Polynôme minimal en un vecteur

Notation :

- *E désigne un $\mathbb{K}-$espace vectoriel de dimension finie $n \geqslant 2$, ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) et $f \in \mathcal{L}_{\mathbb{K}}(E)$*
- *π_f le polynôme minimal de f*
- $\mathbb{K}[f] = \{P(f) \ /P \in \mathbb{K}[X]\}$
- *Pour $x \in E$, on pose $I_x = \{P \in \mathbb{K}[X] \ / \ P(f)(x) = 0\}$ et $E_x = E_f(x) = \{ \ P(f)(x) \ / \in \mathbb{K}[X]\}$*

1. Soit $x \in E$. Montrer qu'il existe un unique polynôme unitaire $\pi_x \in \mathbb{K}[X]$ tel que :
$$I_x = (\pi_x) = \pi_x \mathbb{K}[X]$$
2. On pose $k = \deg(\pi_f)$ et $r = \deg(\pi_x)$
   (a) Vérifier que $r \leqslant k$
   (b) Montrer que E_x est un sous-espace vectoriel de E de dimension r et en donner une base
   (c) Montrer que $\mathbb{K}[f]$ est une sous-algèbre de $\mathcal{L}(E)$ et en donner une base
3. Soient x_1 et x_2 de deux éléments de E
   (a) On suppose que $E_{x_1} \cap E_{x_2} = \{0\}$, montrer que $\pi_{x_1+x_2} = ppcm(\pi_{x_1}, \pi_{x_2})$
   (b) On suppose que π_{x_1} et π_{x_2} sont premiers entre eux . Montrer que $E_{x_1+x_2} = E_{x_1} \oplus E_{x_2}$
4. Soient $x_1, x_2, ..., x_p$ des vecteurs de E
   (a) On suppose que $E_{x_1}, E_{x_2} \ , ..., E_{x_p}$ sont en somme directe . Montrer que :
$$\pi_{x_1+x_2+...+x_p} = ppcm\left(\pi_{x_1}, \pi_{x_2}, .., \pi_{x_p}\right)$$
   (b) On suppose que $\pi_{x_1}, \pi_{x_2} \ , ..., \pi_{x_p}$ sont deux à deux premiers entre eux . Montrer que :
$$E_{x_1+x_2+...+x_p} = E_{x_1} \oplus E_{x_2} \oplus ... \oplus E_{x_p}$$
5. Soit P un facteur irréductible de π_f de multiplicité α
   (a) Soit $x \in \operatorname{Ker}(P^\alpha(f))$. Montrer qu'il existe un entier $\alpha_x \leqslant \alpha$ tel que : $\pi_x = P^{\alpha_x}$
   (b) En déduire qu'il existe $x \in \operatorname{Ker}(P^\alpha(f))$ tel que $\pi_x = P^\alpha$

On pourra raisonner par l'absurde en supposant que $\forall x \in Ker(P^\alpha(f)) \ , \alpha_x < \alpha$

6. En déduire qu'il existe $x \in E$ tel que : $\pi_x = \pi_f$
7. On dit qu'un endomorphisme f est cyclique s'il existe $x \in E$ tel que : $E_x = E$.
   Etablir que les assertions suivantes sont équivalents :
   (i) f est cyclique
   (ii) $\deg(\pi_f) = n$
   (iii) $\pi_f = \chi_f$
8. On suppose que f est cyclique.
   (a) Montrer qu'il existe une base $\mathcal{B}$ de E telle que :
$$\operatorname*{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \ddots & \vdots & a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}$$
   (b) Montrer que $\chi_f = X^n - \sum_{i=0}^{n-1} a_i X^i$

POLYNÔME MINIMAL EN UN VECTEUR

1. On va montrer que $I_x = \{P \in \mathbb{K}[X] \ / \ P(f)(x) = 0\}$ est un idéal de $\mathbb{K}[X]$.

   - On a $I_x \neq \emptyset$ (Car contient le polynôme nul)
   - Pour tout $(P, Q) \in I_x^2$, alors $(P - Q)(f)(x) = P(f)(x) - Q(f)(x) = 0$ donc $P - Q \in I_x$.
   - Pour tout $P \in \mathbb{K}[X]$ et $Q \in I_x$, on a
     $(PQ)(f)(x) = P(f) \circ Q(f)(x) = P(f)(Q(f)(x)) = P(f)(0) = 0$ donc $PQ \in I_x$

   I_x est un idéal non nul de $\mathbb{K}[X]$ car il contient π_f, donc il existe un unique polynôme unitaire $\pi_x \in \mathbb{K}[X]$ tel que :
   $$I_x = (\pi_x) = \pi_x \mathbb{K}[X]$$

2. (a) On a $\pi_f(f) = 0$ donc $\pi_f(f)(x) = 0$ et, par suite, $\pi_f \in I_x = (\pi_x)$. Par définition de l'idéal π_x divise π_f, donc $r = \deg(\pi_x) \leqslant \deg(\pi_f) = k$

   (b) - Pour $P = 0$, on a $P(f)(x) = 0$ donc $0 \in E_x$
       - Si $y_1 = P_1(f)(x)$ et $y_2 = P_2(f)(x)$ sont deux éléments de E_x et $\lambda \in \mathbb{K}$ alors $\lambda y_1 + y_2 = (\lambda P_1 + P_2)(f)(x) \in E_x$.

   Donc E_x est un sous-espace vectoriel de E

   c) Soit $y \in E_x$ alors il existe $P \in \mathbb{K}[X]$ tel que $y = P(f)(x)$

   A l'aide de la division euclidienne il existe $(Q, R) \in (\mathbb{K}[X])^2$ tel que
   $$P = Q\pi_x + R \text{ avec } \deg(R) < \deg(\pi_x) = r$$
   Par suite $y = P(f)(x) = Q(f) \circ \pi_x(f)(x) + R(f)(x) = R(f)(x)$ (car $\pi_x(f)(x) = 0$)

   Posons $R = \sum_{k=0}^{r-1} a_k X^k$, on a alors $y = R(f)(x) = \sum_{k=0}^{r-1} a_k f^k(x) \in Vect\{x, f(x), ..., f^{r-1}(x)\}$

   Ainsi $\{x, f(x), ..., f^{r-1}(x)\}$ est génératrice de E_x . On va montrer qu'elle est libre

   Soit $(\lambda_0, \lambda_1, ..., \lambda_{r-1}) \in \mathbb{K}^r$ tel que $\sum_{k=0}^{r-1} \lambda_k f^k(x) = 0$

   Posons $P = \sum_{k=0}^{r-1} \lambda_k X^k$. On a $P(f)(x) = \sum_{k=0}^{r-1} \lambda_k f^k(x) = 0$ donc $P \in I_x$ par suite π_x divise P

   Or $\deg(P) < \deg(\pi_x)$ donc $P = 0$. On en déduit que $\lambda_0 = \lambda_1 = ... = \lambda_{r-1} = 0$.

   Ainsi $\mathcal{B} = \{x, f(x), ..., f^{r-1}(x)\}$ est une base de E_x . Par suite $\dim E_x = r$.

   (c) $id_E \in \mathbb{K}[f]$ de plus si $h, g \in \mathbb{K}[f]$ et $\lambda \in \mathbb{K}$, $h = P(f)$ et $g = Q(f)$ alors
   $$\lambda h + g = (\lambda P + Q)(f) \in \mathbb{K}[f] \text{ et } h \circ g = (PQ)(f) \in \mathbb{K}[f]$$
   donc $\mathbb{K}[f]$ est une sous-algèbre de $\mathcal{L}(E)$.

   A l'aide d'un raisonnement analogue à la question précédente , on a $\{Id, f, ..., f^{k-1}\}$ est une base de $\mathbb{K}[f]$ donc $\dim \mathbb{K}[f] = k = \deg(\pi_f)$

3. Soient x_1 et x_2 de deux éléments de E

   (a) Posons $P = ppcm(\pi_{x_1}, \pi_{x_2})$, on a π_{x_1} et π_{x_2} divisent P donc $P(f)(x_i) = 0$, $i = 1, 2$

   On a alors $P(f)(x_1 + x_2) = P(f)(x_1) + P(f)(x_2) = 0$ donc $\pi_{x_1+x_2}$ divise P

   D'autre part $\pi_{x_1+x_2}(f)(x_1 + x_2) = 0$ donc
   $$\underbrace{\pi_{x_1+x_2}(f)(x_1)}_{\in E_{x_1}} = \underbrace{-\pi_{x_1+x_2}(f)(x_2)}_{\in E_{x_2}} \in E_{x_1} \cap E_{x_2} = \{0\}$$

Polynôme minimal en un vecteur

Donc $\pi_{x_1+x_2}(f)(x_1)=\pi_{x_1+x_2}(f)(x_2)=0$ par suite π_{x_1} et π_{x_2} divisent $\pi_{x_1+x_2}$

On en déduit que $P=ppcm(\pi_{x_1},\pi_{x_2})$ divise $\pi_{x_1+x_2}$

(b) Supposons que π_{x_1} et π_{x_2} sont premiers entre eux .

D'après le théorème de Bezout , il existe $(P,Q)\in(\mathbb{K}[X])^2$ tel que $(*) : P\pi_{x_1}+Q\pi_{x_2}=1$

Donc $id_E=P(f)\circ\pi_{x_1}(f)+Q(f)\circ\pi_{x_2}(f)$.

Vérifions d'abord que $E_{x_i}\subset E_{x_1+x_2}$. Soit $y\in E_{x_i}$, il existe $U_i\in\mathbb{K}[X]$ tel que

$$y=U_i(f)(x_1)=(U_i+\pi_{x_i})(f)(x_1+x_2)\in E_{x_1+x_2}$$

D'après $(*)$ on a $U=UP\pi_{x_1}+UQ\pi_{x_2}=P_1\pi_{x_1}+P_2\pi_{x_2}$ avec $P_1=UP$ et $P_2=UQ$ donc :

$$y=P_1(f)\circ\pi_{x_1}(f)(y)+P_2(f)\circ\pi_{x_2}(f)(y)$$

Si $y\in E_{x_1}\cap E_{x_2}$ alors il existe $S_1,S_2\in\mathbb{K}[X]$ tel que $y=S_1(f)(x_1)=S_2(f)(x_2)$.
On a alors

$$P_i(f)\circ\pi_{x_i}(f)(y)=P_i(f)\circ\pi_{x_i}(f)\circ S_i(f)(x_i)=P_i(f)\circ S_i(f)\circ\pi_{x_i}(f)(x_i)=0$$

Par suite

$$y=P_1(f)\circ\pi_{x_1}(f)(x_1)+P_2(f)\circ\pi_{x_2}(f)(x_2)=0.$$

Donc $E_{x_1}\cap E_{x_2}=\{0\}$.

Soit $y\in E_{x_1+x_2}$, il existe $P\in\mathbb{K}[X]$ tel que $y=P(f)(x_1+x_2)=P(f)(x_1)+P(f)(x_2)\in E_{x_1}+E_{x_2}$
On en déduit que $E_{x_1+x_2}=E_{x_1}\oplus E_{x_2}$

4. *Généralisation :* Soient $x_1,x_2,...,x_p$ des vecteurs de E

(a) Rappelons que si $F_1+F_2+...F_p$ est une somme directe et si $u_i\in F_i$, $i=1,...,p$ sont tels que $u_1+u_2+...u_p=0$ alors $u_1=u_2=...=u_p=0$

Supposons que E_{x_1},E_{x_2} ,...., E_{x_p} sont en somme directe .

Posons $P=ppcm\left(\pi_{x_1},\pi_{x_2},..,\pi_{x_p}\right)$ on a pour tout $i\in\{1,2,...,p\}$, $P(f)(x_i)=0$

Donc $P(f)(x_1+x_2+...+x_p)=P(f)(x_1)+...+P(f)(x_p)=0$ par suite $\pi_{x_1+x_2+...+x_p}$ divise P .

D'autre part , on a $\pi_{x_1+x_2+...+x_p}(x_1+x_2+...+x_p)=0$ donc $\displaystyle\sum_{i=1}^{p}\underbrace{\pi_{x_1+x_2+...+x_p}(f)(x_i)}_{\in E_{x_i}}=0$

La somme $E_{x_1}+E_{x_2}+....+E_{x_p}$ étant directe , donc

$$\pi_{x_1+x_2+...+x_p}(f)(x_1)=...=\pi_{x_1+x_2+...+x_p}(f)(x_p)=0$$

On en déduit que , pour tout $i\in\{1,2,...,p\}$, π_{x_i} divise $\pi_{x_1+x_2+...+x_p}$

Par conséquent $P=ppcm\left(\pi_{x_1},\pi_{x_2},..,\pi_{x_p}\right)$ divise $\pi_{x_1+x_2+...+x_p}$.

(b) Par récurrence sur p . Pour $p=2$ c'est déjà établi
Supposons la propriété vraie pour $p-1$.

On a $E_{x_1}+E_{x_2}+...+E_{x_{p-1}}=E_{x_1+x_2+...+x_{p-1}}$ de plus $\pi_{x_1+x_2+...+x_{p-1}}=ppcm\left(\pi_{x_1},\pi_{x_2},..,\pi_{x_{p-1}}\right)$

Comme π_{x_p} est premier avec π_{x_i} pour $1\leqslant i\leqslant p-1$ donc π_{x_p} est premier avec $\pi_{x_1+x_2+...+x_{p-1}}$
Par suite la somme $\left(E_{x_1}+E_{x_2}+...+E_{x_{p-1}}+E_{x_p}\right)$ est directe .

Et comme $E_{x_1}+E_{x_2}+...+E_{x_{p-1}}$ est une somme directe (hypothèse de récurrence)
Donc

$$E_{x_1+x_2+...+x_p}=E_{x_1}\oplus E_{x_2}\oplus ...\oplus E_{x_p}$$

5. Soit P un facteur irréductible de π_f de multiplicité α

   (a) Soit $x\in Ker\left(P^{\alpha}\left(f\right)\right)$. On a $P^{\alpha}\left(f\right)\left(x\right)=0$ donc π_x divise P^{α}

   Comme P est irréductible , alors les diviseurs de P^{α} sont de la forme P^k avec $k\leqslant\alpha$.

   En particulier il existe un entier $\alpha_x\leqslant\alpha$ tel que : $\pi_x=P^{\alpha_x}$

   (b) Supposons que $\forall x\in \operatorname{Ker}\left(P^{\alpha}\left(f\right)\right)$, $\alpha_x<\alpha$. Soit $\beta=\max\left\{\alpha_x\ /x\in Ker\left(P^{\alpha}\left(f\right)\right)\right\}$

   On a $\beta<\alpha$, pour tout $x\in Ker\left(P^{\alpha}\left(f\right)\right)$, on a $P^{\beta}\left(f\right)\left(x\right)=P^{\beta-\alpha_x}\left(f\right)\circ P^{\alpha_x}\left(f\right)\left(x\right)=0$

   Donc $P^{\beta}\left(f\right)\left(x\right)=0$ pour tout $x\in Ker\left(P^{\alpha}\left(f\right)\right)$. On en déduit que $Ker\left(P^{\alpha}\left(f\right)\right)=Ker\left(P^{\beta}\left(f\right)\right)$

   Posons $\pi_f=P^{\alpha}Q$ avec P et Q premiers entre eux . Soit $R=P^{\beta}Q$
   On a
   $$E=Ker\left(P^{\alpha}\left(f\right)\right)\oplus Ker\left(Q\left(f\right)\right)=Ker\left(P^{\beta}\left(f\right)\right)\oplus Ker\left(Q\left(f\right)\right)$$
   Pour $x\in E$, $x=x_1+x_2$ avec $x_1\in KerP^{\beta}\left(f\right)$ et $x_2\in KerQ\left(f\right)$, donc
   $$R\left(f\right)\left(x\right)=R\left(f\right)\left(x_1\right)+R\left(f\right)\left(x_2\right)=Q\left(f\right)\circ P^{\beta}\left(f\right)\left(x_1\right)+P^{\beta}\left(f\right)\circ Q\left(f\right)\left(x_2\right)=0$$
   Par suite $R\left(f\right)\left(x\right)=0$ pour tout $x\in E$.

   On en déduit que $R\left(f\right)=0$ et donc π_f divise R ce qui est absurde .

6. Soit $\pi_f=P_1^{\alpha_1}P_2^{\alpha_2}...P_m^{\alpha_m}$ la décomposition en produit de facteurs irréductibles de π_f .

   D'après la question précédente , on a pour tout $i\in\{1,2,...,m\}$, il existe $x_i\in Ker\left(P_i^{\alpha_i}\left(f\right)\right)$
   tel que : $P_i^{\alpha_i}\left(f\right)=\pi_{x_i}$

   D'autre part $\pi_{x_1},\pi_{x_2},...,\pi_{x_m}$ sont deux à deux premiers entre eux , donc
   $$\pi_{x_1+x_2+...+x_p}=ppcm\left(\pi_{x_1},\pi_{x_2},..,\pi_{x_p}\right)=\pi_{x_1}\times\pi_{x_2}\times..\times\pi_{x_p}=P_1^{\alpha_1}P_2^{\alpha_2}...P_m^{\alpha_m}=\pi_f$$

7. (ii)$\Leftrightarrow$(iii) est immédiate , en effet on a π_f divise χ_f et $\deg\left(\chi_f\right)=n$
   Donc $\deg\left(\pi_f\right)=n$ si et seulement si χ_f et π_f sont proportionnels

   Et comme π_f est unitaire et $\chi_f=\left(-1\right)^nX^n+...$

   Donc $\deg\left(\pi_f\right)=n$ si et seulement si $\chi_f=\left(-1\right)^n\pi_f$.

   Reste à établir l'équivalence entre (i) et (ii) .

$(i)\Rightarrow(ii)$ Supposons que f est cyclique , alors il existe $x_0\in E$ tel que : $E=E_{x_0}$

D'après les questions $\mathbf{2}^{\circ})\,(a)$ et $\mathbf{2}^{\circ})\,(b)$, on a $n=\dim E=\dim E_x=\deg\left(\pi_x\right)\leqslant\deg\left(\pi_f\right)\leqslant n$
Donc $\deg\left(\pi_f\right)=n$.

$(ii)\Rightarrow(i)$ Supposons que $\deg\left(\pi_f\right)=n$. Soit $x_0\in E$ tel que $\pi_{x_0}=\pi_f$

Alors $\dim E_{x_0}=\deg\left(\pi_f\right)=n=\dim E$ donc $E=E_{x_0}$ par suite f est cyclique .

POLYNÔME MINIMAL EN UN VECTEUR

8. Supposons que f est cyclique , soit $x_0 \in E$ tel que $E = E_{x_0}$.

   (a) On va établir que $\mathcal{B} = \left(x_0, f(x_0), ..., f^{n-1}(x_0)\right)$ est une base de E .

   Soit $(\lambda_0, \lambda_1, ..., \lambda_{n-1}) \in \mathbb{K}^n$ tel que : $\lambda_0 x_0 + \lambda_1 f(x_0) + ... + \lambda_{n-1} f^{n-1}(x_0) = 0$

   Posons $P = \lambda_0 + \lambda_1 X + ... + \lambda_{n-1} X^{n-1}$, on a $P(f)(x_0) = 0$

   Donc $\pi_{x_0} = \pi_f$ divise P et comme $\deg(P) \leqslant n-1$ alors $P = 0$ par suite $\lambda_0 = \lambda_1 = ... = \lambda_{n-1} = 0$

   $\mathcal{B}$ est libre et $Card(\mathcal{B}) = n$ donc base .

   (b) $\mathcal{B}$ étant base de E donc il existe $(a_0, a_1, ..., a_{n-1}) \in \mathbb{K}^n$ tel que :

   $$f^n(x_0) = a_0 x_0 + a_1 f(x_0) + ... + a_{n-1} f^{n-1}(x_0)$$

   La matrice de f dans la base $\mathcal{B}$ est alors :

   $$mat_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \ddots & \vdots & a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}$$

   Soit $P = X^n - a_{n-1}X^{n-1} - ... - a_1 X - a_0$, On a

   $$P(f)(x_0) = f^n(x_0) - \left(a_0 x_0 + a_1 f(x_0) + ... + a_{n-1} f^{n-1}(x_0)\right) = 0$$

   Donc $\pi_{x_0} = \pi_f$ divise P et comme $\deg(P) = n = \deg(\pi_f)$ et sont unitaires donc $P = \pi_f$

   f étant cyclique donc $\chi_f = (-1)^n \pi_f = (-1)^n \left(X^n - \sum_{i=0}^{n-1} a_i X^i\right)$