TEOREMES D'ÀLGEBRA LINEAL

Nil Fons
Andreu Huguet
Èric Sierra

ApuntsFME

Universitat Politècnica de Catalunya
Barcelona

Gener 2018

1 Teorema d'Steinitz

Sigui $\mathbb{E}$ un $\Bbbk$ espai vectorial finitament generat, sigui $\{u_1, \ldots, u_n\}$ un conjunt de generadors de $\mathbb{E}$ i sigui $\{w_1, ..., w_m\}$ un conjunt de vectors linealment indepentents de $\mathbb{E}$. Aleshores, $m \leq n$ i podem substituir m vectors del conjunt $\{u_1, ..., u_n\}$ pels m vectors de $\{w_1, ..., w_m\}$ de manera que el conjunt sigui conjunt de **generadors** de $\mathbb{E}$.

Demostració
Raonem per inducció sobre m, que és el cardinal de $\{w_1, ..., w_m\}$.

Volem saber si el conjunt substituït és generador de $\mathbb{E}$. Per tant, començarem la inducció amb la hipòtesi que el conjunt $\{w_1, ..., w_m, u_{m+1}, ..., u_m\}$ és generador de $\mathbb{E}$.

(1) $m = 0$. És fàcil veure que si no traiem cap vector de $\{u_1, ..., u_n\}$, aquest conjunt és generador de $\mathbb{E}$ per hipòtesi.

(2) $m \geq 1$. En aquest cas, assumirem que el cas $m-1$ del teorema és cert i volem veure si el cas m també ho és.

Suposarem que el conjunt $\{w_1, ..., w_{m-1}\}$ és linealment independent. Per tant, $m-1 \leq n = \dim(\mathbb{E})$ ja que no hi pot haver més vectors linealment independents que el cardinal de la dimensió de $\mathbb{E}$. També podem suposar que $\mathbb{E} =< w_1, ..., w_{m-1}, u_m, ..., u_n >$, ja que el cas $m-1$ era cert.

Per hipòtesi, w_m és un vector d'$\mathbb{E}$: $w_m \in \mathbb{E} =< w_1, ..., w_{m-1}, u_m, ..., u_n > \Leftrightarrow w_m = \lambda_1 w_1 + ... + \lambda_{m-1} w_{m-1} + \mu_m u_m + ... + \mu_n u_n$. És a dir, que com que el conjunt $\{w_1, ..., w_m\}$ és linealment independent per hipòtesi, hi ha almenys un μ_k que acompanya un u_k, que no és nul: $\exists \mu_k \neq 0$ i podem suposar que aquest $\mu_k = \mu_m \neq 0$.

En conclusió, ens queda que $m \leq n$ i aïllant u_m de l'equació:

$$w_m = \lambda_1 w_1 + ... + \lambda_{m-1} w_{m-1} + \mu_m u_m + ... + \mu_n u_n.$$

Passant-ho tot restant i aïllant el terme $\mu_m u_m$,

$$w_m - \lambda_1 w_1 - ... - \lambda_{m-1} w_{m-1} - \mu_{m+1} u_{m+1} - ... - \mu_n u_n = \mu_m u_m.$$

I finalment divint les dues equacions per $\mu_m \neq 0$,

$$\frac{1}{\mu_m} w_m - \frac{\lambda_1}{\mu_m} w_1 - ... - \frac{\lambda_{m-1}}{\mu_m} w_{m-1} - \frac{\mu_{m+1}}{\mu_m} u_{m+1} - ... - \frac{\mu_n}{\mu_m} u_n = u_m.$$

Així doncs, $u_m \in < w_1, ..., w_m, u_{m+1}, ..., u_n >$. És a dir, el conjunt $\{w_1, ..., w_m, u_m, ..., u_n\}$, generador de $\mathbb{E}$ per la hipòtesi d'inducció, pot ser expressat amb combinacions lineals del nou conjunt $< w_1, ..., w_m, u_{m+1}, ..., u_n >$. Consegüentment,

$$\mathbb{E} = < w_1, ..., w_m, u_{m+1}, ..., u_n > .$$

□

Corol·lari 1.1
En un $\Bbbk$-espai vectorial finitament generat $\mathbb{E}$, totes les bases són finites i tenen el mateix cardinal.

Demostració

- Sigui B_1 base de $\mathbb{E}$ de cardinal n ($|B_1| = n$).
- Sigui B_2 base de $\mathbb{E}$ de cardinal m ($|B_2| = m$).

Pel Teorema d'Steinitz $m \leq n$ i $n \leq m$, per tant, $n = m$. □

2 Fórmula de Grassmann

Si $\mathbb{F}, \mathbb{G}$ són dos subespais vectorials d'un $\Bbbk$-espai vectorial $\mathbb{E}$, aleshores:

$$\dim(F + G) + \dim(F \cap G) = \dim(F) + \dim(G).$$

Demostració
Primer de tot, si $\mathbb{F}$ i $\mathbb{G}$ no són finitament generats i les seves dimensions són infinites: $\dim\ \mathbb{F} = \dim\ \mathbb{G} = \infty \ \Rightarrow\ \dim(\mathbb{F} + \mathbb{G}) = \infty$ i per definició $\dim(\mathbb{F} \cap \mathbb{G}) \geq 0$, la fórmula queda $\infty = \infty$. Per tant, ens concentrarem en subespais finitament generats.

Si les dimensions de $\mathbb{F}$ i $\mathbb{G}$ són finites, anomenarem $n = \dim\ \mathbb{F}$ i $m = \dim\ \mathbb{G}$. Com que observem que $\mathbb{F} \cap \mathbb{G}$ és un subespai de $\mathbb{F}$ i de $\mathbb{G}$ a la vegada, anomenem $r = \dim\ \mathbb{F} \cap \mathbb{G}$ i obtenim les següents inequacions $r \leq m$, $r \leq n$.

Sigui $\{u_1, ..., u_r\}$ una base de $\mathbb{F} \cap \mathbb{G}$ (i per tant, linealment independents), la podem substituïr per r vectors de les bases de $\mathbb{F}$ i $\mathbb{G}$ en virtut del Teorema d'Steinitz, aconseguint dos nous conjunts linealment independents i generadors $\mathbb{F}$ i $\mathbb{G}$ de respectivament:

- $\{u_1, ..., u_r, w_{r+1}, ..., w_m\}$ base de $\mathbb{F}$,
- $\{u_1, ..., u_r, w'_{r+1}, ..., w'_n\}$ base de $\mathbb{G}$.

Veurem que, $B = \{u_1, ..., u_r, w_{r+1}, ..., w_m, w'_{r+1}, ..., w'_n\}$ és base de $\mathbb{F} + \mathbb{G}$ i això acabarà la demostració per què tindrem que $\dim(F+G) = n+m-r = \dim(F)+\dim(G)-\dim(F \cap G) = |\{u_1, ..., u_r, w_{r+1}, ..., w_m, w'_{r+1}, ..., w'_n\}|$.

Per veure que B és una base de $\mathbb{F} + \mathbb{G}$, s'ha de mirar si B és un conjunt de generadors de $\mathbb{F} + \mathbb{G}$ i si B és linealment independent.

(1) B és un conjunt de generadors de $\mathbb{F} + \mathbb{G}$, perquè B és la unió d'una base de $\mathbb{F}$ i una base de $\mathbb{G}$. Visualment, el conjunt repetit $\{u_1, ..., u_r\}$, no es repeteix **quan** es fa la unió: $B = \{u_1, ..., u_r, w_{r+1}, ..., w_m, w'_{r+1}, ..., w'_n\} = \{u_1, ..., u_r, w_{r+1}, ..., w_m\} \cup \{u_1, ..., u_r, w'_{r+1}, ..., w'_n\}$.

(2) B és linealment independent de $\mathbb{F}+\mathbb{G}$ si suposem que per contradicció, B és linealment dependent i es pot representar el $\mathbf{0}$ com a combinació lineal del conjunt. Usarem les següents combinacions lineals:

$$\mathbf{u} = \lambda_1 u_1 + ... + \lambda_r u_r \in \mathbb{F} \cap \mathbb{G},$$
$$\mathbf{w} = \mu_{r+1} w_{r+1} + ... + \mu_m w_m \in \mathbb{F},$$
$$\mathbf{w}' = \mu'_{r+1} w'_{r+1} + ... + \mu'_n w'_n \in \mathbb{G}.$$

Per tant tenim

$$\mathbf{0} = \overbrace{\lambda_1 u_1 + ... + \lambda_r u_r}^{\mathbf{u}} + \overbrace{\mu_{r+1} w_{r+1} + ... + \mu_m w_m}^{\mathbf{w}} + \overbrace{\mu'_{r+1} w'_{r+1} + ... + \mu'_n w'_n}^{\mathbf{w}'}.$$

Amb aquesta igualtat es té que $\mathbf{w}' = -\mathbf{u} - \mathbf{w}$. Això ens dona dues proposicions: $-\mathbf{u} - \mathbf{w}$ és una combinació lineal d'elements d'$\mathbb{F}$, per tant, $\mathbf{w}' \in \mathbb{F}$ i $\mathbf{w}' \in \mathbb{G}$. És a dir, que $\mathbf{w}'$ pertany a $\mathbb{F}$ i $\mathbb{G} \Rightarrow \mathbf{w}'$ pertany a $\mathbb{F} \cap \mathbb{G}$. Aleshores,

$$\mathbf{w}' = \alpha_1 u_1 + ... + \alpha_r u_r = \mu'_1 u_1 + ... + \mu'_r u_r.$$

Podem passar restant tots els termes μ_k restant i ens queda el $\mathbf{0}$ com a una combinació lineal de vectors de $\mathbb{F} \cap \mathbb{G}$ i de vectors de $\mathbb{G}$.

$$\mathbf{0} = \alpha_1 u_1 + ... + \alpha_r u_r - \mu'_1 u_1 - ... - \mu'_r u_r.$$

Però com que els vectors $\mathbf{u}$ i $\mathbf{w}'$ són linealment independents per definició (la seva unió és la base de $\mathbb{G}$), aleshores els escalars que els acompanyen són tots nuls.

$$\alpha_1 = ... = \alpha_r = \mu'_{r+1} = ... = \mu'_n = 0 \Rightarrow \mathbf{w}' = \mathbf{0}.$$

Ens queda, per la hipòtesi, que si B és linealment dependent, $\mathbf{w}'$ és el vector $\mathbf{0}$.

$$\mathbf{w}' = -\mathbf{u} - \mathbf{w} = \mu'_{r+1} w'_{r+1} + ... + \mu_n w'_n = \mathbf{0}.$$

Consegüentment, ens queda que $\mathbf{u} = \mathbf{w}$ i com que els vectors $\mathbf{u}$ i $\mathbf{w}$ formen la base de $\mathbb{F}$, són linealment independents. Per tant, no poden representar el vector $\mathbf{0}$ com a combinació lineal dels dos excepte si els escalars que els acompanyen són tots nuls.

$$\mathbf{0} = \mathbf{u} + \mathbf{w} = \lambda_1 u_1 + ... + \lambda_r u_r + \mu_{r+1} w_{r+1} + ... + \mu_n w_n,$$
$$\lambda_1 = ... = \lambda_r = \lambda_{r+1} = ... = \mu_n = 0.$$

En conclusió, el vector $\mathbf{0}$ només podrà ser representat com a combinació lineal dels vectors de $B = \{u_1, ..., u_r, w_{r+1}, ..., w_m, w'_{r+1}, ..., w'_n\}$ si els coeficients reals que els acompanyen són 0, wue és la definició de conjunt linealment independent.

Finalment tenim que B és un conjunt de generadors de $\mathbb{F}+\mathbb{G}$ i és linealment independent, és a dir que B és base de $\mathbb{F} + \mathbb{G}$ i la fórmula de Grassmann queda demostrada. $\square$

3 Teorema d'Isomorfisme

Siguin $\mathbb{E}$, $\mathbb{F}$ dos $\Bbbk$-espais vectorials, i sigui $f\colon \mathbb{E} \longrightarrow \mathbb{F}$ una funció lineal, aleshores:

$$\begin{aligned} g : \mathbb{E}/\operatorname{Nuc}(f) &\longrightarrow \operatorname{Im}(f) \\ u + \operatorname{Nuc}(f) &\longmapsto f(u) \end{aligned}$$

és un isomorfisme, és a dir, és una aplicació lineal bijectiva.

Demostració
Abans de començar, cal comprovar que la funció g està ben definida. En efecte, siguin u, $v \in \mathbb{E}$ tals que $u + \operatorname{Nuc}(f) = v + \operatorname{Nuc}(f)$, és a dir, que estiguin a la mateixa classe de l'espai quocient, aleshores:

$$\begin{gathered} (u - v) \in \operatorname{Nuc}(f) \implies f(u - v) = 0 \implies f(u) - f(v) = 0 \implies \\ \implies g(u + \operatorname{Nuc}(f)) - g(v + \operatorname{Nuc}(f)) = 0. \end{gathered}$$

Com que $g(u + \operatorname{Nuc}(f)) = g(v + \operatorname{Nuc}(f))$, u i v tenen la mateixa imatge sota g, per tant el representant és independent i la funció està ben definida. Cada representant particular (o cada classe) és enviat a una sola imatge.

Ara que ja hem comprovat que la funció g està ben definida, podem començar a demostrar que g és una aplicació lineal bijectiva (definició d'isomorfisme).

Primer, vegem que g és **lineal**, és a dir, que, per tot λ, $\mu \in \Bbbk$ i tot u, $v \in \mathbb{E}$,

$$\begin{gathered} g(\lambda u + \mu v + \operatorname{Nuc}(f)) = f(\lambda u + \mu v) = \lambda f(u) + \mu f(v) = \\ = \lambda g(u + \operatorname{Nuc}(f)) + \mu g(v + \operatorname{Nuc}(f)). \end{gathered}$$

Ara que ja hem vist que g és lineal, cal veure que g és bijectiva. És a dir, **injectiva** i **exhaustiva** a la vegada. Ho comprovarem per separat:

Per a demostrar la **injectivitat** de g aplicarem: g injectiva $\Leftrightarrow \operatorname{Nuc}(g) = \{0\}$

$$u \in \operatorname{Nuc}(g) \implies g(u + \operatorname{Nuc}(f)) = 0 \implies f(u) = 0 \implies u \in \operatorname{Nuc}(f).$$

Per tant $u = 0 \Leftrightarrow u + \operatorname{Nuc}(f) = \operatorname{Nuc}(f)$, que és el neutre en l'espai quocient $E/\operatorname{Nuc}(f)$. Així doncs, com que els vectors del $\operatorname{Nuc}(g)$ també ho són del $\operatorname{Nuc}(f)$, és a dir $\operatorname{Nuc}(g) = \mathbf{0}_{E/\operatorname{Nuc}(f)}$, i conseqüentment g és injectiva.

Per a demostrar la **exhaustivitat**, utilitzarem que per a tot element de la imatge de f (espai d'arribada de g), existeix una classe de vectors de l'espai quocient $E/\operatorname{Nuc}(f)$ (espai de sortida de g) tal que la seva imatge és l'element de f: $\forall\ y \in \operatorname{Im}(f)\ \exists \bar{x} \in \mathbb{E}/\operatorname{Nuc}(f)$ tal que $g(\bar{x}) = y$.

Com que $y \in \operatorname{Im}(f)$, sabem que $\exists x \in \mathbb{E}$ tal que $f(x) = y$. A més, com que la funció g està ben definida, tota la classe de x en l'espai quocient, notem-la $\bar{x} = x + \operatorname{Nuc}(f)$, tindrà la mateixa imatge sota g que qualsevol dels seus representants sota f, és a dir, $g(\bar{x}) = f(x) = y$.

Per tant, existeix $\bar{x} \in \mathbb{E}/\operatorname{Nuc}(f)$ tal que $g(\bar{x}) = y$, i g és exhaustiva.

Alternativament, podem comprovar que els elements y estan continguts a la imatge de g: $y = f(x) = g(x + \text{Nuc}(f)) \in \text{Im}(g)$, per tant tots els elements $y \in \text{Im}(f)$ estaran dins la $\text{Im}(g)$: $\text{Im}(f) \subseteq \text{Im}(g)$. I trivialment, $\text{Im}(g) \subseteq \text{Im}(f)$ ja que $\text{Im}(f)$ és el codomini de g. Per tant, $\text{Im}(g) = \text{Im}(f)$ i g és exhaustiva.

En conclusió, g és una aplicació lineal i bijectiva, i per tant, un **isomorfisme**. □

4 Teorema de Cayley-Hamilton

Si $f \in \text{End}(\mathbb{E})$ amb $\mathbb{E}$ un $\mathbb{k}$ espai vectorial de dimensió finita. Aleshores,

$$Q_f(f) = 0.$$

Això es tradueix a que el polinomi característic de f aplicat en f és 0, que és equivalent a que $Q_A(A) = 0, \forall A \in \mathcal{M}_n(\mathbb{k})$. Per notació: $Q_f(T) = Q_A(T) = \det(A - T\ \text{Id}_n) = a_nT^n + ... + a_1T + a_0$ on $A = M_B(f)$ per alguna base de $\mathbb{E}$.

Demostració
Sigui $u \in \mathbb{E}, u \neq 0$. Volem veure $Q_f(f)(u) = 0$. Aleshores, sigui $m \geq 1$ el nombre mínim tal que el conjunt $\{u, f(u), ..., f^m(u)\}$ és linealment dependent. Així doncs, $\{u, f(u), ..., f^{m-1}(u)\}$ és linealment independent i el podem ampliar per Steinitz a una base B de $\mathbb{E}$. I també es té que f^m és combinació lineal de $\{u, f(u), ..., f^{m-1}(u)\}$:

$$f^m(u) = a_0u + a_1f(u) + ... + a_{m-1}f^{m-1}(u).$$

Per tant, si apliquem la funció f al conjunt de generadors de$\mathbb{E}$ampliat per Steinitz (amb $n = \dim \mathbb{E}$): $\{u, f(u), ..., f^{m-1}(u), w_m, ..., w_n\}$, ens queda una matriu de canvi de base $M_B(f)$ de quatre blocs:

$$M_B(f) = \begin{pmatrix} A & * \\ 0 & C \end{pmatrix}.$$

- **A**: Uns a la segona diagonal ja que i tots els altres elements nuls $f^k(u) = 0 \cdot f(u) + ... + 1 \cdot f^k(u) + ... + 0 \cdot f^{m-1}(u),\ \forall k \in [1, m-1]$. La última columna, però, són els coeficients $a_0, a_1, ..., a_{m-2}, a_{m-1}$ de $f^m(u)$.
- $*$: les columnes són els coeficients de les imatges de $\{w_m, w_{m+1}, ..., w_n\}$ que acompanyen a $\{u, f(u), ..., f^{m-1}(u)\}$ i poden tenir valors qualssevol, així que ho denominem $*$ per indicar valors qualssevol.
- **C**: semblant a $*$, són els coeficients de $\{f(w_m), f(w_{m+1}), ..., f(w_n)\}$ que acompanyen a $\{w_m, w_{m+1}, ..., w_n\}$. També són valors qualssevol.
- 0: coeficients de $\{f(u), ..., f^m(u)\}$ que acompanyen a $\{w_m, w_{m+1}, ..., w_n\}$. Com que $\{w_m, w_{m+1}, ..., w_n\}$ són linealment independents amb $\{u, f(u), ..., f^{m-1}(u)\}$ ja que la seva unió és base de $\mathbb{E}$, són valors nuls.

Visualment, la matriu és representada així:

$$M_B(f) = \begin{array}{c} \\ u \\ f(u) \\ f^2(u) \\ \vdots \\ f^{m-1}(u) \\ w_m \\ \vdots \\ w_n \end{array} \begin{array}{c} \begin{array}{ccccc} f(u) & f^2(u) & \dots & f^{m-1} & f^m(u) \end{array} \\ \left(\begin{array}{ccccc|ccc} 0 & 0 & \dots & 0 & a_0 & & & \\ 1 & \ddots & & \vdots & a_1 & & & \\ 0 & \ddots & \ddots & \vdots & a_2 & & * & \\ \vdots & \ddots & \ddots & 0 & \vdots & & & \\ 0 & \dots & 0 & 1 & a_{m-1} & & & \\ \hline & & & & & & & \\ & & 0 & & & & C & \\ & & & & & & & \end{array}\right) \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ f(w_m) \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ \dots \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ f(w_n) \\ \\ \\ \\ \\ \\ \\ \\ \end{array}.$$

Per definició, el polinomi característic de f serà el determinant de la matriu de canvi de base $M_B(f)$ menys $T \cdot \mathrm{Id}_n$ i l'obtindrem fent el determinant per blocs:

$$Q_f(T) = \det(M_B(f) - T \cdot \mathrm{Id}_n) = Q_A(T) \cdot Q_C(T) - Q_*(T) \cdot Q_0(T).$$

Com que $Q_0(T) = 0$ perquè no toca la diagonal principal (i per tant no té Ts), sabem que $Q_f(T) = Q_A(T) \cdot Q_C(T) = Q_C(T) \cdot Q_A(T)$. Per tant, ens podem concentrar en determinar $Q_A(T)$ que és el polinomi el qual sabem els seus valors. L'obtindrem desenvolupant per la última columna de la submatriu A, és a dir, $\sum_{i=1}^{m-1} (-1)^{(m-1)+i} a_{im+1} M_{im+1}$:

$$\frac{Q_A(T)}{(-1)^{m-1}} = -a_0 \begin{vmatrix} 1 & -T & 0 & \cdots & 0 \\ 0 & 1 & -T & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & 1 & -T \\ 0 & \dots & \dots & 0 & 1 \end{vmatrix} + a_1 \begin{vmatrix} -T & -T & 0 & \cdots & 0 \\ 0 & 1 & -T & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & 1 & -T \\ 0 & \cdots & \cdots & 0 & 1 \end{vmatrix} -$$

$$-a_2 \begin{vmatrix} -T & 0 & 0 & \cdots & \cdots & 0 \\ 1 & -T & 0 & \ddots & & \vdots \\ 0 & 0 & 1 & -T & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 & -T \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{vmatrix} + \cdots + (-1)^{m-1}(a_{m-1} - T) \begin{vmatrix} -T & & \\ & \ddots & \\ & & -T \end{vmatrix}.$$

Calcular els determinants que acompanyen els coeficients $a_0, a_1, ..., a_{m+1}$ no és difícil, ja que al ser majoritàriament nuls, només pren rellevància la diagonal principal (fent-ho per Sarrus per exemple). Així doncs, ens queda:

$$\begin{aligned} Q_A(T) &= (-1)^{m-1} \left(a_0 \cdot 1 - a_1(-T) + ... + (-1)^{m-1}(a_{m-1} - T)(-T)^{m-1}\right) = \\ &= (-1)^m \left(-a_0 \cdot 1 + a_1 T + ... + (-1)^{k+1} a_k T^k + ... - a_{m-1} T^{m-1} + T^m\right). \end{aligned}$$

Per tant, si apliquem f a aquest polinomi característic $Q_A(f)(u)$ ens que la següent expressió:

$$Q_A(f)(u) = (-1)^m \left(f^m(u) - \left(a_0 u + a_1 f(u) + ... + a_{m-1} f^{m-1}(u) \right) \right).$$

I com hem definit abans, $f^m(u)$ és una combinació lineal tal que $f^m(u) = a_0 u + a_1 f(u) + ... + a_{m-1} f^{m-1}(u)$, i consegüentment $Q_A(f)(u) = (-1)^m (f^m(u) - f^m(u)) = 0$. Aleshores, $Q_f(f) = (Q_C(f) Q_A(f))(u) = 0$; és a dir, el polinomi característic de f aplicat en f és 0 i es demostra el Teorema de Cayley-Hamilton. □

5 Primer Teorema de Descomposició

Sigui $\mathbb{E}$ un $\Bbbk$-espai vectorial de dimensió finita, $f \in \text{End}(\mathbb{E})$. Suposem que un polinomi $P(T) \in \Bbbk[T]$ factoritza en $\Bbbk[T]$ com a producte de polinomis coprimers:

$$P(T) = P_1(T) \cdots P_n(T), \quad \text{mcd}(P_i, P_j) = 1, \quad \forall i \neq j.$$

Aleshores, $\text{Nuc}(P(f)) = \text{Nuc}(P_1(f)) \oplus \text{Nuc}(P_2(f)) \oplus \cdots \oplus \text{Nuc}(P_n(f))$. És a dir, que el nucli del polinomi podrà ser expressat de forma única com a suma directa dels nuclis dels seus polinomis coprimers.

Demostració
Per a demostrar el Teorema, utilitzarem un cas d'inducció sobre n on només caldrà demostrar el cas $n = 2$, i aplicar-lo successivament:

$$\begin{aligned} \text{Nuc}(p(f)) &= \text{Nuc}(p_1(f)) \oplus \text{Nuc}((p_2 ... p_n)(f)) \\ &= \text{Nuc}(p_1(f)) \oplus \text{Nuc}(p_2(f)) \oplus \text{Nuc}((p_3 ... p_n)(f)) \\ &= ... \end{aligned}$$

Si agafem $n = 2$ tenim

$$p(t) = p_1(T) p_2(T) \text{ amb } \text{mcd}(p_1(T), p_2(T)) = 1.$$

Com que la hipòtesi és una suma directa, volem veure dues coses: (1) la suma dels dos nuclis és igual al nucli original, i que (2) la intersecció entre els dos nuclis és el zero.

1. $\text{Nuc}(p(f)) = \text{Nuc}(p_1(f)) + \text{Nuc}(p_2(f))$,
2. $\text{Nuc}(p_1(f)) \cap \text{Nuc}(p_2(f)) = \{\mathbf{0}\}$.

Vegem (1), separant la igualtat en dues inclusions:

Volem veure que $\text{Nuc}(p_1(f)) + \text{Nuc}(p_2(f) \subseteq \text{Nuc}(p(f))$. Per tant, agafarem un vector x del $\text{Nuc}(p_1(f))$ i veurem que és del nucli de $p(f)$, aprofitant que $p_2(f)(0) = 0$,

$$x \in \text{Nuc}(p_1(f)) \implies p_1(f)(x) = 0 \implies p_2(f)(p_1(f)(x)) = 0 \implies x \in \text{Nuc}(p(f)).$$

Ja que $p_2(f)(p_1(f)(x)) = (p_2(f) \circ p_1(f))(x) = (p_1(f)) \circ (p_2(f)) = p(f)$. Anàlogament, $x \in \text{Nuc}(p_2(f)) \implies x \in \text{Nuc}(p(f))$. Per tant, com que $\text{Nuc}(p_1(f)) \subseteq \text{Nuc}(p(f))$ i també $\text{Nuc}(p_2(f)) \subseteq \text{Nuc}(p(f))$ es té que: $\text{Nuc}(p_1(f)) + \text{Nuc}(p_2(f)) \subset \text{Nuc}(p(f))$.

Ara, volem veure la inclusió contrària: $\text{Nuc}(p(f)) \subseteq \text{Nuc}(p_1(f)) + \text{Nuc}(p_2(f))$. Per la identitat de Bézout, es té que $\text{mcd}(p, q) = a \cdot p + b \cdot q$, amb a, $b \in \mathbb{Z}$.

Com que p i q són coprimers:

$$1 = a(T)p_1(T) + b(T)p_2(T) \implies Id = a(f) \circ p_1(f) + b(f) \circ p_2(f)$$

Per tant, qualsevol $x \in \text{Nuc}(p(f))$ s'expressa com a $x = (Id)(x) = (a(f) \circ p_1(f))(x) + (b(f) \circ p_2(f))(x) = x_1 + x_2$, amb $x_1 \in \text{Nuc}(p_2(f))$ i $x_2 \in \text{Nuc}(p_1(f))$.

Ja que $p_2(f)(x_1) = (p_2(f) \circ a(f) \circ p_1(f) \circ)(x) = (a(f) \circ p(f))(x) = a(f) \circ (p(f)(x)) = 0$. Perquè $x \in \text{Nuc}(p(f))$, i per tant, $x_1 \in \text{Nuc}(p_2(f))$. Anàlogament, $x_2 \in \text{Nuc}(p_1(f))$.

Amb això conclou la demostració de l'apartat (1), i ara queda per demostrar l'apartat (2), que diu que la intersecció entre els nuclis de $p_1(f)$ i $p_2(f)$ és el zero.

Sigui $x \in \text{Nuc}(p_1(f)) \cap \text{Nuc}(p_2(f))$, és a dir, $x \in \text{Nuc}(p_1)(f)$ i $x \in \text{Nuc}(p_2)(f)$. Aleshores, sigui u un vector del nucli de $(p_2(f))$ i v un vector del nucli de $(p_1(f))$. És a dir, $u = a(f)(p_1(f)(x)) = \mathbf{0}$ i $v = b(f)(p_2(f)(x)) = \mathbf{0}$. I, per tant, $x = u + v = \mathbf{0} + \mathbf{0} = \mathbf{0}$ és l'únic vector del nucli de la intersecció. Queda demostrada, doncs, la suma directa. $\square$