k\text{Id}))$ y s es la multiplicidad del cero k
del polinomio característico, entonces $r \leq s$.

dem:

Sea $\{v_1, \dots, v_r\}$ una base de $\ker(\underbrace{f - k\text{Id}}_{g})$. La completamos hasta una base de E : $\{v_1, \dots, v_r, w_{r+1}, \dots, w_n\} = \beta$.

La matriz asociada es:

$$M_{\beta}(g) = \begin{pmatrix} k & 0 & \dots & 0 & a_{1,r+1}, \dots, a_{1,n} \\ 0 & k & \dots & 0 & a_{2,r+1}, \dots, a_{2,n} \\ \vdots & \vdots & \ddots & k & a_{r,r+1}, \dots, a_{r,n} \\ 0 & 0 & \dots & 0 & a_{n,r+1}, \dots, a_{n,n} \end{pmatrix}$$

Desarrollando por la primera columna:

$$P_g(x) = (k-x)^r \cdot p(x) \Rightarrow r \leq s \quad (\text{pues } p(x)$$

podría ser $(k-x)^j \cdot q(x)$ de manera que $s = r+j \leq n$).

Observar que siempre es necesariamente $r \leq s \leq n$. \square

Si f es diagonalizable $\rightarrow \begin{pmatrix} k_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & k_n \end{pmatrix}$ y los valores propios no son todos necesariamente distintos, es:

$$p(x) = (k_1-x)^{s_1} \cdots (k_n-x)^{s_n} \rightarrow \begin{array}{l} \text{Se descompone en} \\ \text{factores lineales.} \end{array}$$

(Observar: $\sum_{i=1}^n s_i = n$).

Si k_i aparece s veces en la diagonal, la multiplicidad de $(x-k_i)$ es s .

F

Por otra parte, $(f - k_i I)$ tendrá una matriz diagonal formada por s ceros en la diagonal, donde $\dim(\ker(f - k_i I)) = s$.

Esto caracteriza los endomorfismos diagonalizables como se demuestra abajo.
 $(r \leq s)$ y tenemos s vectores linealmente independientes por la matriz diagonal $\Rightarrow r=s$ y forman base $(f - k_i I)$

Teorema 2.4 (diagonalización)

(Teorema 8.10 pág. 367 libro Vera).

Un endomorfismo es diagonalizable \Leftrightarrow

$\Leftrightarrow P_f(x)$ se descompone en factores lineales y la multiplicidad

de cada uno de ellos coincide con la de valor propio de f.

$$\forall i, m(k_i) = \dim(V(k_i))$$

dem-:

\Rightarrow)

Probado con la observación de la prop 2.3

\Leftarrow)

Sea $P_f(x) = (-1)^n \cdot (x - k_1)^{n_1} \cdot (x - k_2)^{n_2} \cdots (x - k_r)^{n_r}$.

$$\text{con } n_1 + \cdots + n_r = n$$

Decimos que $E(k_i) = \ker(f - k_i \text{Id})$. Veamos que:

$$E = E(k_1) + \cdots + E(k_n). \quad (1)$$

Una vez probado, bastará tomar bases de los diferentes subespacios y juntarlos todos para hallar una base de E formada por vectores propios ($\beta = \{v_1, \dots, v_{n_1}, \dots, w_1, \dots, w_{n_r}\} \rightarrow$ de vectores propios)

base $E(k_i) \hookrightarrow$ base $E(k_n) \rightarrow$ Los de $E(k_i)$ independientes
 (linealmente indepe) (son linealmente indepe) de los $E(k_j)$ ($i \neq j$)

y por tanto sería diagonalizable.

Para demostrar (1) vamos a demostrar que la expresión de $V \in E$ como vectores de $E(k_1), \dots, E(k_r)$ es única.

Tomemos $V \in E$ tal que:

$$V = V_1 + \dots + V_r = W_1 + \dots + W_r \text{ con } V_i, W_i \in E(k_i), \forall i \in \{1, \dots, r\}.$$

$$\Rightarrow (V_1 - W_1) + (V_2 - W_2) + \dots + (V_r - W_r) = \vec{0} \text{ que es una}$$

combinación lineal de vectores propios iguales a 0. Sabemos que entonces los coeficientes son 0, pero como son 1 \Rightarrow

$$\Rightarrow V_i - W_i = \vec{0} \in E(k_i) \Rightarrow V_i = W_i \quad \forall i \in \{1, \dots, r\} \text{ y}$$

es la misma descomposición. Como además, $E(k_i) \cap E(k_j) = \{\vec{0}\}$ para $i \neq j$ (pues vectores propios asociados a valores propios distintos son linealmente independientes por proposición 2.1). y $n_1 + \dots + n_r = n$

$$\Rightarrow \sum_{i=1}^r \dim(E(k_i)) = n = \dim(E) \Rightarrow \text{La suma de}$$

$$\text{los subespacios de los } E(k_i) \text{ es directa} \Rightarrow \sum_{i=1}^r E(k_i) = E,$$

Como queríamos ver, y esto concluye la prueba. \square

($\sum_{i=1}^r \dim(E(k_i)) = n$. Sabemos que si $U \subseteq E$ y $W \subseteq E$,

$$U + W \subseteq E. \text{ Si } \dim(U + W) = \dim(E) \Rightarrow U + W = E.$$

y en ese caso $U \oplus W = E$. Hemos tomado $E(k_i) \subseteq E \quad \forall i \in \{1, \dots, r\}$, tales que $E(k_i) \cap E(k_j) = \{\vec{0}\}$ y $\sum_{i=1}^r \dim(E(k_i)) = n$. Por ser

subespacio de E , necesariamente ha de darse que $\downarrow \text{(Fórmulas Grassmann)}$

$$E(k_1) \oplus \dots \oplus E(k_r) = E$$

$$\begin{aligned} &= n_1 + \dots + n_r + \sum_{i,j} \dim(E(k_i) \cap E(k_j)) \\ &= n \end{aligned}$$

Definición:

Una matriz $A = (a_{ij})_{i,j}$ se dice que es **triangular superior** si $a_{i,j} = 0 \quad \forall i < j$. (Respectivamente triangular inferior).

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{nn} \end{pmatrix}$$

Decimos que un endomorfismo f es **triangularizable** si existe una matriz \downarrow respecta de la que es triangular superior.
asociada a f

Teorema 2.5 (de triangularización)

(Teorema 8.5 página 360).

Un endomorfismo es triangularizable \Leftrightarrow

Se descompone en factores de primer grado $P_h(x)$.

dem:
 \Rightarrow

$$\text{Sea } M_p(f) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ 0 & 0 & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} \Rightarrow$$

$$P_h(x) = \det(M_p(f) - xI_n) = (x - a_{11})(x - a_{22}) \dots (x - a_{nn})$$

$\forall i, k_i \in K$

Ej. en \mathbb{R} sería que $\forall i, k_i \in \mathbb{R}$
(no hay ningún k_i que se escape a \mathbb{C}).

Vole

\Leftrightarrow

Por inducción sobre n .

$n=1 \rightarrow$ Trivial, pues toda matriz es triangular.

Supongamos cierto para $n-1$ y veamos que se cumple para $n \geq 2$.

Sabemos que $P_n(x)$ se descompone en factores lineal \Rightarrow hay como mínimo un valor propio con un vector propio asociado $\{V\}$. Ampliamos a una base de E respecto de la cual:

$$M_B(g) = \begin{pmatrix} k & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{nn} & \cdots & a_{nn} \end{pmatrix}$$

Consideremos que: $g: \langle v_2, \dots, v_n \rangle \longrightarrow \langle v_2, \dots, v_n \rangle$ dada

$$\text{por } \begin{pmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix} \quad (\text{observar: } M_B(g) = \begin{pmatrix} k & B \\ 0 & C \end{pmatrix} \rightsquigarrow$$

(C es \bar{g} asociada a $g \Rightarrow g = \bar{g}$).

Tenemos que:

$$|g - xI_d| = (k-x) \cdot \det(g - xI) \Rightarrow \underbrace{P_g(x)}_{\substack{\text{se descompone} \\ \text{en factores simples}}} = (k-x) \cdot P_{\bar{g}}(x)$$

\nearrow hip. inducción

$\Rightarrow P_{\bar{g}}(x)$ se descompone en factores simples \Rightarrow es triangularizable.

$$\begin{pmatrix} b_{22} & b_{23} & \cdots & b_{2n} \\ 0 & b_{33} & \cdots & b_{3n} \\ 0 & 0 & \cdots & b_{nn} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{pmatrix}$$

en la base $\{v_2, \dots, v_n\}$ de $\langle v_2, \dots, v_n \rangle$.

ASC : ↗ (1)

$$\text{ASE: } f(v_i) = \underbrace{a_{2i} \cdot v_2}_{(1)} + g(v_i) \quad i=2, \dots, n \quad (g: \langle v_2, \dots, v_n \rangle \rightarrow \langle v_2, \dots, v_n \rangle)$$

$$\text{Si tomamos } u_j = \sum_{i=2}^n c_{ji} v_i \Rightarrow$$

$$\Rightarrow f(u_j) = \sum_{i=2}^n c_{i,j} g(v_i) = \sum_{i=2}^n c_{i,j} (a_{i,1} v_1 + g(v_i)) = \\ = \left(\sum_{i=2}^n c_{j,i} \cdot a_{i,1} \right) v_1 + g(u_j) \quad \forall j=2, \dots, n. \quad (2)$$

La matriz de f en la base $\{v_1, u_2, \dots, u_n\}$ se obtiene a la matriz de g una primera columna $(k, 0, \dots, 0)$ y una primera fila $(k, b_{21}, \dots, b_{n1})$, con $b_{ji} = \sum_{i=2}^n c_{ji} a_{i1}$ $j \geq 2$ y es de esta manera, $M_{\beta\beta}(f)$ triangular \square .

(1) pensar en $\left(\frac{k+A(g)}{0+M_B(g)} \text{ (sila } A = (a_{ij}, :)) \right)$

(2) Esto en definitiva prueba que: $f(u_j) = \text{cte} \cdot v_i + g(u_j)$ es decir: que si la nueva matriz de f va a respetar la matriz nueva de g , es decir:

$$M_{\beta \text{ nueva}}(g) = \begin{pmatrix} a_{11} & \underline{\text{cte}_2 \quad \text{cte}_3 \quad \text{cte}_4 \dots \text{cte}_n} \\ a_{21} & \\ \vdots & \\ a_{n1} & M_{\beta \text{ nueva}}(g) \end{pmatrix}$$

(pensez $M_{\beta^i}(f) \cdot u_j$, $i \geq 2$) (= $f(u_j)$)

Tomamos w_1 de la base tal que:

$$\left(\begin{array}{c|c} k & \text{cte} \\ \hline 0 & M_{\text{pura}}(g) \end{array} \right),$$

VIII.3 Polinomio mínimo

Nos falta simplificar la matriz en el caso general. Vamos a descomponer E en suma directa de subespacios que permitan obtener bases convenientes en las que se pueda expresar el endomorfismo. (es lo que nos ha servido en el caso de la diagonalización).

Dado f un homomorfismo, consideremos f^r como $\underbrace{f \circ f \circ \dots \circ f}_r$.

De manera que:

$$f^0 = \text{Id}; \quad f^1 = f, \quad f^2 = f \circ f, \quad \dots, \quad f^r = f \circ f^{r-1}$$

Observamos que si $r = n^2$, $\{\text{Id}, f, f^2, \dots, f^{n^2}\}$ es \mathbb{k} -largo.

Para probar esto vamos a demostrar que $\dim(\text{End}_{\mathbb{k}}(V)) = n^2$.

Recordemos: $\text{End}_{\mathbb{k}}(V) \underset{\downarrow}{\sim} \text{Mat}_{n \times n}(\mathbb{k})$. Por tanto, basta demostrar

que $\dim(\text{Mat}_{n \times n}) = n^2$. En efecto, consideremos $e_{ij} \begin{pmatrix} 0 & \dots & ? \\ \vdots & \ddots & 1 \\ 0 & \dots & 0 \end{pmatrix}$

(matriz todo ceros excepto en la posición a_{ij}).

Veremos que: $\{e_{11}, e_{12}, \dots, e_{1n}, e_{21}, \dots, e_{2n}, \dots, e_{n1}, \dots, e_{nn}\}$ es \mathbb{k} -libre:

$$\lambda_{11}e_{11} + \lambda_{12}e_{12} + \dots + \lambda_{nn}e_{nn} = 0 \Rightarrow$$

$$\Rightarrow \sum_{i,j} \lambda_{ij} e_{ij} = -\lambda_{11}e_{11} \rightarrow \Rightarrow \lambda_{ij} = 0 \quad \forall i, j \text{ por } (i, j) \neq (1, 1)$$

construcción, pues e_{11} es la única matriz con la primera entrada no nula.

$$\Rightarrow \text{Es } \mathbb{k}\text{-libre.}$$

Vemos que es \mathbb{K} -s.g. Sea $A = (a_{ij})_{i,j} \in \text{Mat}_{n \times n}(\mathbb{K})$.

En efecto:

$$a_{11}e_{11} + a_{12}e_{12} + \dots + a_{1n}e_{1n} + a_{21}e_{21} + \dots + a_{2n}e_{2n} + \dots + a_{nn}e_{nn} + \dots$$

$$\dots + a_{nn}e_{nn} = A = \sum_{i,j} a_{ij}e_{ij}$$

$$\Rightarrow \text{Es base} \Rightarrow \underbrace{\dots}_{\text{ya dicho}} \Rightarrow \dim(\text{End}_{\mathbb{K}}(V)) = n^2 //$$

Por tanto, al tomar la siguiente \mathbb{K} -c.l.:

$$\underbrace{\lambda_0 \text{Id} + \lambda_1 f + \lambda_2 f^2 + \dots + \lambda_{n^2} f^{n^2}}_{\underline{n^2+1} \text{ términos}} = 0$$

Es \mathbb{K} -ligado y no necesariamente son todos los coeficientes nulos.

Este nos lleva a considerar el núcleo de la siguiente aplicación:

$$\Phi_f : \mathbb{K}[x] \longrightarrow \text{End}_{\mathbb{K}}(E)$$

$$p(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_r x^r \mapsto p(f) = \lambda_0 \text{Id} + \lambda_1 f + \dots + \lambda_r f^r$$

Se cumplen las siguientes propiedades:

- $\Phi_f(p(x) + q(x)) = p(f) + q(f) = \Phi_f(p(x)) + \Phi_f(q(x))$
- $\Phi_f(p(x) \circ q(x)) = p(f) \circ q(f) = \Phi_f(p(x)) \circ \Phi_f(q(x))$
- $\Phi_f(k p(x)) = k p(f) = k \Phi_f(p(x))$

Por tanto deducimos que Φ es un morfismo (homomorfismo entre (creo que son) anillo commutativo y anillo no commutativo).

De la commutatividad de $\mathbb{k}[x]$ se deduce que:

$$p(f) \circ q(g) = q(g) \circ p(f)$$

(Los matrices asociadas a los $p(x)$ comutan si o si).

El núcleo es:

$$\ker(\Phi) = \{ p(x) \in \mathbb{k}[x] \mid p(f) = 0 \}$$

El núcleo es un ideal de $\mathbb{k}[x]$.

Nota:

$(m(x))$ = el conjunto de los múltiplos (multiplicar por constante) de $m(x)$.

Un ideal $I \subset \mathbb{k}[x]$. Es un subconjunto en el que se cumple:

- 1) $a(x), b(x) \in I \Rightarrow a(x) + b(x) \in I$
- 2) $a(x) \in I, c(x) \in \mathbb{k}[x] \Rightarrow a(x) \cdot c(x) \in I$

Como es un ideal, hay un teorema (II.2, pág 27), que nos garantiza que $\exists! p(x) \in \mathbb{k}[x]$ mónico (si $\text{grado}(p(x)) = n$, tomamos $a_n x^n + \dots + a_0 = p(x)$, con $a_n = 1$) de manera que

$I = (p(x))$. Así afirmamos que:

$$\ker(\Phi) = \{ p(x) \in \mathbb{k}[x] \mid p(f) = 0 \} = (m_f(x))$$

Para cierto polinomio mónico $m_f(x) \in \mathbb{k}[x]$.

(Al elegir el $m_f(x)$ que representa el ideal, lo tomamos del menor grado posible).

Definición:

Al polinomio $m_f(x) \in \mathbb{K}[x]$ que cumple que:

$$\ker(\mathbb{D}f) = \{ p(x) \in \mathbb{K}[x] \mid p(f) = 0 \} = (m_f(x))$$

lo llamamos **polinomio mínimo asociado a f**.

A los múltiplos del polinomio mínimo, o al resto de polinomios que pertenecen a $\ker(\mathbb{D}f)$ los llamamos **polinomios anuladores de f**.

Tomemos $m_f(x) \in \mathbb{K}[x]$ un polinomio **mónico**, es decir que el coeficiente del grado máximo es 1.

Si $m_f(x) = a_0 + a_1 x + \dots + a_r x^r \Rightarrow a_r = 1$ (por ser mónico).

$$m_f(x) = a_0 + a_1 x + \dots + a_r x^r$$

Ejemplos:

1) $E = \{\bar{0}\}$ (no es el más trivial).

El único $f \in \text{End}_{\mathbb{K}}(V)$ es $f: \{\bar{0}\} \rightarrow \{\bar{0}\} \Rightarrow f(v) = v = f(0) \quad \forall v \in V$

$\ker(\mathbb{D}f) = \{ p(x) \in \mathbb{K}[x] \mid p(f) = 0 \}$ Tomemos $p(x) = a_0 + a_1 x + \dots + a_r x^r$
 $\rightarrow p(f) = a_0 \cdot \text{Id} + a_1 0 + a_2 0 + \dots + a_r 0 = a_0 \text{Id} \Rightarrow p(f)(v) = a_0 f(v) = 0$
 $\forall v \in V \Rightarrow p(x) \in \ker(\mathbb{D}f) \quad \forall p(x) \in \mathbb{K}[x] \Rightarrow \ker(\mathbb{D}f) = \mathbb{K}[x] = (a_0), 0 \neq a_0 \in \mathbb{K}$

Sup. pol. min(f) = a_0 , $0 \neq a_0 \in \mathbb{K} \Rightarrow \ker(\mathbb{D}f) = (a_0) = \{ a_0 \cdot c(x), c(x) \in \mathbb{K}[x] \} = \mathbb{K}[x] \Rightarrow \forall p(x) \in \mathbb{K}[x], p(f) = 0 \Rightarrow$ En particular, $p(x) = 1 \Rightarrow p(f) = \text{Id} = 0 \Rightarrow \forall v \in V, \text{Id}(v) = v = \bar{0} \Rightarrow V = \{\bar{0}\}$

2) $E \neq \{\bar{0}\}$ y $f = 0$

$$\ker(\mathbb{D}f) = \{ p(x) \in \mathbb{K}[x] \mid p(f) = 0 \} = (x)$$

$$(p(x) = x, p(f) = f = 0)$$

3) $E \neq \{\bar{0}\}$ y $f = \text{Id}$

Observamos que $\Phi(x-1) = -1 \cdot \text{Id} + f = -\text{Id} + \text{Id} = 0$
 $\Rightarrow (x-1) \in \ker(\Phi_f)$.

Ahora: $m_f(x) | (x-1)$ y como no puede ser constante (no pertenecería a $\ker(\Phi_f)$) $\Rightarrow m_f(x) = (x-1)$.

4) $E \neq \{\bar{0}\}$, $f = k \text{Id}$, $k \in K$.

Análogamente a 3), $m_f(x) = (x-k)$.

Fijado un vector $v \in E$, consideramos la siguiente aplicación:

$$\begin{aligned}\Phi_u: K[x] &\longrightarrow E \\ p(x) &\longmapsto p(f)(v)\end{aligned}$$

Aplicar hacer $g(v)$ con $g \in \text{End}(K[V])$, $g = p(f) = \Phi_f(p(x))$.

Análogamente a antes, Φ_u es un ideal de $K[x]$ (su núcleo).

$$\ker(\Phi_u) = \{p(x) \in K[x] \mid p(f)(u) = \bar{0}\} = (m_u(x))$$

El polinomio mónico $m_u(x)$ se llama **polinomio mínimo de f en u** o simplemente **polinomio mínimo de u** . Como antes, si lo tomamos mónico es único, pese a que siempre podemos

$$\text{tomar sus múltiplos } ((m_u(x)) = \{c(x) \cdot m_u(x) \mid c \in K\})$$

\downarrow
mónico $\in K[x]$

$$(c(x) \in K[x])$$

Proposición 3.1

Sea:

$$m_u(x) = \underbrace{a_0 + a_1x + \dots + a_s x^s}_{s+1 \text{ términos}} \in k[x] \quad \text{grado } (s)$$

el polinomio mínimo de u . Entonces:

$\{u, f(u), \dots, f^{s-1}(u)\} \rightarrow$ linealmente independiente.

$\{u, f(u), \dots, f^{s-1}(u), f^t(u)\}, t \geq s \rightarrow$ linealmente dependientes.

demos..:

Supongamos que $\{u, f(u), \dots, f^{s-1}(u)\}$ sean linealmente dependientes.

Entonces, $\exists \lambda_i \in k, i \in I$ tales que:

$$\lambda_0 u + \lambda_1 f(u) + \dots + \lambda_{s-1} f^{s-1}(u) = 0 \quad \text{con } \lambda_1 \neq 0, \dots, \lambda_s \neq 0. \quad (1)$$

Sin embargo, eso contradice que $m_u(x)$ es polinomio mínimo porque:

Por (1), $\exists p(x) \in k[x]$ tal que:

$$p(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_{s-1} x^{s-1} \quad \text{con} \quad p(f)(u) = 0 \Rightarrow$$

$$\Rightarrow p(x) \in \ker(\Phi_u).$$

Sin embargo, para representar el ideal $\ker(\Phi_u)$ se toma el polinomio de menor grado mónico, que era por hipótesis de polinomio de menor grado mónico, que era por hipótesis de grado s . Como $\deg(p(x)) = s-1$, esto contradice que $m_u(x)$ sea de grado s . (hipótesis). La contradicción parte de suponer que $\{u, f(u), \dots, f^{s-1}(u)\}$ son linealmente dependientes, por tanto han de ser linealmente independientes //

Por otra parte, lo demostramos por inducción:

$$as^s(u)$$

||

Si $t=s$,

$$mu(x) \in \text{Ker}(\oplus f) \Rightarrow a_0 u + a_1 f(u) + a_2 f^2(u) + \dots + a_t f^t(u) = 0 \quad (2)$$

Com al menos $a_s \neq 0$ (pues es monico de grado s por

hipótesis ($mu(x)$)).

$\Rightarrow \exists a_i \in k$, no todos nulos que cumplen (2) \Rightarrow son linealmente dependientes.

Si $t \geq s$, suponemos cierto para $t-1$. Por hipótesis:

$$f^{t-1}(u) \in \langle u, f(u), \dots, f^{s-1}(u) \rangle$$

$\Rightarrow \exists z_i, i \in \{0, \dots, s-1\}$ t.q.

$$z_0 u + z_1 f(u) + \dots + z_{s-1} f^{s-1}(u) = f^{t-1}(u)$$

Entonces:

hip.

$$f^t(u) = f(f^{t-1}(u)) = f\left(\sum_{i=0}^{s-1} z_i f^i(u)\right) = \sum_{i=0}^{s-1} z_i f(f^i(u)) =$$

$$= z_0 f(u) + z_1 f^2(u) + \dots + z_{s-1} f^{s-1}(u) + z_s f^s(u)$$

$$\Rightarrow f^t(u) \in \langle f(u), f^2(u), \dots, f^{s-1}(u), f^s(u) \rangle = \langle u, f(u), \dots, f^{s-1}(u) \rangle$$

probado cosa
 $t=s$ (base
de la inducción).

$\Rightarrow \{u, f(u), \dots, f^{s-1}(u), f^t(u)\}$ son linealmente dependientes,

completando la demostración \square

VIII. 4 Subespacios invariantes

Definición:

Un subespacio $F \leq E$ es **invariante** cuando cumple que:

$$f(F) \subset F$$

Observar que en este caso, f induce un endomorfismo de F :

$$\begin{aligned} f' = f|_F : F &\longrightarrow F \\ v &\longmapsto f(v) \end{aligned}$$

Que llamaremos **restricción** de f a F .

Proposición 4.1

El polinomio mínimo de una restricción de f , $m_{f'}(x)$ divide a $m_f(x)$.

dem.:

$$\text{Por def: } m_f(f) = 0 \Rightarrow m_f(f)(u) = \vec{0} \quad \forall u \in E \Rightarrow m_f(f')(v) = \vec{0}$$

$$= \vec{0} = m_f(f)(v) = \vec{0}, \quad \forall v \in F \stackrel{(2)}{\Rightarrow} m_f(x) \in (m_{f'}(x)) \quad \boxed{\square}$$

(1) Porque como $\forall v \in F, m_f(f)(v) = \vec{0} \Rightarrow m_f(x) \in \ker(\Phi_u) \Rightarrow$

$\Rightarrow m_f(x) \in \{p(x) \in k[x] \mid p(f)(u) = \vec{0}\} = (m_{f'}(x)), \text{ pues por def:}$

$$\left(\begin{array}{l} \Phi_u : k[x] \rightarrow F \\ p(x) \mapsto p(f)(u) \end{array} \right) \text{ y por hip. } \ker(\Phi_u) = (m_{f'}(x))$$

Corolario 4.2

Si dos subespacios $F, G \subseteq E$, invariantes por f , tienen polinomios mínimos primos entre sí, $\Rightarrow F \cap G = \{0\}$.

dem:

Si $F, G \subseteq E$ son invariantes \Rightarrow

$\forall v \in F, f(v) \in F \Rightarrow \forall v \in F \cap V, f(v) \in F \cap G \Rightarrow F \cap G$ es f -invariante.

$\forall v \in G, f(v) \in G$

Ahora bien, por la proposición 4.1:

$$F \cap G \subseteq F \Rightarrow m_f(x) \in (m_h(x))$$

$$F \cap G \subseteq G \Rightarrow m_g(x) \in (m_h(x))$$

$$\Rightarrow m_h(x) | m_f(x) \text{ y } m_h(x) | m_g(x) \Rightarrow m_h(x) \text{ divide a}$$

ambos polinomios, pero como por hipótesis son $m_f(x)$ y $m_g(x)$ primos entre sí \Rightarrow el único $p(x) \in \mathbb{K}[x]$ tal que $p(x) | m_f(x)$ y $p(x) | m_g(x)$ es $p(x) = 1 \in \mathbb{K} \Rightarrow m_h(x) = 1$.

$$\left(\begin{array}{l} \text{Ejemplo 1} \\ \text{pag. 17} \end{array} \right) \ker(\mathbb{D}f) \stackrel{(1)}{=} (1) = \mathbb{K}[x] \Rightarrow \forall p(x) \in \mathbb{K}[x], p(f) = 0 \Rightarrow$$

$$\Rightarrow f = 0, \forall g \in \text{End}_{\mathbb{K}}(F \cap V) \Rightarrow \text{Id} \in \text{End}_{\mathbb{K}}(F \cap V) \text{ o } \text{Id} = 0$$

$$\Rightarrow \forall v \in V, \text{Id}(v) = 0 \Rightarrow v = 0 \Rightarrow F \cap V = \{0\} \quad \square$$

(1)

Recordar: $(1) = \{p(x) \in \mathbb{K}[x] \mid p(x) = c(x) \cdot 1, c(x) \in \mathbb{K}[x]\} = \mathbb{K}[x]$

(2)

En particular tomamos $f = \text{Id}$.

Proposición 4.3

$\forall p(x) \in \mathbb{K}[x]$, tenemos $\ker(p(f)) \subset \text{Im}(p(f))$ son subespacios invariantes para f . Es decir:

$$\forall v \in \ker(p(f)) \text{ es } f(v) \in \ker(p(f))$$

$$\forall v \in \text{Im}(p(f)) \text{ es } f(v) \in \text{Im}(p(f))$$

dem.:

(1)

Sea $u \in \ker(p(f))$. Entonces:

$$p(f)(f(u)) = a_0 f(u) + a_1 f(f(u)) + a_2 f^2(f(u)) + \dots = \\ = f(a_0 u + a_1 f(u) + a_2 f^2(u) + \dots) = f(p(f)(u))$$

Como $u \in \ker(p(f)) \Rightarrow p(f)(u) = 0 \Rightarrow f(p(f)(u)) = f(\bar{0})$. y

como f es lineal, $f(\bar{0}) = f(v - v) = f(v) - f(v) = \bar{0}$

$\Rightarrow p(f)(f(u)) = \bar{0} \Rightarrow f(u) \in \ker(p(f))$ y así tenemos que $\ker(p(f))$ es f -invariante.

(2)

Sea $u = p(f)(v) \in \text{Im}(p(f))$. Entonces:

$$f(u) = f(p(f)(v)) = p(f)(f(v)) \Rightarrow f(v) \in \text{Im}(p(f)) \quad \square$$

(Pues $\exists w \in E, w = f(v)$. t.q. $f(u) = p(f)(w)$).

(Nota: nos van a interesar los \ker más que los imágenes , porque estos últimos van a ser disjuntos, los imágenes no tienen porque).

Proposición 8.13

Sea $h \in \text{End}_{\mathbb{K}}(V)$ y supongamos que $V = V_1 \oplus V_2$ con V_i subespacio h -invariante, para $i = 1, 2$. Sean $h_i|_{V_i} \in \text{End}_{\mathbb{K}}(V_i)$ y $p_i(x) = \text{pol. min}(h_i)$. Entonces: $\text{pol. min}(h) = \text{lcm}(p_1(x), p_2(x))$

dem:

Sea $p(x) = \text{pol. min}(h) \Rightarrow p(g) = 0 \Rightarrow p(g)(v) = \bar{0} \quad \forall v \in V$.

En particular, $p(h)(v_i) = \bar{0} \quad \forall v_i \in V_i \Rightarrow p(h|_{V_i}) = 0$ y por 4.1 $\Rightarrow p_i(x)$ divide a $p(x)$ en $\mathbb{K}[x]$ para $i = 1, 2$.

Sea $q(x) = \text{lcm}(p_1(x), p_2(x)) \in \mathbb{K}[x]$.

Por hipótesis, dada $v \in V$, $\exists v_1 \in V_1$ y $v_2 \in V_2$ t.q. $V = V_1 + V_2$.

Como $p_i(x)$ divide a $q(x) \Rightarrow q(h_i) = 0 \Rightarrow$

$\Rightarrow q(h_i)(v_i) = \bar{0}, i = 1, 2$. Así obtenemos:

$$q(h)(v) = q(h)(v_1 + v_2) = q(h_1)(v_1) + q(h_2)(v_2) = \bar{0} + \bar{0} = \bar{0}, \quad \forall v \in V$$

Por tanto $q(h) = 0$, y como $p(x)$ es polinomio mínimo de $h \Rightarrow q(x)$ divide a $p(x)$.

Observar que si $q(x) \neq p(x) \Rightarrow$ como $q(x)$ es producto de dos monicos es mónico, y si divide a $p(x)$ pero es distinto de $p(x)$ necesariamente ha de tener grado menor, contradiciendo que $p(x)$ es polinomio mínimo $\Rightarrow q(x) = p(x)$. \square

$\left\{ \begin{array}{l} \text{Si } q(g) = 0 \Rightarrow q(x) \in (p(x)) \Rightarrow \text{como } q(x) \text{ divide a } \\ p(x), \text{ grad}(q(x)) \leq \text{grad}(p(x)) \end{array} \right. \Rightarrow \text{grad}(q(x)) = \text{grad}(p(x)) \text{ y } q(x) = p(x)$

por ser
múltiplo de $p(x)$

mónicos y se divide

Sea $\text{pol-min}(f)$ el polinomio mínimo de f . Supongamos que se descompone en producto de dos factores (mónicos) primos entre sí:

Si:

$$\text{pol.-min}(f) = p(x) \cdot q(x)$$

Consideremos $\ker(p(f))$ y $\ker(q(f))$. (Invariantes por 4.3).

Entonces, consideramos $f|_{\ker(p(f))}$ y $f|_{\ker(q(f))}$.

H.v.e $\ker(p(f)) = \{v \in E \text{ t.q. } p(f)(v) = 0\}$ es necesariamente:

$p(f|_{\ker(p(f))})(v) = 0$ (análogo para q). Por tanto,

podemos afirmar que $p(f|_{\ker(p(f))}) = 0$ y es anulador de la restricción de f . (análogo para q).

Así, estamos en condiciones de aplicar 4.2 \Rightarrow

$$\ker(p(f)) \cap \ker(q(f)) = \{0\}$$

Veamos que:

$$\ker(p(f)) \supset \text{Im}(q(f)) \quad (\text{análogo } \ker(q(f)) \supset \text{Im}(p(f))).$$

Comprobaremos:

$u = q(f)(v) \in \text{Im}(q(f))$. Entonces:

$$p(f)(u) = p(f)(q(f)(v)) = (p(f) \circ q(f))(v) \stackrel{\downarrow}{=} \text{pol.-min}(f)(v) = 0$$

por ser
polinomio
mínimo.

(1) Una propiedad del ideal es que:

$$\boxed{\text{Dg}(P(x) \cdot Q(x)) = P(x) \circ Q(x)} \quad \left(\begin{array}{l} \text{En nuestro caso, } P(x) \cdot Q(x) = \\ = \text{pol.-min}(x) \text{ con Dg}(\text{pol.-min}(x)) \\ = \text{pol.-min}(f) \end{array} \right)$$

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_r x^r$$

$$q(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_s x^s$$

(Explicación para entender la idea)

$$P(g)(q(g)(v)) =$$

$$= a_0 (b_0 v + b_1 g(v) + \dots + b_s g^s(v)) + a_1 g((b_0 v + b_1 g(v) + \dots + b_s g^s(v))) =$$

$$+ \dots + a_r g^r ((b_0 v + b_1 g(v) + \dots + b_s g^s(v))) =$$

g lineal

$$\stackrel{\uparrow}{=} a_0 b_0 v + (a_0 b_1 + a_1 b_0) g(v) + (a_0 b_2 + a_1 b_1 + a_2 b_0) g^2(v) + \dots$$

+ ... En definitiva,

$$= g(g)(v) \quad \text{con} \quad g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots \Rightarrow$$

$$g(x) = p(x) q(x).$$

En resumen:

$$P(g)(u) = 0 \Rightarrow u = q(g)(v) \in \ker(p(g)) \Rightarrow$$

$$\Rightarrow \text{Im}(q(g)) \subset \ker(p(g)). \quad (\text{análogo } \text{Im}(p(g)) \subset \ker(q(g)))$$

Además, por el primer teorema de isomorfía:

$$\frac{V}{\ker(p(g))} \simeq \text{Im}(p(g)) \xrightarrow{\text{Aplicamos dimensiones}} \dim(V) - \dim(\ker(p(g))) = \dim(\text{Im}(p(g)))$$

$$(\text{Im}(p(g)) \subset \ker(q(g))) \Rightarrow \dim(\text{Im}(p(g))) \leq \dim(\ker(q(g)))$$

$$\Rightarrow n = \dim(\ker(p(g))) + \dim(\text{Im}(p(g))) \leq$$

$$\leq \dim(\ker(p(g))) + \dim(\ker(q(g))) = (1)$$

$$= \dim(\ker(p(g)) + \ker(q(g))) \leq n$$

$$\left(\begin{array}{l} \ker(p(g)) + \ker(q(g)) \subseteq E \\ \downarrow \\ \text{Subespacio} \end{array} \right)$$

(1) Se ha visto que: (pág. 276, teorema 7.10 libro Vera).

$$\dim_{\mathbb{K}}(U+W) = \dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W) - \dim_{\mathbb{K}}(U \cap W)$$

En nuestro caso:

$$\begin{aligned} \dim_{\mathbb{K}}(\ker(p(f)) + \ker(q(f))) &= \dim_{\mathbb{K}}(\ker(p(f))) + \dim_{\mathbb{K}}(\ker(q(f))) + \\ &\quad - \dim_{\mathbb{K}}(\underbrace{\ker(p(f)) \cap \ker(q(f))}_{\text{sof}}) \end{aligned}$$

Entonces tenemos:

$$n \leq \dim(\ker(p(f))) + \dim(\ker(q(f))) \leq n \Rightarrow \text{la suma es } n.$$

$$\ker(p(f)) + \ker(q(f)) \leq E \quad (\dim(E) = n) \quad y$$

$$\ker(p(f)) \cap \ker(q(f)) = \{0\}$$

$$\Rightarrow \ker(p(f)) \oplus \ker(q(f)) = E$$

¿Cuáles son los polinomios mínimos de la restricción de f a esos dos subespacios invariantes en que se descompone E ? Sean $\bar{p}(x)$ y $\bar{q}(x)$ respectivamente. Como $p(x)$ y $q(x)$ son anuladores de la restricción: $p(x) \in (\bar{p}(x))$ y $q(x) \in (\bar{q}(x))$. Además,

$\bar{p}(x) \cdot \bar{q}(x)$ es anulador de f porque:

$$\begin{aligned} \bar{p}(f) \cdot \bar{q}(f) &= c(f) \cdot p(f) \cdot q(f) = c(f) \cdot \text{pol. min.}(f) = 0 \\ &(\text{c}(x) \in \mathbb{K}[x] \mid p(x) \cdot q(x) = \bar{p}(x) \cdot \bar{q}(x) \cdot c(x)) \end{aligned}$$

O mejor: $u \in E$ es $u = u_1 + u_2$, $u_1 \in \ker(p(f))$ y $u_2 \in \ker(q(f))$

$$\bar{p}(f) \cdot \bar{q}(f) = \bar{q}(f) \bar{p}(f)(u_1) + \bar{p}(f) \bar{q}(f)(u_2) = \bar{0} + \bar{0} = \bar{0}$$

Así, por una parte:

$\bar{p}(x) \cdot \bar{q}(x) \in (\text{pol. min.}(x))$ y por otra parte lo divide $\Rightarrow \text{grad}(\bar{p}(x) \cdot \bar{q}(x)) \leq \text{grad} \text{pol. min.}(x) \Rightarrow$
 $\Rightarrow \text{grad}(\bar{p}(x) \cdot \bar{q}(x)) = \text{grad}(\text{pol. min.}(x))$ y al ser múltiplo:

$$\bar{p}(x) \cdot \bar{q}(x) = \text{pol. min.}(x) = p(x) \cdot q(x) \Rightarrow \widetilde{p(x)} = p(x) \text{ y}$$
$$\bar{q}(x) = q(x) \quad (p(x) \in (\bar{p}(x)), \text{ y lo divide etc. análogo } q(x)).$$

Es decir: si $\text{pol. min.}(x) = p(x) \cdot q(x)$ y definimos $\ker(p(f))$ y $f|_{\ker(p(f))}$, el polinomio mínimo de f restringido al subespacio es $p(x)$ (análogo a q) y además los subespacios son suma directa.

Naturalmente, si ahora $p(x)$ ($\circ q(x)$), se descompone en factores primos, podemos descomponer $\ker(p(f))$ ($\circ \ker(q(f))$) en suma de subespacios invariantes y proceder así tantas veces como podamos.

Así, podemos descomponer el polinomio mínimo en producto de factores primos entre sí, asociar un espacio invariante a cada uno de ellos de manera que el polinomio mínimo sea ese factor primo (con su multiplicidad correspondiente) y estos subespacios sean suma directa del espacio. Así obtenemos el siguiente teorema.

Teorema 4.4 (primer teorema de descomposición)

Si el polinomio mínimo de $f \in \text{End}(E)$ es

$$\text{pol. min}_f(x) = m_1(x)^{n_1} \cdot \dots \cdot m_r(x)^{n_r}, \quad (1)$$

donde $m_1(x), \dots, m_r(x)$ son factores irreducibles, el espacio E es suma directa de subespacios invariantes

$$E = E^1 \oplus \dots \oplus E^r$$

de forma que el polinomio mínimo de la restricción de f a E^i es $m_i(x)^{n_i}$. Esta descomposición es única:

$$E^i = \ker(m_i(f)^{n_i}), \quad i = 1, \dots, r$$

dem:

La prueba está ya hecha en los páginas 24-27.
Falta por demostrar la unicidad de la descomposición.

Supongamos que tenemos una descomposición en subespacios invariantes:

$$E = E^1 \oplus \dots \oplus E^r$$

de la cual lo único que sabemos es que el polinomio mínimo de $f|_{E^i}$ es $m_i(x)^{n_i}$ para $i = 1, \dots, r$.

Esta última condición implica que: $E^i \subset \ker(m_i(\mathcal{F})^{n_i})$,

Veamos que es cierto:

$$m_i(x) = p(x) = \text{pol. min } \mathcal{F}|_{E^i}(x).$$

Sea $v \in E^i$. Por ser $p(x)$ polinomio mínimo de $\mathcal{F}|_{E^i}$,

$\forall v \in E^i, \text{ pol. min } \mathcal{F}|_{E^i}(v) = 0 \Rightarrow v \in \ker(p(x)) = \ker(m_i(\mathcal{F})^{n_i})$,
y la inclusión es cierta. $\Rightarrow \dim(E^i) \leq \dim(\ker(m_i(\mathcal{F})^{n_i}))$

De aquí deducimos:

$$\begin{aligned} n &= \dim(E^i) + \dots + \dim(E^r) \leq \\ &\downarrow \\ &\text{hipótesis} \end{aligned}$$

$$\leq \dim(\ker(m_1(\mathcal{F})^{n_1})) + \dots + \dim(\ker(m_r(\mathcal{F})^{n_r})) = n$$

\Rightarrow La desigualdad tiene que ser, pues, una igualdad y
todas las inclusiones anteriores tienen que ser igualdades:

Como $E^i \cap E^j = \{0\} \quad \forall i \neq j$ y $\ker(m_i(\mathcal{F})^{n_i}) \cap \ker(m_j(\mathcal{F})^{n_j}) = \{0\}$

$\forall i \neq j$ y $E^i \subset \ker(m_i(\mathcal{F})^{n_i})$ la única posibilidad
para que el \leq sea una igualdad es que

$$\dim(E^i) = \dim(\ker(m_i(\mathcal{F})^{n_i})) \Rightarrow E^i = \ker(m_i(\mathcal{F})^{n_i})$$

la descomposición es única.

(Si $\dim(E^i) \neq \dim(\ker(m_i(\mathcal{F})^{n_i}))$, como $E^i \subset \ker(m_i(\mathcal{F})^{n_i}) \Rightarrow$

$$\Rightarrow \dim(E^i) < \dim(\ker(m_i(\mathcal{F})^{n_i})) \Rightarrow n = \sum_{i=1}^r \dim(E^i) < \sum_{i=1}^r \dim(m_i(\mathcal{F})^{n_i})$$

, que es una contradicción $\Rightarrow \dim(E^i) = \dim(\ker(m_i(\mathcal{F})^{n_i})) \quad \forall i$)

(1) Recordar que en $\mathbb{k}[x]$ la descomposición de un polinomio en factores monios irreducibles es única

La descomposición de E en suma directa de subespacios invariantes reduce el estudio del comportamiento de f al estudio de sus restricciones a cada uno de los subespacios. Si escribimos la matriz de f en una base de E formada por bases de cada uno de los subespacios, obtenemos

$$A = \begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ 0 & & \ddots A_r \end{pmatrix}.$$

La matriz está formada por matrices A_1, \dots, A_r con la diagonal sobre la de A , y 0 en el resto de posiciones.

El estudio de A se reduce, pues, al de las matrices A_i , que son precisamente las matrices de las restricciones de f a cada uno de los subespacios en que se descompone E .

Observación:

Está probado del año pasado el determinante de una matriz de bloques triangular (una diagonal es triangular) es producto de los determinantes de los bloques. Es decir, en nuestro caso:

$$\det(A) = \det(A_1) \cdot \det(A_2) \cdot \dots \cdot \det(A_r)$$

Proposición (4.5) (pág. 373 libro Vera, prop 8.12)

Si $k \in \mathbb{K}$ es una raíz del polinomio característico de $h \in \text{End}_{\mathbb{K}}(V)$, entonces k es también raíz del pol. min. (h).

dem:

Sea v un vector propio asociado a k , es decir: $h(v) = kv$. Denotamos pol. min. (h) = $p(x)$. (v vector propio $\Rightarrow v \neq \bar{0}$).

Por ser el polinomio mínimo, $p(h) = 0 \Rightarrow \forall v \in V, p(h)(v) = \bar{0}$

y en particular, $p(h)(v) = \bar{0} \Rightarrow$

$$\Rightarrow \sum_{i=0}^m a_i h^i(v) = \bar{0}, \text{ con } p(x) = \sum_{i=0}^m a_i x^i.$$

$$\begin{aligned} \text{Como } h(v) = k \cdot v \Rightarrow h^m(v) &= h^{m-1}(h(v)) = h^{m-1}(kv) = \\ &= k h^{m-1}(v) \Rightarrow h^m(v) = k^m \cdot v \end{aligned}$$

Por tanto:

$$\bar{0} = \sum_{i=0}^m a_i h^i(v) = \sum_{i=0}^m (a_i \cdot k^i \cdot v) = \left[\sum_{i=0}^m (a_i k^i) \right] v = p(k) \cdot v = \bar{0}$$

Como $v \neq \bar{0} \Rightarrow p(k) = 0 \Rightarrow k$ es también raíz del

pol. min. (h) \square

Teorema 4.6 (de diagonalización)

Un endomorfismo es diagonalizable \Leftrightarrow

\Leftrightarrow su pol. min. (h) se descompone en factores lineales no repetidos.

Dem.:

(\Leftarrow)

Sea $\text{pol. min.}(x) = (x - a_1) \cdots (x - a_r)$, $a_i \neq a_j \forall i \neq j$

Por 4.4, $E = E^1 \oplus \cdots \oplus E^r$, donde: $E^i = \ker(h - a_i \text{Id})$

Observamos que $E^i = V(a_i)$, subespacio de vectores propios del valor propio a_i . Observamos que se tienen bases de vectores propios para cada subespacio y tenemos una base de E formada por vectores propios cuya matriz asociada a h es diagonal.

(Basta aplicar que tiene n valores propios distintos $\Rightarrow h$ es diagonalizable (proposición 8.8 pg 365 libro Vera)).

(\Rightarrow)

E diagonalizable $\Leftrightarrow \exists \beta = \{e_1^1, \dots, e_n^1, e_1^2, \dots, e_n^2, \dots, e_1^r, \dots, e_n^r\}$ formada por vectores propios de h . (Suponemos que si $j=i$, e_t^j y e_t^i están asociados al mismo valor propio).

Ponemos $E^i = \langle e_1^i, \dots, e_n^i \rangle$ tenemos que:

$$E = E^1 \oplus \cdots \oplus E^r$$

Tomemos $h|_{E^i}$. Sea $p(x) = -a_i + x$, Entonces:

$$p(h|_{E^i}) = -a_i \text{ y } h|_{E^i} = -a_i I_d \text{ y } a_i I_d = 0 \Rightarrow$$

$\Rightarrow (x-a_i)$ es anulador de h . Observamos que es mínimo, pues si tuviera menor grado sería $p(x) = a_0$, $a_0 \neq 0$ y entonces, tendríamos que todos sus múltiplos son anuladores

$$\text{de } h|_{E^i}. \text{ Contraseña: } p(x) = a_0 \cdot \left(-\frac{a_j}{a_0} + \frac{x}{a_0} \right) = -a_j + x$$

$$p(h|_{E^i}) = -a_j I_d + h|_{E^i} = -a_j I_d + a_i I_d = (-a_j + a_i) \cdot I_d$$

que no es necesariamente nulo, pues $i \neq j \Rightarrow a_i + a_j \Rightarrow (a_i - a_j) \neq 0$ e I_d no es necesariamente nulo.

\Rightarrow Polinomio de menor grado mínimo que cumple $p(h|_{E^i}) = 0$

$$\text{es } p(x) = x - a_i.$$

Así, $\forall i$, el polinomio mínimo de $g|_{E^i}$ es

$$\text{pol. min.}(h|_{E^i}) = (x - a_i)$$

$\forall i$, por 4.1, $\text{pol. min.}(h|_{E^i})$ divide a $\text{pol. min.}(h)$.

(o incluso por 4.5).

Observamos que como $(x - a_i)$ divide a $\text{pol. min.}(h) \quad \forall i = 1, \dots, r$,

como $\forall i \neq j$ $(x - a_i)$ es coprimo con $(x - a_j)$. Ha de

darse que $\text{pol. min.}(h) = (x - a_1)(x - a_2) \cdots (x - a_r) \circ C(x)$

con $C(x) \in \mathbb{K}[x]$. (Si no fuera así, y no tuviera a $(x - a_i)$

como factor, entonces este no lo dividiría y llegaríamos a

una contradicción $\Rightarrow (x - a_1)(x - a_2) \cdots (x - a_r)$ divide al $\text{pol. min.}(h)$).

Ahora vamos a ver que es un anel ideal \Rightarrow
 $(x-a_1) \cdots (x-ar) \in (\text{pd. min.}(h))$.

Si es múltiple del polinomio mínimo $\Rightarrow = \text{pol. min.}(h) \cdot C(x)$,
 $C(x) \in \mathbb{K}[x]$.

Como acabamos que ver que lo divide \Rightarrow pol

$$\text{pol. nún. } (h) = (x - a_1) \cdots (x - a_r) \cdot c(x), \quad c(x) \in k[x].$$

Juntando ondas.

$$\Rightarrow C(x) = C'(x) = 1 \quad \text{und} \quad \text{pol. min.}(h) = (x-a_1) \cdots (x-ar).$$

Vemos pues que es un onubador.

Sea $u \in E$. Por la suma directa $\Rightarrow u = u_1 + u_2 + \dots + u_r$ con

$u_i \in E^i$, $i = 1, \dots, r$, se tiene: ①

Son aplicaciones lineales y
reorganizamos la
↑ = composición (que se
puede hacer porque
 $(x-a) \cdot (x-ar)$ pertenece a
un ideal etc.

$$\begin{aligned}
 & (\mathbf{f} - a_1 \mathbf{Id}) \circ (\mathbf{f} - a_2 \mathbf{Id}) \circ \dots \circ (\mathbf{f} - a_r \mathbf{Id})(\mathbf{u}) = \text{composición (que se} \\
 & \text{puede hacer porque} \\
 & \boxed{(-a) \dots (x-a)} \text{ pertenece a} \\
 & \text{un ideal etc.} \\
 & = (\mathbf{f} - a_2 \mathbf{Id}) \circ (\mathbf{f} - a_3 \mathbf{Id}) \circ \dots \circ (\mathbf{f} - a_r \mathbf{Id})(\mathbf{u}_1) + \\
 & + (\mathbf{f} - a_1 \mathbf{Id}) \circ (\mathbf{f} - a_3 \mathbf{Id}) \circ \dots \circ (\mathbf{f} - a_r \mathbf{Id})(\mathbf{u}_2) + \\
 & \dots \\
 & + (\mathbf{f} - a_1 \mathbf{Id}) \circ (\mathbf{f} - a_2 \mathbf{Id}) \circ \dots \circ (\mathbf{f} - a_r \mathbf{Id})(\mathbf{u}_r) \\
 & = (\mathbf{f} - a_2 \mathbf{Id}) \circ (\mathbf{f} - a_3 \mathbf{Id}) \circ \dots \circ (\mathbf{f}(\mathbf{u}_1) - a_1 \mathbf{Id}(\mathbf{u}_1)) + \\
 & \quad \overbrace{\mathbf{a}_1 \mathbf{u}_2 - \mathbf{a}_1 \mathbf{u}_1}^{\mathbf{a}_2 \mathbf{u}_2 \circ \dots \circ -\mathbf{a}_2 \mathbf{u}_2} \\
 & \quad (\mathbf{f} - a_1 \mathbf{Id}) \circ (\mathbf{f} - a_3 \mathbf{Id}) \circ \dots \circ (\mathbf{f}(\mathbf{u}_2) - a_2 \mathbf{Id}(\mathbf{u}_2)) + \\
 & \quad \overbrace{\mathbf{a}_2 \mathbf{u}_3 - \mathbf{a}_2 \mathbf{u}_2}^{\mathbf{a}_3 \mathbf{u}_3 \circ \dots \circ -\mathbf{a}_3 \mathbf{u}_2} \\
 & \quad \vdots \\
 & \quad + (\mathbf{f} - a_1 \mathbf{Id}) \circ (\mathbf{f} - a_2 \mathbf{Id}) \circ \dots \circ (\mathbf{f}(\mathbf{u}_r) - a_{r-1} \mathbf{Id}(\mathbf{u}_r)) \\
 & \quad \overbrace{\mathbf{a}_{r-1} \mathbf{u}_r - \mathbf{a}_{r-1} \mathbf{u}_r}^{\mathbf{a}_r \mathbf{u}_r \circ \dots \circ -\mathbf{a}_r \mathbf{u}_r} \\
 & \quad \overbrace{\mathbf{0}}^{\mathbf{0}}
 \end{aligned}$$

→ hacemos:
 $(\mathbf{f} \circ \mathbf{g})(\mathbf{v}) = \mathbf{f}(\mathbf{g}(\mathbf{v}))$,
 sólo para el elemento
 final. Obtenido:
 $\mathbf{f}'(\mathbf{f}(\mathbf{u}_r) - a_{r-1} \mathbf{Id}(\mathbf{u}_r))$
 $= \mathbf{f}'(\mathbf{u}_r \cdot a_r - a_r \cdot \mathbf{u}_r) =$
 $= \mathbf{f}'(\mathbf{0}) = \mathbf{0}$
 ↓ \mathbf{f}' lineal

$= \bar{0} + \bar{0} + \dots + \bar{0} = \bar{0} \Rightarrow (x-a_1) \cdots (x-ar)$ es
un anulador \downarrow
ya visto

\Rightarrow el polinomio mínimo se descompone en factores lineales
no repetidos. \square

(1)

Queremos ver que $p(x) = (x-a_1) \cdots (x-ar)$ es un
anulador $\Rightarrow p(x) \in \ker(\Phi f) = \{p(x) \in k[x] \mid \Phi f(p(x)) = p(f) = 0\}$.
Y vemos de una de las propiedades que se cumplen para Φf

es:

$$\Phi f(p(x) \cdot q(x)) = p(f) \circ q(f) = \Phi f(p(x)) \circ \Phi f(q(x))$$

(página 157 libro M. Castellet).

Observación:

Este teorema es muy útil porque nos permite ver si una
matriz es diagonalizable observando su polinomio mínimo de f .

(Nuevo capítulo siguiente cosa)

VIII. 5 Grado del polinomio mínimo

Por la definición original que dieron de pol. mín. (h), sabemos que $\text{grad}(\text{pol. mín.}(h)) \leq n^2$. Vamos a buscar una cota mejor para el grado del polinomio mínimo.

Proposición 5.1

Si $\dim(E) = n$ y $h \in \text{End}_{\mathbb{K}}(V)$. Entonces:

$$\text{grad}(\text{pol. mín.}(h)) < n$$

($m_i(x)$ es irreducible, no tiene porque ser lineal.)

dem:

$$\text{Sea pol. mín.}(h) = \overbrace{m_1(x)^{n_1} \cdot m_2(x)^{n_2} \cdots m_r(x)^{n_r}}^{\sim} \text{ y}$$

$E = E^1 \oplus \cdots \oplus E^r$ la descomposición de 4.4. Basta

$$\text{Ver que } \text{grad}(m_i(x)^{n_i}) = k_i \leq \dim(E^i) \quad \forall i \in \{1, \dots, r\}$$

$$(\Rightarrow \text{grad}(\text{pol. mín.}) = n_1 + n_2 + \cdots + n_r \leq \dim(E^1) + \cdots + \dim(E^r) = n).$$

Dado que $m_i(x)^{n_i}$ es el polinomio mínimo de la restricción de f a E^i , $\exists v_i \in E^i$ t.q. $m_i(f)^{n_i}(v_i) = 0$ pero $m_i(f)^{n_i-1}(v_i) \neq 0$ (si no, podríamos tomar $m_i(x)^{n_i-1}$ o de menor grado anulador de la restricción de f que contradice que $m_i(x)^{n_i}$ sea pol. min.).

Ase, el polinomio mínimo de v_i es $m_i(x)^{n_i}$ y por (3.1) $\{v_i, f(v_i), \dots, f^{k_i-1}(v_i)\}$ son linealmente independientes con $k_i = \text{gr}(m_i(x)^{n_i})$.

Como $m_i(x)$ no tiene porque ser lineal, será

$$\text{gr}(m_i(x)) \cdot n_i = \text{gr}(m_i(x)^{n_i})$$

Como es un subconjunto \mathbb{k} -libre de un espacio E^i de dimensión $\dim(E^i)$, necesariamente ha de ser:

$$k_i \leq \dim(E^i)$$

(pues si fuera mayor, sería un conjunto de vectores de cardinal mayor al de un \mathbb{k} -libre maximal y necesariamente sería \mathbb{k} -ligado \Rightarrow contradice que es \mathbb{k} -libre \Rightarrow ha de ser igual o menor).

Así:

$$\begin{aligned} \text{grad}(\text{pol. min.}(h)) &= k_1 + k_2 + \dots + k_r \leq \\ &\leq \dim(E^1) + \dim(E^2) + \dots + \dim(E^r) = n \end{aligned}$$

□

VIII. 6 El teorema de Cayley-Hamilton

En 4.5 probamos que los ceros del polinomio característico dividen al polinomio mínimo.

Vemos el recíproco.

Proposición 6.1

a es un cero de $\text{pol. min.}(h) \Leftrightarrow a$ es un cero de $\text{pol. car.}(h) = P_f(x)$.

dem.:

\Leftrightarrow) Es la proposición 4.5.

\Rightarrow

Si a es un cero de pol. min. $(h) = \text{mf}(x) \Rightarrow$
 $\Rightarrow \text{mf}(x) = (x-a) \cdot m_1(x) \quad (m_1(x) \in K[x]).$

Afirmamos que $\exists u \in E$ t.q. $m_1(f)(u) \neq \bar{0}$. En efecto, si
 $\forall u \in E \quad m(f)(u) = \bar{0} \Rightarrow m_1(x)$ es anulador de f . Lo cual
es una contradicción pues por ser $\text{mf}(x)$ el pol. min. \Rightarrow
Los anuladores son $(\text{mf}(x))$ pero $m_1(x) \notin (\text{mf}(x))$. Así,
ha de existir dicho vector.

Veamos que $w = m_1(f)(u)$ es un vector asociado al valor
propio a :

$$(f - a\text{Id})(w) = (f - a\text{Id})(m_1(f)(u)) \underbrace{(f - a\text{Id}) \circ (m_1(f))}_{(\text{recordar } \Phi_f \text{ y el ideal de } K[x])}(u) =$$

$$= \text{mg}(f)(u) = \bar{0} \quad \text{por ser mg el polinomio mínimo.}$$

Por tanto, a es un cero de $P_f(x)$. \square

No validos aún.

$$\left(\begin{array}{l} (P_f(f)(u) = ((\text{mg}(f)) \circ C(f))(u) = (C(f))(\text{mg}(f)(u)) = \bar{0} \\ P_f(x) = \text{mg}(x) \cdot C(x) \quad \downarrow \quad \left. \begin{array}{l} \text{(comutativo por pertenecer)} \\ \text{de ideal} \end{array} \right\} \quad \rightarrow \quad \begin{array}{l} \text{Aún no} \\ \text{hemos probado!} \end{array} \\ \in K[x] \quad \in K[x] \end{array} \right) \quad \left. \begin{array}{l} \text{f lineal} \\ \bar{0} \end{array} \right\} \quad P_f(x) \in (\text{mg}(x))$$

(1)

$$\Phi_f(p(x) \cdot q(x)) = p(f) \circ q(f) = \Phi_f(p(x)) \circ \Phi_f(q(x))$$

Teorema 6.2

Si el pol. min. (f) = $m_f(x)$ y el pol. cor (f) = $p_f(x)$ se descomponen en factores lineales, entonces $p_f(x)$ es un anulador de f ; esto es, $p_f(f) = 0$. (\Leftarrow $p_f(x) \in (m_f(x))$)

dem.:

Sea $m_f(x) = (x - a_1)^{n_1} \cdots (x - a_r)^{n_r}$ y sea

$E = E^1 \oplus \cdots \oplus E^r$ la descomposición de (4.4). La matriz de f en una base formada por las bases de los subespacios E^i es de la forma:

$$A = \begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ 0 & & \ddots A_r \end{pmatrix}$$

Si $P_i(x)$ es el polinomio característico de A_i (de $f|_{E^i}$). Entonces necesariamente:

$$P_f(x) = P_1(x) \cdot P_2(x) \cdot P_3(x) \cdots P_r(x)$$

$$(\det(A - x\text{Id})) = \det(A_1 - x\text{Id}) \cdot \det(A_2 - x\text{Id}) \cdots \det(A_r - x\text{Id})$$

Como $P(x)$ se descompone en factores lineales, así lo hará de hacer los $P_i(x)$. Además, sus ceros son los del pol. min de E^i , con única cero ($x - a_i$). $\Rightarrow P_i(x) = (x - a_i)^{m_i}$ con $m_i = \dim(E^i)$. Por (5.1), $n_i \leq m_i \Rightarrow \forall i, (x - a_i)^{n_i}$ divide a $P_i(x) \Rightarrow (x - a_1)^{n_1} \cdots (x - a_r)^{n_r}$ divide a $P_1(x) \cdots P_r(x) = P(x) \Rightarrow m_f(x)$ divide a $P(x) \Rightarrow P(x) \in (m_f(x)) \Rightarrow P(x)$ es un anulador de f . \square

Observación:

El resultado (6.2) es válido en condiciones mucho más generales (Teorema de Cayley - Hamilton). Para demostrarlo, sin embargo, necesitamos utilizar teoremas de estructura para módulos sobre dominios de ideales primos (Libro Vera), por tanto, aquí nos limitaremos a dar la idea de cómo se procede.

Si $A \in \text{Mat}_{n \times n}(\mathbb{K})$, podemos referirnos al pol. car. de A , $P_A(x)$. y al pol. min. de A $m_A(x)$ tal y como hemos hecho hasta ahora.

Así, $m_A(x)$ será un polinomio de grado mínimo del ideal $\{p(x) \in \mathbb{K}[x] \mid p(A) = 0\}$, donde:

$$p(x) = a_0 + a_1 x + \dots + a_n x^n \rightsquigarrow p(A) = a_0 I_n + a_1 A + \dots + a_n A^n.$$

Si $P_A(x)$ y $m_A(x)$ se descomponen en factores lineales, (6.2) asegura que:

$$P_A(A) = 0$$

Sea ahora A una matriz real. Como $\mathbb{R} \subset \mathbb{C}$, A es también una matriz compleja y su polinomio característico es el mismo: $P_A(x) = \det(A - x \text{Id})$. Entonces, como \mathbb{C} es algebraicamente cerrado;

$$P_A(A) = 0$$

y naturalmente, esta igualdad vale también en \mathbb{R} , pese a que en

Vez de todo factores lineales tenemos algún factor no lineal (motivo por el que habíamos ampliado a \mathbb{C}).

Este roazonamiento hecho para los cuerpos \mathbb{R} y \mathbb{C} sirve para los cuerpos cualesquiera $K \subset K'$ tales que todo polinomio de $K'[x]$ se descomponga en factores lineales. Se puede demostrar (excepto el objetivo de este curso) que para todo cuerpo K existe un cuerpo KK' denominado clausura algebraica de K (abi aplicaciones 6.2 para resolver el teorema). Es decir, podemos ampliar K a un cuerpo algebraicamente cerrado $(K'[x])$, descomponer en lineales $p(x)$ y demostrarlo.

(Idea: x^2+1 irreducible en \mathbb{R} . En \mathbb{C} $x^2+1 = (x-i)(x+i)$, factores lineales $\Rightarrow p(A) = (A-i\text{Id})(A+i\text{Id}) = 0$ y como $p(A) = A^2 + \text{Id} \Rightarrow p(A) = 0$ también en \mathbb{R} , lo que queríamos probar).

Obtendríamos así el siguiente teorema:

Teorema 6.3 (de Cayley - Hamilton)

El pol. min. (h) divide siempre al pol. cor (h).

demos:

No va a ser demostrado aquí, leer observación previa.

Observación:

Este teorema proporciona un método para calcular el pol. min. (h). Si $P_h(x)$ es el pol. car. (h), lo descomponemos en factores irreducibles y buscamos el menor de sus divisores $q(x)$ tal que $q(8) = 0$. Este será $m_f(x)$.

VIII.7 Matriz canónica (general) de un endomorfismo.

El teorema de descomposición (4.4) permite reducir el estudio de un endomorfismo f al estudio de sus restricciones a ciertos subespacios invariantes E^i . En casos particulares podemos aplicar (4.6) para obtener una matriz que diagonalice $f|_{E^i}$. Vamos a estudiar ahora el caso general.

(Libro Vera).

Definición:

Sea $v \in V$ y $h \in \text{End}_{\mathbb{K}}(V)$. Sea $\Omega = \{W \mid W \leq V \text{ t.q. } v \in W \text{ y } h(W) \subseteq W\}$. Como $V \in \Omega$, Ω es no vacío. Sea:

$$C(v, h) = \bigcap_{W \in \Omega} W = \bigcap \{W \mid W \leq V \text{ t.q. } v \in W \text{ y } h(w) \subseteq W\}$$

(Observar, $C(v, h)$ es un subespacio de V , pues la intersección de subespacios es subespacio (pág. 275, proposición 7.9)).

$C(v, h)$ es el menor subespacio de V que contiene al vector v y es h -invariante (los de V y h -invariante le vienen por

definición, es el menor subespacio porque si $W \subseteq V$ y W es h -invariante, (el menor) entonces $W \subseteq C(v, h)$ y $C(v, h) \subseteq W$ por def. por tanto si es el menor, $C(v, h) = W$ y es el menor también).

Es claro que:

$$C(v, h) = \{f(h)(v) \mid f(x) \in k[x]\} = k[h](v)$$

(por una parte, $f(x) = 1 \in k[x]$ y $f(h)(v) = \text{Id}(v) = v \in \{\dots\}$. y probemos que es h -invariante $\Rightarrow \{\dots\} \subseteq S_2 \Rightarrow C(v, h) \subseteq \{\dots\}$. Si $v \in \{\dots\}$, $f(h)(v) \in \{\dots\}$ y $f(x) \in k[x] \Rightarrow v \in C(v, h)$ y $C(v, h) \subseteq \{\dots\}$ Idea más o menos).

Así denominamos a $C(v, h)$ el subespacio cíclico de V relativo a h .

$$C(v, h) = \{f(h)(v) \mid f(x) \in k[x]\} = k[h](v) = \\ = \bigcap \{W \mid W \subseteq V \text{ t.q. } v \in W \text{ y } h(w) \in W\}$$

$$C(v, h) = k[h](v) \Rightarrow \boxed{\langle v, f(v), f^2(v), \dots \rangle = C(h, v)} \rightarrow \underline{\text{Clave}}$$

En efecto:

$$(2) \quad W \subseteq C(v, h) \Rightarrow \exists p(x) \in k[x] \text{ t.q. } p(f)(v) = w \Rightarrow$$

$$\Rightarrow a_0 v + a_1 f(v) + \dots = w \Rightarrow w \in \langle v, f(v), \dots \rangle$$

$$(3) \quad w \in \langle v, f(v), \dots \rangle \Rightarrow w = a_0 v + a_1 f(v) + \dots \Rightarrow \text{sea } p(x) \in k[x]$$

$$\text{t.q. } p(x) = a_0 + a_1 x + \dots \text{ Entonces: } p(f)(v) = w \Rightarrow w \in k[h](v)$$

$$\Rightarrow w \in C(v, h)$$

Proposición (8.18) (Libre Vera)

Sea $v \in V - \{0\}$ y $h \in \text{End}_{\mathbb{K}}(V)$. Si s es el menor entero tal que $\{v, h(v), \dots, h^s(v)\}$ es \mathbb{K} -ligado, entonces, existen escalares $a_0, a_1, \dots, a_{s-1} \in \mathbb{K}$ tales que:

$$h^s(v) = a_0 + a_1 h(v) + \dots + a_{s-1} h^{s-1}(v),$$

$p(x) = x^s - a_{s-1}x^{s-1} - \dots - a_1x - a_0$ es el polinomio mínimo de $h|_{C_{V,h}}$, $\dim_{\mathbb{K}} C_{V,h} = s$ y la matriz coordenada de $h|_{C_{V,h}}$ respecto de $\{v, h(v), \dots, h^{s-1}(v)\}$ es:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{s-1} \end{pmatrix}$$

demos:

$\{v, h(v), \dots, h^s(v)\}$ \mathbb{K} -ligado \Rightarrow (Por 3.1) $h^s(v)$ es una ligadura $\Rightarrow h^s(v) = a_0 v + a_1 h(v) + \dots + a_{s-1} h^{s-1}(v)$.

Por 3.1:

$h^t(v) \in \langle v, h(v), \dots, h^{s-1}(v) \rangle \quad \forall t \geq s$ y en consecuencia:

$C(h,v) = \mathbb{K}v \oplus \mathbb{K}h(v) \oplus \dots \oplus \mathbb{K}h^{s-1}(v)$ porque:

$\{v, h(v), \dots, h^{s-1}(v)\}$ es \mathbb{K} -libre maximal $B \subset \langle v, h(v), \dots, h^{s-1}(v) \rangle \subset$

$C \subset \langle v, h(v), \dots, h^{s-1}(v) \rangle = C(v, h) \Rightarrow$

$\Rightarrow \{v, h(v), \dots, h^{s-1}(v)\}$ es base de $C(v, h) \Rightarrow \dim_{\mathbb{K}} C(v, h) = s$

(Además, por ser \mathbb{K} -libre $\mathbb{K}v \cap \mathbb{K}h(v) \cap \dots \cap \mathbb{K}h^{s-1}(v) = \{0\}$).

Respecto de esta base:

$$h(v) = \alpha v + 1h(v) + \dots + 0h^{s-1}(v)$$

$$h(h(v)) = h^2(v) = \alpha v + 0h(v) + 1h^2(v) + \dots + 0h^{s-1}(v)$$

$$h(h^{s-1}(v)) = h^s(v) = \alpha_0 v + \alpha_1 h(v) + \dots + \alpha_{s-1} h^{s-1}(v)$$

$$\Rightarrow M_{\beta'}(h) = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_0 \\ 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \alpha_{s-1} \end{pmatrix}$$

$\alpha_0 \neq 0$. Pero
hacemos lo mismo.
para todos y ya.

Finalmente: si tomamos $p(x) \in \mathbb{K}[x]$ t.q.:

$$p(x) = x^s - \alpha_{s-1}x^{s-1} - \dots - \alpha_1x - \alpha_0 \text{ entonces}$$

$$p(g_1)(w), w \in C(v, h) \text{ y } g_1|_{C(v, h)} \rightarrow w = h^k(v) \quad \uparrow$$

$$\Rightarrow p(g_1)(h^k(v)) = h^s(h^k(v)) - \alpha_{s-1}h^{s-1}(h^k(v)) - \dots - \alpha_1h(h^k(v)) - \alpha_0h^k(v)$$

y como h es lineal, h^k también es lineal \Rightarrow hip.

$$\Rightarrow p(g_1)(h^k(v)) = h^k(h^s(v) - \alpha_{s-1}h^{s-1}(v) - \dots - \alpha_1h(v) - \alpha_0v) =$$

$$= h^k(\bar{0}) = \bar{0} \quad (h^k \text{ lineal})$$

$$\Rightarrow \forall w \in C(v, h) \quad p(g_1)(w) = 0 \Rightarrow p(g_1|_{C(v, h)}) = 0 \quad y$$

$p(x)$ es anulador de la restricción de f . $\Rightarrow p(x) \in (\underbrace{m g_1(x)}_{\text{pol. min. } g_1(x)})$

Además, como s es el mínimo que lo cumple por hipótesis.

grad. (pol. min. ($h|_{C(v, h)}$)) = s y como $p(x)$ divide a pol. min. ($h|_{C(v, h)}$)

y ambos son ménicos $\Rightarrow p(x) = \text{pol. min. } (h|_{C(v, h)})$.

Completando así la demostración. \square

Recapitulación:

$$C(u, g) = \mathbb{K}[g](v) = \langle u, g(u), g^2(u), \dots \rangle$$

$$\dim(C(u, g)) = s = \text{grad}(\text{pol. min.}(g|_{C(u, h)}))$$

$$\text{Si pol. min.}(g|_{C(u, h)}) = -a_0 - a_1 x - a_2 x^2 - \dots - a_{s-1} x^{s-1} + x^s$$

Respecto de $\beta = \{u, g(u), \dots, g^{s-1}(u)\}$ es $M_\beta(g)$:

$$M_\beta(g) = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{s-1} \end{pmatrix}$$

(Importante para calcular el pol. min.)

Teorema (8.19)

Sea $h \in \text{End}_\mathbb{K}(V)$ y $\{v_1, \dots, v_n\}$ una \mathbb{K} -base de V .

Entonces:

$$\text{pol. min.}(h) = \text{m.c.m.}\{\text{pol. min.}(h|_{C(v_i, h)}) \mid i=1, \dots, n\}$$

dem...

Sea $q(x) = \text{pol. min.}(h)$ y $q_i(x) = \text{pol. min.}(h|_{C(v_i, h)}) \quad \forall i \in \{1, \dots, n\}$.

Como es el pol. min.(h) $\Rightarrow q(h) = 0 \Rightarrow q(h|_{C(v_i, h)}) = 0$.

Luego, $q(x)$ anula $h|_{C(v_i, h)}$ $\Rightarrow q(x) \in (q_i(x)) \quad \forall i \in \{1, \dots, n\}$.

Así: $q_i(x)$ divide a $q(x) \quad \forall i \in \{1, \dots, n\}$ y si tomamos $p(x) = \text{mcm}(q_i(x))$, $p(x)$ divide a $q(x)$ (propiedades de

los polinomios en $\mathbb{K}[x]$). Con números: si 2 divide a 36 y 6 divide a 36, $\text{mcm}(2, 6) = 6$ divide a 36 etc. $\text{mcm}(36, 4) = 36 \mid 36$, $\text{mcm}(4, 9) = 36 \mid 36, \dots$).

Por construcción, $p(x)$ es un múltiplo de $q_i(x)$ y por tanto, anula $h|cc(v_i, h) \Rightarrow p(h)(v_i) = p(h|cc(v_i, h))(v_i) = 0$
 $\forall i \in \{1, \dots, n\}$. Tomamos $v \in V$ t.q. $v = z_1 v_1 + \dots + z_n v_n \Rightarrow$
 $\Rightarrow p(h)(v) = p(h|cc(v_1, h))(v_1) + \dots + p(h|cc(v_n, h))(v_n) = \bar{0} + \dots + \bar{0} = \bar{0} \quad (\forall v \in V)$

Así, $p(x)$ es anulador de $h \Rightarrow p(x) \in (q(x))$. Y
 $q(x)$ divide a $p(x)$.

Como $q(x) \in (p(x))$ y $q(x) \in (q(x)) \Rightarrow p(x) = q(x) \Rightarrow$
 $\Rightarrow \text{pol. min.}(h) = \text{m.c.m.}\{\text{pol. min.}(h|cc(v_i, h)) \mid i = 1, \dots, n\} \quad \square$

(1)
 $q(x) \in (p(x)) \Rightarrow q(x) = p(x) \cdot c_1(x), \quad c_1(x) \in \mathbb{K}[x]$
 $p(x) \in (q(x)) \Rightarrow p(x) = q(x) \cdot c_2(x), \quad c_2(x) \in \mathbb{K}[x]$
 $\Rightarrow q(x) = p(x) \cdot c_1(x) = q(x) \cdot c_1(x) \cdot c_2(x) \Rightarrow c_1(x) \cdot c_2(x) = 1$
 $\text{Com } c_i(x) \in \mathbb{K}[x] \Rightarrow c_1(x) = c_2(x) = 1 \Rightarrow p(x) = q(x)$

(Con números serán: $(a, b, c_1, c_2 \in \mathbb{N}^*)$)
 $a = c_1 \cdot b \quad \Rightarrow \quad a = c_1 \cdot b_1 = c_1 \cdot c_2 \cdot a \Leftrightarrow c_1 \cdot c_2 = 1$
 $b = c_2 \cdot a$

Como en \mathbb{N}^* no hay inversos para el producto, necesariamente
 $c_1 = c_2 = 1 \Rightarrow a = b$).

Con este teorema, tenemos un método para calcular
el pol. min. (h)!

(De ahora en adelante continuamos con el libro de Vera:
Cap. VIII pág. 383).

VIII. 4 Primera forma canónica de Jordan

Definición:

Sea $g \in \text{End}_{\mathbb{K}}(V)$. Decimos que g es un \mathbb{K} -endomorfismo nilpotente, si $\exists m \in \mathbb{N}$ tal que $g^m = 0$. Llamamos a $r \in \mathbb{N}$ el índice de nilpotencia de g , al menor entero r tal que $g^r = 0$.

Definición:

Sea $h \in \text{End}_{\mathbb{K}}(V)$ y $v \in V - \{0\}$. Diremos que v es h -cíclico de orden s , si se verifica que $h^s(v) = \overline{0}$, y además s es el menor entero positivo que cumple ésta relación. Dicho de otros palabras, si $h|_{\mathbb{K}[h](v)}$ es nilpotente de índice s .

Lema (8.20)

Sea $v \in V - \{0\}$ h -cíclico de orden s . Entonces:

$$\{v, h(v), \dots, h^{s-1}(v)\},$$

es una \mathbb{K} -base del espacio (h -cíclico) $\mathbb{K}[h](v) = W$ y la matriz coordenada de $(h+k \cdot \text{Id})|_W$ respecto a esta base es

$$\left(\begin{array}{cccc|c} k & 1 & 0 & \cdots & 0 \\ 0 & k & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & k \end{array} \right), \text{ para cada } k \in \mathbb{K}.$$

dem:

Supongamos que: $\{v, h(v), \dots, h^{s-1}(v)\}$ es \mathbb{k} -ligado. Entonces, $\exists c_i \in \mathbb{k}, c_i$ no necesariamente nulos (no todos nulos), tales que:

$$c_0 v + c_1 h(v) + \dots + c_{s-1} h^{s-1}(v) = \bar{0}$$

$$\text{Sea } f(x) = c_0 + c_1 x + \dots + c_{s-1} x^{s-1}. \Rightarrow f(h)(v) = \bar{0}.$$

Así, $\forall t \geq 0$:

$$\begin{aligned} f(h)(ht(v)) &= c_0 ht(v) + c_1 h(ht(v)) + \dots + c_{s-1} h^{s-1}(ht(v)) \\ &= ht(c_0 v + c_1 h(v) + \dots + c_{s-1} h^{s-1}(v)) = ht(f(h)(v)) = ht(\bar{0}) = \bar{0} \end{aligned}$$

\downarrow
h lineal.

linealidad
de h.

h lineal

ocabemos
de probar

$$\text{Por tanto, } \forall w \in W, f(h)(w) = f(h)\left(\sum_{i=0}^n h^i(v)\right) \stackrel{\text{h lineal}}{=} \sum_{i=0}^n f(h)(h^i(v)) \stackrel{\text{ocabemos de probar}}{=}$$

$$= \sum_{i=0}^n \bar{0} = \bar{0} \Rightarrow f(x) \text{ es anulador de } h|_W. \Rightarrow$$

pol min. ($h|_W$) divide a $f(x)$. $\Rightarrow \text{grad.}(f(x)) \leq s-1$,

que contradice la elección de $s \Rightarrow$ Es \mathbb{k} -libre, y por

ser h cálculo de orden s, $h^s(v) = h^{s+1}(v) = \dots = \bar{0} \Rightarrow$
es \mathbb{k} -libre maximal $\Rightarrow \{v, h(v), \dots, h^{s-1}(v)\}$ es base de W .

Tomemos ahora el escalar $k \in \mathbb{k}$ y el siguiente endomorfismo:

$h+k \cdot \text{Id}: V \rightarrow V$. Como $h(v)+kv \in W \Rightarrow h+k \cdot \text{Id}$

es un endomorfismo de W . (Siguiente cora).

$$(h+k)(hv) = h^2(v) + kh(v) \in W, (h+k)(h^s(v)) = h^{s+1}(v) + kh^s(v) \in W.$$

Suma de endomorf.

Observamos:

$$(h+k)(v) = k(v) + h(v) + 0h^2(v) + 0h^3(v) + \dots + 0h^{s-2}(v) + 0h^{s-1}(v)$$

$$(h+k)(h(v)) = 0 + k(h(v)) + h^2(v) + 0h^3(v) + \dots + 0h^{s-2}(v) + 0h^{s-1}(v)$$

$$(h+k)(h^2(v)) = 0 + 0 + kh^2(v) + h^3(v) + \dots + 0h^{s-2}(v) + 0h^{s-1}(v)$$

⋮

$$(h+k)(h^{s-2}(v)) = 0 + 0 + 0 + 0 + \dots + kh^{s-2}(v) + h^{s-1}(v)$$

$$(h+k)(h^{s-1}(v)) = 0 + 0 + 0 + 0 + \dots + 0 + kh^{s-1}(v)$$

Así, la matriz asociada es:

$$M_{\beta}(h+k) = \begin{pmatrix} k & 0 & 0 & \cdots & 0 & 0 \\ 1 & k & 0 & \cdots & 0 & 0 \\ 0 & 1 & k & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & k & 0 \\ 0 & 0 & 0 & \cdots & 1 & k \end{pmatrix} \quad \square$$

Definición:

A los matrices $M_{\beta}(h+k)$ del Lema 8.20 les
llamamos bloques básicos de Jordan pertenecientes a k .

Lema 8.21

Sea $g \in \text{End}(K(V))$ nilpotente. Entonces, cualquier endomorfismo de la forma $a_0 + a_1 g + a_2 g^2 + \dots + a_m g^m$ con $a_i \in K$ y $a_0 \neq 0$, es inversible.

dem:

Sea g -nilpotente. Por def. $\exists t \in \mathbb{N}$ tal que $g^t = 0$.

Sean $a_i \in K$, $a_i \rightarrow V_i \in \{1, \dots, m\}$ con $a_0 \neq 0$.

Consideremos el siguiente endomorfismo:

$$a_0 + a_1 g + a_2 g^2 + \dots + a_m g^m \quad (1)$$

$$\text{Sea } a = a_0$$

$$\text{Sea } h = a_1 g + a_2 g^2 + \dots + a_m g^m$$

Reescribimos (1) como:

$$a + h$$

$$\text{Sea } h^i = a_1 g^{i-1} + a_2 g^i + a_3 g^{i+1} + \dots + a_m g^{i+(m-1)}$$

Entonces:

$$h = (h^1 \circ g)$$

$$h^t = (h^1 \circ g)^t = (g(h^1))^t = (a_1 g + a_2 g^2 + \dots + a_m g^m)^t$$

Podemos tomar:

$$p(x) = a_1 + a_2 x + a_3 x^2 + \dots + a_m x^{m-1}$$

$$q(x) = 0 + x$$

$$\Rightarrow h = \bigoplus g(p(x) \cdot q(x)) = p(g) \circ q(g) = c(g), \quad c \in K[x]$$

$$\Rightarrow h^t = c(g)^t = \bigoplus g(c(x)^t)$$

$$\begin{aligned}
 h^t &= ((P(g) \circ q(g))^t)^t = (\text{Dg}(P(x) \circ q(x)))^t = \\
 &= (P(g) \circ q(g))^{t-1} \circ (P(g) \circ q(g)) = \\
 &= (\text{Dg}(P(x) \cdot q(x)))^{t-1} \circ \text{Dg}(P(x) \cdot q(x))
 \end{aligned}$$

En efecto: (Ejemplo)

$$\begin{aligned}
 h^2 &= h \circ h = (a_1 g + \dots + a_m g^m) \circ (a_1 g + \dots + a_m g^m) = \\
 &= a_1 g(a_1 g + \dots + a_m g^m) + \dots + a_m g(a_1 g + \dots + a_m g^m) = \\
 &= a_1^2 g^2 + a_1 a_2 g^3 + \dots + a_1 a_m g^{m+1} + \dots + a_m a_1 g^{m+1} + \dots + a_m g^{2m}
 \end{aligned}$$

Observamos que $\forall n$, en h todos los términos son potencias de g mayores o iguales a g^n . Tomando $n \geq t$, como g es nulpotente de índice t , $g^n = 0 \quad \forall n \geq t \Rightarrow h^t = 0 \quad \forall n \geq t$.

Observamos que:

$$\begin{aligned}
 (\underbrace{a_0 + h}_g) \circ (\underbrace{a_0^{-1} - a_0^{-2} h + a_0^{-3} h^2 + \dots + (-1)^{t-1} (a_0)^{-t}}_{\in \text{End}_{\mathbb{K}}(V)} h^{t-1}) &= \\
 &= a_0 \text{Id} \circ (a_0^{-1} - a_0^{-2} h + a_0^{-3} h^2 + \dots + (-1)^{t-1} (a_0)^{-t}) h^{t-1} + \\
 &\quad + h (a_0^{-1} - a_0^{-2} h + a_0^{-3} h^2 + \dots + (-1)^{t-1} (a_0)^{-t}) h^{t-1} = \\
 &= \text{Id} - a_0^{-1} h + a_0^{-2} h^2 + \dots + \underbrace{(-1)^{t-1} (a_0)^{-t+1}}_{0} h^{t-1} \\
 &\quad + a_0^{-1} h - a_0^{-2} h^2 + \dots + (-1)^{t-2} (a_0^{-t+2}) h^{t-1} + h^{t-1} (a_0)^{-t} h^t = \\
 &= \text{Id} + 0 + 0 + \dots + 0 + 0 = \text{Id} \\
 \Rightarrow \exists f = a_0^{-1} - a_0^{-2} h + \dots + (-1)^{t-1} (a_0)^{-t} h^{t-1} \in \text{End}_{\mathbb{K}}(V)
 \end{aligned}$$

$$t \cdot g \cdot g \circ f = f \circ g = \text{Id} \Rightarrow \exists f = g^{-1} \quad \square$$

Si hubiera un $a_i = 0$, simplemente descartamos el término del sumando y no hay problemas.

Lema 8.22

Sea $g \in \text{End}_{\mathbb{K}}(V)$ nulpotente, con índice s . Sea v g -cíclico de orden s y $t \in \mathbb{N}$, $t \leq s$. Sea $w \in \mathbb{K}[g](V)$ tal que $g^{s-t}(w) = \bar{0}$. Entonces, $\exists w_0 \in \mathbb{K}[g](V)$ tal que $w = g^t(w_0)$.

Observar que habríanos encontrado $w \in \mathbb{K}[g](V)$ tal que:

$g^r(w_0) \neq \bar{0} \quad \forall r < s, \quad g^s(w_0) = \bar{0} \quad \text{y} \quad g^r(w_0) = \bar{0} \quad \forall r \geq s$.

Dem:

Por el Lema 8.20, $\{v, g(v), \dots, g^{s-1}(v)\}$ es base de $\mathbb{K}[g](V)$. Así, existen $c_i \in \mathbb{K}$ t.q.:

$$w = c_0 v + c_1 g(v) + \dots + c_{s-1} g^{s-1}(v).$$

Por tanto:

$$\begin{aligned} \bar{0} &= g^{s-t}(w) = c_0 g^{s-t}(v) + c_1 g^{s-t+1}(v) + \dots + \\ &\quad + c_{s-1} g^{s-t+s-1}(v) = \underbrace{c_0 g^{s-t}(v)}_{\bar{0}} + \underbrace{c_1 g^{s-(t-1)}(v)}_{\bar{0}} + \dots + \underbrace{c_{s-1} g^{s-1}(v)}_{\bar{0}} + \\ &= c_0 g^{s-t}(v) + c_1 g^{s-(t-1)}(v) + \dots + c_{t-1} g^{s-1}(v) + \\ &\quad + \underbrace{c_t g^s(v)}_{\bar{0}} + \dots + \underbrace{c_{s-1} g^{2s-(t+1)}(v)}_{\bar{0}} = \\ &= c_0 g^{s-t}(v) + c_1 g^{s-(t-1)}(v) + \dots + c_{t-1} g^{s-1}(v) \quad (1) \end{aligned}$$

(porque $\forall r \geq s, g^r(v) = \bar{0}$)

Como $\{v, g(v), \dots, g^{s-1}(v)\}$ es base, $\{g^{s-t}(v), \dots, g^{s-1}(v)\}$ es \mathbb{k} -libre (pues está contenido en una base, \mathbb{k} -libre maximal).
 ⇒ La \mathbb{k} -c-l. igualada a $\bar{0}$ tiene coeficientes necesariamente nulos y $\Rightarrow \forall i \in \{0, \dots, t-1\}, c_i = 0$.

Así, volviendo a la relación inicial:

$$\begin{aligned} w &= \underbrace{c_0 v + c_1 g(v) + \dots + c_{t-1} g^{t-1}(v)}_{c_i = 0} + c_t g^t(v) + \dots + c_{s-1} g^{s-1}(v) = \\ &\quad \text{linealidad de } g \\ &= c_t g^t(v) + \dots + c_{s-1} g^{s-1}(v) = \\ &= g^t(c_t v + \dots + c_{s-1} g^{s-1-t}(v)) = \\ &= g^t(w_0) \quad \text{con } w_0 = c_t v + \dots + c_{s-1} g^{s-1-t}(v) \in \mathbb{k}[g](v) \end{aligned}$$

Si $t=s$, tenemos que: $g^{s-t}(w) = \bar{0}$ (hipótesis) $\Rightarrow \text{Id}(w) = \bar{0}$
 $\Rightarrow w = \bar{0}$. Y tomando v (por hip. $g^s(v) = \bar{0}$) \Rightarrow
 $\Rightarrow w = g^s(v) = g^t(v)$. \square

Lema 8.23 (2do Teorema de la descomposición)

Sea $g \in \text{End}_{\mathbb{k}}(V)$ nilpotente de índice s y $W = \mathbb{k}[g](v)$ con v g -cíclico de orden s . Entonces, $\exists U \subseteq V$ g -invariante tal que $V = W \oplus U$.

dem:

Buscamos $U \subseteq V$ g -invariante que complemente a W hasta V . Elegimos la $\dim_{\mathbb{k}}(U)$ para que sea la máxima posible que cumple estos condiciones (siguiente cor).

$$\dim_{\mathbb{K}}(U) = \max \{ |X| \text{ con }$$

$$X = \{ \dim_{\mathbb{K}}(T) \mid T \leq V, g\text{-invariante es } T \text{ y } T \cap W = \overline{\{0\}} \}$$

Como $\overline{0} \leq V$, g -invariante y $\overline{\{0\}} \cap W = \overline{\{0\}}$ $\Rightarrow 0 \in X$
 $\text{y } X \neq \emptyset$. Así, $\dim_{\mathbb{K}}(U)$ está bien definida.

Veamos que $V = U \oplus W$. Por red. abs.

Supongamos que $\exists z \in V - (U \oplus W)$. Como $g^s = 0$,
 $g^s(z) \in W + U$ ($\overline{0} = g^s(z) \in W + U$). Esto nos permite
afirmar: $\exists e, l \in \mathbb{K}$, $e < l$ t.q.

$$g^e(z) \notin W + U \text{ pero } g^l(z) \in W + U$$

(Por lo que hemos visto, se da seguro para $e = 0$
por elección de z y $l = s$ por $g^s = 0$. Como podrá
darse en más casos, lo dejamos en genérico).

Sea $g^e(z) = w + u$, $w \in W$ y $u \in U$. Tenemos que:

$$\overline{0} = g^s(z) = g^{s-l}(g^l(g^e(z))) = g^{s-l}(g^e(w) + g^e(u))$$

Como g es de índice s , s es el menor entero tal que
 $g^s = 0$ \wedge $s < l \Rightarrow g^{s-l} \neq 0$ pero por ser lineal,

$$g^{s-l}(g^e(w) + g^e(u)) = \overline{0} \Rightarrow g^e(w) + g^e(u) = \overline{0}$$

$$\bar{0} = g^s(z) = g^{s-l}(g^l(z)) = g^{s-l}(w+u) = \\ = g^{s-l}(w) + g^{s-l}(u) \Rightarrow g^{s-l}(w) = -g^{s-l}(u).$$

Como w y u son g -invariantes y $V^t = g^{s-l}(w) = -g^{s-l}(u)$
 $\Rightarrow V^t \in W$ y $V^t \in U \Rightarrow V^t \in W \cap U = \{\bar{0}\} \Rightarrow V^t = 0$
 $\Rightarrow g^{s-l}(w) = \bar{0} = -g^{s-l}(u)$. Aplicando el Lema 8.22,
 $\exists w_0 \in W$ tal que $w = g^l(w_0)$ y podemos escribir que

$$g^l(z-w_0) = g^l(z) - g^l(w_0) = \\ = w+u - w = u \in U$$

Como U es g -invariante $\Rightarrow g^m(z-w_0) \in U \quad \forall m \geq l$.

Si $e < l$, $g^e(z-w_0) \notin U$, por red. abs.:

$$g^e(z) = \underbrace{g^e(w_0)}_{\in W \text{ por ser } g\text{-invariante}} + \underbrace{g^e(z-w_0)}_{\notin U \text{ por hip.}} \Rightarrow g^e(z) \in U + W$$

Pero por habíamos tomado l tal. que $g^l(z) \in W+U$
y $g^e(z) \notin W+U \quad \forall e < l \Rightarrow$ Absurdo $\Rightarrow g^e(z-w_0) \notin U$.

Por tanto, $\exists z_1 = z - w_0$ tal que:

$$g^m(z_1) \in U \quad \forall m \geq l, \quad g^e(z_1) \notin U \quad \forall e < l$$

Sea ahora:

$$U_z = U + \mathbb{K}z_1 + \mathbb{K}g(z_1) + \dots + \mathbb{K}g^{l-1}(z_1)$$

$U_1 \supset U$ porque $z_1 = g^*(z_1)$, y $\in \ell$ pues ℓ es un entero positivo. $\Rightarrow g^*(z_1) \notin U$ y $z_1 \in U_1 \Rightarrow$
 $\Rightarrow \dim_K(U_1) > \dim_K(U)$. (con $z_1 \in U_1 - U$)

Además, U_1 es g -invariante. Tomemos $a \in U_1$.

$$a = u + k_1 z_1 + k_2 g(z_1) + \dots + k_{e-1} g^{e-1}(z_1)$$

$$g(a) = \underbrace{g(u)}_{\in U} + \underbrace{k_1 g(z_1)}_{\in U_1} + \dots + \underbrace{k_{e-2} g^{e-1}(z_1)}_{\in U_1} + \underbrace{k_{e-1} g^e(z_1)}_{\in U \text{ por lo visto}}$$

$\Rightarrow g(a) \in U_1 \Rightarrow U_1$ es g -invariante.

Observemos que como $\dim_K(U)$ era la máxima para la que un $U \subseteq V$ g -invariante tenía $U \cap W = \{\bar{0}\} \Rightarrow U_1 \cap W \neq \{\bar{0}\}$.

Por tanto, $\exists w \neq \bar{0}, w \in U_1 \cap W$ y es: $(u_0 \in U, z_1 \in U_1 - U)$

$$w^1 = u_0 + c_0 z_1 + c_1 g(z_1) + \dots + c_{e-1} g^{e-1}(z_1), \text{ con los}$$

coeficientes no todos nulos (sino, $w \in W$ sería $w = u_0 \in U \Rightarrow W \cap U \neq \emptyset$ que contradice la hipótesis). Sea r el primer subíndice tal que $c_r \neq 0$. Entonces:

$$w^1 = u_0 + (c_r + c_{r+1} g + \dots + c_{e-1} g^{e-1-r})(g^r(z_1)) \\ = u_0 + h(g^r(z_1)) \text{ con}$$

$$h = c_r + c_{r+1} g + \dots + c_{e-1} g^{e-1-r} \text{ y } c_r \neq 0.$$

Aplicando 8.21, h es inversible y su inversa $g = h^{-1}$ es un polinomio en g (por 8.21)). Como U (análogo W) es h -invariante:

$$u \in U \Rightarrow h^m(u) \in U \quad \forall m \geq 0. \quad 8.21$$

$$u \in U \stackrel{?}{\Rightarrow} g^m(u) \in U. \quad g^m(u) = h^{-1}(u) = (a_0^{-1}u + a_0^{-2}h^2(u) \dots)$$

$$\in_U \quad \in_U \quad \in_U$$

$$\Rightarrow g^m(u) \in U$$

$\Rightarrow U$ es g invariante, y análogo para W .

Así,

$$g(w) = \underbrace{g(u_0)}_{\in W \cap U} + \underbrace{g(h(gr(z_1)))}_{\in U} = \underbrace{g(u_0)}_{\in U} + g^r(z_1) \in g(W) \subseteq W$$

$\in W$ por ser
 W g -invariante

$$\text{Luego, } gr(z_1) = \underbrace{g(w)}_{\in W} - \underbrace{g(u_0)}_{\in U} \in W + \underbrace{g(U)}_{\subseteq U} \subseteq W + U$$

que es una contradicción, porque $r \leq l-1 < l \Rightarrow$

$$gr(z) \notin W + U \quad (r \leq l-1 < l)$$

$$\# \left\{ \begin{array}{l} gr(z) \notin W + U \quad (r \leq l-1 < l) \\ gr(z) = gr(z_1 + w_0) = \underbrace{gr(z_1)}_{\in W + U} + \underbrace{gr(w_0)}_{\in W} \Rightarrow gr(z) \in W + U \end{array} \right.$$

Esta contradicción parte de suponer que $\exists z \in V - (W + U) \Rightarrow \nexists z \in V - (W + U) \Rightarrow V = W + U$ y como $U \subseteq X$ y $\dim_{\mathbb{K}}(U) = X$

$$\Rightarrow V = W \oplus U \quad \square$$

Teorema (8.24) JORDAN

Sea $h \in \text{End}_{\mathbb{K}}(V)$ tal que todos sus distintos raíces características b_1, \dots, b_s están en el cuerpo \mathbb{K} . Entonces existe una base de V respecto de la cual la matriz coordenada de h es de la forma:

$$M_{\beta}(h) = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix},$$

siendo para cada i :

$$J_i = \begin{pmatrix} B_{i1} & & 0 \\ & B_{i2} & \\ 0 & & B_{is} \end{pmatrix},$$

y donde B_{i1}, \dots, B_{is} son los bloques básicos de Jordan pertenecientes a b_i , $\forall i \in \{1, \dots, s\}$.

dem-:

Si b_1, \dots, b_s están en \mathbb{K} , $p(x) = (x - b_1)^{m_1} \cdots (x - b_s)^{m_s}$.

Por el teorema de Cayley-Hamilton, $\text{pol. min.}(x)$ divide a $p(x)$.

$\Rightarrow \text{pol. min.}(h) = (x - b_1)^{e_1} \cdots (x - b_s)^{e_s}$, $e_i \leq m_i$, $\forall i \in \{1, \dots, s\}$

Por el primer teorema de descomposición;

$V = V_1 \oplus \cdots \oplus V_s$, con $V_i = \ker((h - b_i)^{e_i})$ $\forall i \in \{1, \dots, s\}$

Por tanto, basta encontrar bases para los subespacios V_i de

manera que los matrices asociados a $h|_{V_i} = J_i$ $\forall i \in \{1, \dots, s\}$.

Procedemos del siguiente modo:

Sea $v \in V_i$, $(h - b_i)$ -cíclico de orden e_i .

$(V_i = \ker((h - b_i)^{e_i}) \Rightarrow v \in V_i, (h - b_i)^{e_i}(v) = \bar{0})$.

Tenemos que $(h - b_i)^{e_i}(v) = \bar{0}$ y $(h - b_i)|_{V_i}$ es nilpotente ($\forall v \in V_i, (h - b_i)^{e_i}(v) = \bar{0}$). Por el lema 8.23, existe un subespacio $(h - b_i)|_{V_i}$ -invariante $U \subseteq V_i$ tal que:

$$V_i = \mathbb{K}[(h - b_i)|_{V_i}](v) \oplus U = \mathbb{K}[h - b_i](v) \oplus U.$$

Tomamos $v' \in U, v' \neq \bar{0}$. Descomponemos U en suma de

dos subespacios $(h - b_i)$ -invariantes, siendo uno de ellos $\mathbb{K}[h - b_i](v')$. De este modo, podemos descomponer V_i en suma directa de subespacios $(h - b_i)$ -invariantes tales que:

$$V_i = \mathbb{K}[h - b_i](v_{i1}) \oplus \dots \oplus \mathbb{K}[h - b_i](v_{is_i})$$

Si e_{ij} es el orden de v_{ij} respecto de $h - b_i$, se sigue que (8.20) que la matriz coordenada de $h|_{V_i}$ respecto de la base

$$\{v_{i1}, (h - b_i)(v_{i1}), \dots, (h - b_i)^{e_{i2}-1}(v_{i2}), \dots, \dots, v_{is_i}, (h - b_i)(v_{is_i}), \dots, (h - b_i)^{e_{is_i}-1}(v_{is_i})\}$$

es precisamente del tipo J_i . \square

Observación:

Podemos elegir β de manera que:

$$e_i = \text{tomo } B_{i1} \geq \text{tomo } B_{i2} \geq \dots \geq \text{tomo } B_{is},$$

$$\forall i = 1, \dots, s.$$

En este caso, la matriz obtenida:

$$\begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix}$$

Se llama la forma de Jordan de h . Se puede probar que dos endomorfismos $h_1, h_2 \in \text{End}_{\mathbb{K}}(V)$ tales que tengan todos sus raíces características en \mathbb{K} , son semejantes \Leftrightarrow tienen asociada la misma forma de Jordan. Así, la forma de Jordan de h determina la clase de semejanza.

