

## PARTIE IV POLYNOME MINIMAL. DECOMPOSITION DE DUNFORD.

(Q1) •  $(Id_E, f, \dots, f^{n^2})$  est une famille d'éléments de  $\mathcal{L}(E)$  de cardinal  $n^2+1$ .

Comme  $\dim \mathcal{L}(E) = n^2+1$ , cette famille est liée.

$$\exists (\lambda_0, \dots, \lambda_{n^2}) \in K^{n^2+1}, (\lambda_0, \dots, \lambda_{n^2}) \neq 0_{K^{n^2+1}} \text{ et } \sum_{\ell=0}^{n^2} \lambda_\ell f^\ell = 0_{\mathcal{L}(E)}$$

Alors  $\sum_{\ell=0}^{n^2} \lambda_\ell X^\ell$  est un polynôme annulateur non nul de  $f$ .

Ainsi  $\mathcal{B}$  possède un élément nul. En particulier  $\mathcal{B}$  n'est pas vide.

$$\forall \lambda \in K, \forall (p, \varphi) \in \mathcal{B}, (\lambda p + \varphi)(f) = \lambda p(f) + \varphi(f) = \lambda 0_{\mathcal{L}(E)} + 0_{\mathcal{L}(E)} = 0_{\mathcal{L}(E)}.$$

$$\underline{\forall \lambda \in K, \forall (p, \varphi) \in \mathcal{B}, \lambda p + \varphi \in \mathcal{B}.$$

$$\forall p \in K[X], \forall \varphi \in \mathcal{B}, (p\varphi)(f) = p(f) \circ \varphi(f) = p(f) \circ 0_{\mathcal{L}(E)} = 0_{\mathcal{L}(E)}.$$

$$\underline{\forall p \in K[X], \forall \varphi \in \mathcal{B}, p\varphi \in \mathcal{B}.$$

$\mathcal{B}$  est un sous-espace vectoriel de  $K[X]$  qui admet une base non nulle qui vérifie (A).

Ainsi  $\exists ! p_f \in K[X]$ ,  $p_f$  unitaire et  $\mathcal{B} = \{ \varphi p_f, \varphi \in K[X] \}$ .

(Q2) a) Soit  $\lambda$  une racine de  $p_f$ .  $\exists T \in K[X]$ ,  $p_f = (X - \lambda)T$ .

$$\text{Alors } 0_{\mathcal{L}(E)} = p_f(f) = (f - \lambda Id_E) \circ T(f).$$

$$\text{Supposons } f - \lambda Id_E \text{ injectif. Alors } T(f) = (f - \lambda Id_E)^{-1} \circ (f - \lambda Id_E) \circ T(f) = 0_{\mathcal{L}(E)} \\ = 0_{\mathcal{L}(E)}$$

Ainsi  $T \in \mathcal{B}$ . Notons que  $T$  n'est pas nul car  $p_f \neq 0_{K[X]}$ .

$$\text{Alors } \exists S \in K[X], T = SP_f \text{ avec } S \neq 0_{K[X]}.$$

$$\deg p_f = \deg((X - \lambda)T) = 1 + \deg T = 1 + \deg(SP_f) = 1 + \deg S + \deg p_f < \deg p_f !$$

$f - \lambda Id_E$  ne peut pas être injectif. Comme  $\dim E = n < +\infty$ ,  $f - \lambda Id_E$  n'est pas injectif.

Alors  $\lambda$  est une valeur propre de  $f$ . Ainsi  $\{ \lambda \in K \mid p_f(\lambda) = 0 \} \subset S_p f$ .

b) Nous venons de voir que  $\{\lambda \in K \mid P_f(\lambda) = 0\} \subset Sp_f$ .

Or  $P_f$  est un polynôme annulateur de  $f$  donc  $Sp_f \subset \{\lambda \in K \mid P_f(\lambda) = 0\}$ .

Ainsi le spectre de  $f$  est l'ensemble des zéros de  $P_f$ .

Q3 a) Si  $P_f$  est scindé alors  $f$  admet un polynôme annulateur scindé :  $P_f$  !

Réciproquement supposons que  $f$  admet un polynôme annulateur scindé  $P$ .

Alors  $P$  est un multiple de  $P_f$ .  $\exists Q \in K[X], P = Q P_f$ .

$\exists c \in K^*, \exists r \in \mathbb{N}^*, \exists (\alpha_1, \dots, \alpha_r) \in K^r, \exists (n_1, \dots, n_r) \in \mathbb{N}^{*r}, P = c \prod_{i=1}^r (X - \alpha_i)^{n_i}$  avec  $\alpha_1, \dots, \alpha_r$  deux à deux distincts.

Soit  $k \in \{1, \dots, r\}$ .  $\alpha_k$  est une racine de  $Q P_f$  donc de  $Q$  ou de  $P_f$ .

Notons  $s_k$  l'ordre de multiplicité de  $\alpha_k$  dans  $P_f$  à savoir que

$s_k = 0$  si  $\alpha_k$  n'est pas racine de  $P_f$ . Or  $\alpha_k$  est racine d'ordre  $n_k - s_k$  de  $Q$  (toujours avec la même convention).

Ainsi  $\prod_{i=1}^r (X - \alpha_i)^{n_i}$  divise  $P_f$  et  $\prod_{i=1}^r (X - \alpha_i)^{n_i - s_i}$  divise  $Q$

$\exists (U, V) \in K[X]^2, P_f = U \prod_{i=1}^r (X - \alpha_i)^{n_i} \text{ et } Q = V \prod_{i=1}^r (X - \alpha_i)^{n_i - s_i}$ .

Alors  $c \prod_{i=1}^r (X - \alpha_i)^{n_i} = P = Q P_f = U \prod_{i=1}^r (X - \alpha_i)^{n_i - s_i} \times V \prod_{i=1}^r (X - \alpha_i)^{n_i} = UV \prod_{i=1}^r (X - \alpha_i)^{n_i}$

Ainsi  $c = UV$ . Or  $U$  et  $V$  sont des polynômes constants et non nuls.

$\exists c' \in K^*, U = c'$ . Alors  $P_f = c' \prod_{i=1}^r (X - \alpha_i)^{n_i}$ .  $P_f$  est scindé.

Finalement  $P_f$  est scindé si et seulement si  $f$  admet un polynôme annulateur scindé.

b) Supposons que  $P_f$  est scindé à racines simples. Alors  $f$  possède un polynôme annulateur scindé à racines simples.

Réciproquement supposons que  $f$  possède un polynôme annulateur scindé à racines simples. Alors  $P_f$  est scindé d'après a) et  $P_f$  divise  $P$ .

Si  $P_f$  admet une racine d'ordre  $m$  mais  $2 \nmid m$  et de même de  $P$  car  $P$  divise  $P$ . Cela n'est pas possible.

Alors  $P_f$  est scindé à racines simples.

Finalement  $P_f$  est scindé à racines simples si et seulement si  $f$  admet un polynôme annulateur scindé à racines simples.

c) Nous avons vu dans III Q1 que si  $f$  est diagonalisable alors  $f$  possède un polynôme annulateur scindé à racines simples.

Ainsi si  $f$  est diagonalisable,  $P_f$  est scindé à racines simples.

Q4 a) En appliquant II Q2 il vient:

$$\ker P_f(f) = G_1 \oplus G_2 \oplus \dots \oplus G_r. \text{ Puis } P_f(f) = 0_{\mathcal{L}(E)} \text{ donc } \ker P_f(f) = E.$$

$$\text{Alors } E = G_1 \oplus G_2 \oplus \dots \oplus G_r = \bigoplus_{k=1}^r G_k = \bigoplus_{k=1}^r \ker (f - \lambda_k \text{Id}_E)^{p_k}.$$

b) Soit  $\lambda \in \mathbb{C}$ .  $\lambda$  est une racine de  $P_f$  d'ordre une valeur propre de  $f$  (IV Q2).

Ainsi  $\ker (f - \lambda \text{Id}_E) \neq \{0_E\}$ . Comme  $\ker (f - \lambda \text{Id}_E) \subset \ker (f - \lambda \text{Id}_E)^{p_k}$ ,

$G_k = \ker (f - \lambda \text{Id}_E)^{p_k}$  n'est pas vide et on obtient nul.

c) Supposons que les racines de  $P_f$  sont simples. Alors  $\forall \lambda \in \mathbb{C}, p_\lambda = 1$ .

Rappelons que  $S_P(f) = \{\lambda_1, \lambda_2, \dots, \lambda_r\}$ .

$$\text{Alors } E = \bigoplus_{k=1}^r G_k = \bigoplus_{k=1}^r K(\mathbb{F}_k \text{ Id}_E)^{P_k} = \bigoplus_{k=1}^r K(\mathbb{F}_k \text{ Id}_E) = \bigoplus_{k=1}^r \text{SEP}(\mathbb{F}_k, 1) = \bigoplus_{\lambda \in S_P(f)} \text{SEP}(\mathbb{F}, \lambda)$$

Ainsi  $f$  est diagonalisable.

Remarque. ... Ceci achève de prouver l'équivalence des trois conditions suivantes

i)  $f$  est diagonalisable    ii)  $f$  est séparable à racines multiples    iii)  $f$  possède un polynôme annulateur séparable à racines multiples.

d) Pour démontrer ce résultat il suffit de prouver que  $\varphi_1, \varphi_2, \dots, \varphi_r$  sont premiers entre eux ( $\text{I} \& \text{II}'$ ).

Soit  $P$  un diviseur commun à  $\varphi_1, \varphi_2, \dots, \varphi_r$ . Supposons  $\deg P \neq 0$ .  $P$  ne peut pas être nul. Soit  $\alpha$  une racine de  $P$  dans  $\mathbb{C}$ .  $\alpha$  est une racine de  $\varphi_1$ . donc  $\deg P \geq 1$ .

Alors  $\exists k \in \llbracket 2, r \rrbracket$ ,  $\alpha = \lambda_k$ .

Comme  $P$  divise  $\varphi_k$ ,  $\alpha$  est également une racine de  $\varphi_k$ . Ainsi  $\lambda_k$  est une racine de  $\varphi_1$   $\alpha$  qui n'est pas.

Il n'existe pas de polynôme de degré non nul qui divise  $\varphi_1, \varphi_2, \dots, \varphi_r$ .

$\varphi_1, \varphi_2, \dots, \varphi_r$  sont premiers entre eux.

$$\text{Alors } \exists (u_1, u_2, \dots, u_r) \in (K[x])^r, \quad \sum_{i=1}^r \varphi_i u_i = 1.$$

e)  $r \in \llbracket 2, n \rrbracket$ .  $k \in \llbracket 1, r \rrbracket$ . Notons  $q_k$  la projection sur  $G_k$  parallèlement à  $\bigoplus_{i \neq k} G_i$ .

et montrons que  $(\varphi_k u_k)(f) = q_k$ .

$$\sum_{i=1}^r \varphi_i u_i = 1 \quad \text{Ainsi} \quad \sum_{i=1}^r (\varphi_i u_i)(f) = \text{Id}_E.$$

$$\text{Soit } x \in E. \quad \sum_{i=1}^r (\varphi_i u_i)(f)(x) = x.$$

$$\text{Posons } \forall i \in \llbracket 1, r \rrbracket, x_i = (\varphi_i u_i)(f)(x). \quad \text{Alors } x = \sum_{i=1}^r x_i.$$

montrons que :  $\forall i \in \llbracket 1, r \rrbracket, x_i \in G_i$

$$\text{Soit } i \in \overline{1, r}, (\mathcal{J} - \lambda_i \text{Id}_E)^{p_i}(x_i) = (\mathcal{J} - \lambda_i \text{Id}_E)^{p_i}((\Phi_i U_i)(\mathcal{J})(x_i)).$$

$$(\mathcal{J} - \lambda_i \text{Id}_E)^{p_i}(x_i) = ((\mathcal{J} - \lambda_i)^{p_i} \Phi_i U_i)(\mathcal{J})(x_i) = (U_i (\mathcal{J} - \lambda_i)^{p_i} \Phi_i)(\mathcal{J})(x_i) = (U_i P_{\mathcal{J}})(\mathcal{J})(x_i).$$

$$(\mathcal{J} - \lambda_i \text{Id}_E)^{p_i}(x_i) = U_i(\mathcal{J})(\underbrace{P_{\mathcal{J}}(\mathcal{J})(x_i)}_{= 0_{\mathcal{L}(E)}}) = U_i(\mathcal{J})(0_E) = 0_E.$$

Donc  $\forall i \in \overline{1, r}, x_i \in G_i$ .

Alors  $q_E(x) = x_E$  car  $x = x_1 + \dots + x_r = x_E + (x_1 + \dots + x_{E-1} + x_{E+1} + \dots + x_r)$  avec

$$x_E \in G_E \text{ et } x_1 + \dots + x_{E-1} + x_{E+1} + \dots + x_r \in \bigoplus_{\substack{i=1 \\ i \neq E}}^r G_i.$$

Donc  $q_E(x) = x_E = (\Phi_E U_E)(\mathcal{J})(x)$  et ceci pour tout  $x$  dans  $E$ .

$(\Phi_E U_E)(\mathcal{J})$  est bien la projection  $q_E$  sur  $G_E$  parallèlement à  $\bigoplus_{\substack{i=1 \\ i \neq E}}^r G_i$ .

$$\mathcal{J} \circ q_E = \mathcal{J} \circ (\Phi_E U_E)(\mathcal{J}) = (\mathcal{J} \Phi_E U_E)(\mathcal{J}) = (\Phi_E U_E \mathcal{J})(\mathcal{J}) = (\Phi_E U_E)(\mathcal{J}) \circ \mathcal{J} = q_E \circ \mathcal{J}.$$

$q_E$  commute avec  $\mathcal{J}$  (... ce qui est normal pour un polynôme de  $\mathcal{J}$ ).

(Q5) a)  $\lambda \in \overline{1, r}$  et  $x \in G_E$ .  $q_E(x) = x$ .

Si  $\lambda \neq E$ :  $\forall i \in \overline{1, r} - \{E\}$ ,  $x \in \bigoplus_{\substack{E=1 \\ E \neq i}}^r G_E$  et  $q_i(x) = 0_E$ .

$$\text{Ainsi, dans tous les cas, } d(x) = \sum_{i=1}^r \lambda_i q_i(x) = \lambda_E q_E(x) = \lambda_E x$$

$$\underline{\underline{\forall \lambda \in \overline{1, r}, \forall x \in G_E, d(x) = \lambda_E x.}}$$

Rappelons que  $\forall \lambda \in \overline{1, r}, G_\lambda \neq \{0_E\}$ .

Pour tout  $\lambda$  dans  $\overline{1, r}$  notons  $B_\lambda$  une base de  $G_\lambda$ .

Notons que pour tout  $\lambda$  dans  $\overline{1, r}$  les éléments de  $B_\lambda$  sont des vecteurs propres de  $d$  associés à la valeur propre  $\lambda_E$ .

$E = \bigoplus_{\lambda=1}^r G_\lambda$  donc  $B = \bigcup_{\lambda=1}^r B_\lambda$  est une base de  $E$  constituée de vecteurs propres de  $d$ .

Par conséquent d est diagonalisable.

b) Pour tout  $i \in \llbracket 1, r \rrbracket$ ,  $q_i$  est un polynôme de  $f$  d'après Q 4 c)

Ainsi  $d = \sum_{i=1}^r \lambda_i q_i$  est un polynôme de  $f$ . Mais il en est de même pour  $v = f - d$ .

d et v sont des polynômes de  $f$ .

Soit  $(H_1, H_2) \in K[X]^2$ ,  $d = H_1(f)$  et  $v = H_2(f)$ .

$$d \circ v = H_1(f) \circ H_2(f) = (H_1, H_2)(f) = (H_2, H_1)(f) = H_2(f) \circ H_1(f) = v \circ d.$$

d et v commutent.

c) Soit  $k \in \llbracket 1, r \rrbracket$ .  $v = H_k(f)$ .

$$\text{Soit } x \in G_k. \quad (f - \lambda_k \text{Id}_E)^{p_k}(v(x)) = (f - \lambda_k \text{Id}_E)^{p_k}(H_k(f)(x)).$$

$$(f - \lambda_k \text{Id}_E)^{p_k}(v(x)) = ((x - \lambda_k)^{p_k} H_k)(f)(x) = (H_k(x - \lambda_k)^{p_k})(f)(x) = H_k(f)((f - \lambda_k \text{Id}_E)^{p_k}(x)).$$

$$\text{Or } x \in G_k \text{ donc } (f - \lambda_k \text{Id}_E)^{p_k}(x) = 0_E \text{ donc } (f - \lambda_k \text{Id}_E)^{p_k}(v(x)) = H_k(f)(0_E) = 0_E.$$

Alors  $v(x) \in G_k$ .

$G_k$  est stable par  $v$ .

$$\text{Soit } x \in G_k. \quad v_k(x) = v(x) = f(x) - d(x) = f(x) - \lambda_k x = (f - \lambda_k \text{Id}_E)(x)$$

$$\text{Alors } v_k^{p_k}(x) = (f - \lambda_k \text{Id}_E)^{p_k}(x) = 0_E \text{ car } x \in G_k.$$

$$\text{Ainsi } \underline{\underline{v_k^{p_k} = 0_{\mathcal{L}(G_k)}}}.$$

$$\text{Posons } \Delta = p_1 p_2 \dots p_r. \quad v_k^\Delta = (v_k^{p_k})^{p_1 \dots p_{k-1} p_{k+1} \dots p_r} = 0_{\mathcal{L}(G_k)}^{p_1 \dots p_{k-1} p_{k+1} \dots p_r} = 0_{\mathcal{L}(G_k)} \text{ (à un petit abus près, } p_i r = 1).$$

$$\underline{\underline{\forall k \in \llbracket 1, r \rrbracket, v_k^\Delta = 0_{\mathcal{L}(G_k)}}}. \text{ Particulièrement alors que } v^\Delta = 0_{\mathcal{L}(E)}.$$

$$\text{Soit } x \in E. \exists (x_1, \dots, x_r) \in G_1 \times \dots \times G_r, x = x_1 + \dots + x_r = \sum_{k=1}^r x_k$$

$$v^\Delta(x) = \sum_{k=1}^r v^\Delta(x_k) = \sum_{k=1}^r v_k^\Delta(x_k) = \sum_{k=1}^r 0_E = 0_E. \text{ Ainsi } v^\Delta = 0_{\mathcal{L}(E)}.$$

Alors  $v$  est nilpotent.

$$\text{Finalement } f = d + v \text{ avec } \begin{cases} (d, v) \in \mathcal{L}(E)^2 \\ d \text{ diagonalisable} \\ v \text{ nilpotent} \\ d \circ v = v \circ d \end{cases}$$

(Q6) unicité de la décomposition.

a)  $f = d' + v'$  et  $d' \circ v' = v' \circ d'$ .

Alors  $f \circ d' = d' \circ d' + v' \circ d' = d' \circ d' + d' \circ v' = d' \circ f$ .

$d'$  commute avec  $f$  et il a été démontré pour  $v'$ .

Si  $d'$  commute avec  $f$ , alors  $d'$  commute avec tout polynôme de  $f$ .

Ainsi  $d' \circ (f - \lambda \text{Id}_E)^{p_\lambda} = (f - \lambda \text{Id}_E)^{p_\lambda} \circ d'$  pour tout  $\lambda \in \mathbb{C}_{1,r} \cup \mathbb{D}$ .

Alors  $\forall \lambda \in \mathbb{C}_{1,r} \cup \mathbb{D}, \forall x \in E_\lambda, (f - \lambda \text{Id}_E)^{p_\lambda}(d'(x)) = d'((f - \lambda \text{Id}_E)^{p_\lambda}(x)) = d'(0_E) = 0_E$ .

Ainsi  $\forall \lambda \in \mathbb{C}_{1,r} \cup \mathbb{D}, \forall x \in E_\lambda, d'(x) \in E_\lambda$ .

pour tout élément  $\lambda$  de  $\mathbb{C}_{1,r} \cup \mathbb{D}$ ,  $E_\lambda$  est stable par  $d'$ .

Cela n'est pas franchement utile !

b)  $d'$  commute avec  $f$  donc avec tout polynôme de  $f$  donc avec  $d$  !

Ainsi  $d$  et  $d'$  sont diagonalisables et  $d \circ d' = d' \circ d$ .

D'après D 94 il existe une base de  $E$  constituée de vecteurs propres pour  $d$  et  $d'$ . Soit  $(u_1, u_2, \dots, u_n)$  cette base.

$\exists (\sigma_i, \sigma'_i) \in \mathbb{K}^2, d(u_i) = \sigma_i u_i$  et  $d'(u_i) = \sigma'_i u_i$  pour tout  $i \in \{1, n\}$ .

Alors  $\forall i \in \{1, n\}, (d - d')(u_i) = (\sigma_i - \sigma'_i) u_i$ .

$(u_1, \dots, u_n)$  est une base de  $E$  constituée de vecteurs propres de  $d - d'$ .

$d - d'$  est diagonalisable.

Cela a  
été  
démontré  
de  
l'unicité.

c)  $v'$  commute avec  $f$  donc avec tout polynôme de  $f$  donc avec  $v$ .

$v$  et  $v'$  sont nilpotents donc  $\exists (n, n') \in \mathbb{N}^{*2}$ ,  $v^n = v'^{n'} = 0_{X(E)}$ .

$$(v'v)^{n+n'} = \sum_{\ell=0}^{n+n'} \binom{n+n'}{\ell} v'^{\ell} \circ (-v)^{n+n'-\ell} = \sum_{\ell=0}^{n'-1} \binom{n+n'}{\ell} v'^{\ell} \circ (-v)^{n+n'-\ell} = 0_{X(E)}$$

$\nearrow$   $v'^{\ell} = 0_{X(E)}, \forall \ell \geq n'$ 
 $\nearrow$   $\ell \leq n'-1 \Rightarrow n+n'-\ell \geq n+1$

Ainsi  $v'v$  est nilpotent.

$$\downarrow$$

$$(-v)^{n+n'-\ell} = 0_{X(E)}$$

d) D'après ce qui précède  $x^{n+n'}$  est un polynôme annulateur de  $v'v$ .

Alors  $\text{Sp}(v'v) \subset \{0\}$ .

A  $f = d + v = d' + v'$  donc  $d - d' = v'v$ . Ainsi  $\text{Sp}(d - d') \subset \{0\}$ .

A  $d - d'$  est diagonalisable.

Ainsi  $\text{Sp}(d - d') = \{0\}$  et  $\text{SEP}(d - d', 0) = E$ .  $\text{KE}(d - d') = E$ .

Ainsi  $d - d' = 0_{X(E)}$ , donc nécessairement  $v'v = 0_{X(E)}$ .

Donc  $d' = d$  et  $v' = v$ .