DM 04 : ENDOMORPHISMES CYCLIQUES

PSI 1 2023/2024 **pour le jeudi 19 octobre 2023**

PARTIE 1 : EXEMPLES ET PREMIÈRE PROPRIÉTÉ

1 La famille $\mathcal{B}$ est déjà génératrice de E par hypothèse. Or si $(a,b,c) \in \mathbb{R}^3$ vérifie $a\sin + b\cos + c = 0$, en dérivant, $a\cos - b\sin = 0$ qu'on évalue en $x = 0$ pour avoir $a = 0$, puis en $x = \dfrac{\pi}{2}$ pour obtenir $b = 0$. Il vient ensuite $c = 0$ et la famille $\mathcal{B}$ est aussi libre donc $\boxed{\mathcal{B} \text{ est une base de } E}$ qui est donc de dimension 3. La linéarité de u est celle de la dérivation. Mais il faut vérifier que E est stable par dérivation ce qui se fait en constatant que $u(\sin) = \cos \in E$, $u(\cos) = -\sin \in E$ et $u(1) = 0 \in E$, $\boxed{u \text{ est un endomorphisme de } E.}$

Si $f_0 = 1 + \sin$, $u(f_0) = \cos$ et $u^2(f_0) = -\sin$ donc $\big(f_0, u(f_0), u^2(f_0)\big)$ est une base de E, donc $\boxed{u \text{ est cyclique.}}$

2 Pour $(\lambda, x, x', y, y', z, z') \in \mathbb{R}^7$, on a $u\big(\lambda(x,y,z) + (x',y',z')\big) = (\lambda x + x', \lambda y + y', \lambda z + z') = \lambda(u(x,y,z) + u(x',y',z')$ donc u est linéaire. De plus, on a clairement $u^2 = \mathrm{id}_E$ avec $E = \mathbb{R}^3$ donc u est une symétrie de E.
On a $F = \mathrm{Ker}(u - \mathrm{id}_E) = \{(x,y,z) \in E \mid x = y\} = \mathrm{Vect}\big((1,1,0),(0,0,1)\big)$ qui est un plan et on a aussi $G = \mathrm{Ker}(u + \mathrm{id}_E) = \{(x,y,z) \in E \mid x + y = z = 0\} = \mathrm{Vect}\big((1,-1,0)\big)$ qui est une droite. Par conséquent, d'après le cours, $\boxed{u \text{ est la symétrie par rapport à } F \text{ parallèlement à } G.}$

Comme, pour tout vecteur $v \in E$, $(v, u(v), u^2(v)) = (v, u(v), v)$ est liée, $\boxed{u \text{ n'est pas cyclique.}}$

3 Nilpotence

3.1 Comme $u^{p-1} \neq 0$, il existe $x_0 \in E$ tel que $u^{p-1}(x_0) \neq 0$. Si $\sum\limits_{k=0}^{p-1} \lambda_k u^k(x_0) = 0$ (R), on applique u^{p-1} à (R) et on obtient (comme $u^j = 0$ dès que $j \geqslant p$) : $\lambda_0 u^{p-1}(x_0) = 0$ donc $\lambda_0 = 0$. On peut répéter l'opération en composant cette fois-ci par u^{p-2} pour obtenir $\lambda_1 = 0$, etc..... $\boxed{\text{la famille } \big(x_0, \cdots, u^{p-1}(x_0)\big) \text{ est libre.}}$

Elle a n vecteurs et $\dim(E) = n$ donc $\boxed{\text{la famille } \big(x_0, \cdots, u^{n-1}(x_0)\big) \text{ est une base de } E \text{ donc } u \text{ est cyclique.}}$

3.2 D'abord, comme $\big(x_0, \cdots, u^{p-1}(x_0)\big)$ de cardinal p est libre dans E de dimension n, on a forcément $p \leqslant n$.
$(\Longrightarrow)$ Par contre-apposée, si $p < n$, pour tout $x_1 \in E$, la famille $\big(x_1, \cdots, u^{p-1}(x_1), u^p(x_1), \cdots, u^{n-1}(x_1)\big)$ est liée car elle contient le vecteur nul $u^p(x_1)$; ainsi u n'est pas cyclique.
$(\Longleftarrow)$ Si $p = n$, la famille $\big(x_0, \cdots, u^{p-1}(x_0)\big)$ est libre et a n vecteurs dans E de dimension n donc c'en est une base et par définition u est cyclique.

Au final, on a bien $\boxed{\big(u \text{ est cyclique}\big) \Longleftrightarrow \big(p = n\big).}$

4 Minoration du rang d'un cyclique

4.1 D'après le cours, $\mathrm{Im}\,(u) = \mathrm{Vect}\big(u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0), u^n(x_0)\big)$ car $\big(x_0, u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0)\big)$ est une base de E. En passant aux dimensions, $\boxed{\mathrm{rang}\,(u) = \mathrm{rang}\,\big(u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0), u^n(x_0)\big).}$

4.2 La famille $\big(u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0)\big)$ est libre puisque c'est une sous-famille d'une base donc le rang vaut n si $u^n(x_0) \notin \mathrm{Vect}\big(u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0)\big)$ et $n-1$ si $u^n(x_0) \in \mathrm{Vect}\big(u(x_0), u^2(x_0), \cdots, u^{n-1}(x_0)\big)$.

On a donc uniquement deux cas, $\boxed{\mathrm{rang}\,(u) = n - 1 \text{ ou } \mathrm{rang}\,(u) = n.}$

PARTIE 2 : C'EST DU PROPRE

1 Si on avait $r = 1$, on aurait (e_1) liée alors que $e_1 \neq 0$, c'est absurde donc $\boxed{r \geqslant 2.}$ On applique u à la relation (1) $\alpha_1 e_1 + \cdots + \alpha_r e_r = 0$ pour obtenir (2) $\alpha_1 \lambda_1 e_1 + \cdots + \alpha_r \lambda_r e_r = 0$ (linéarité de u et $\forall k \in [\![1;r]\!],\ u(e_k) = \lambda_k e_k$). On effectue maintenant $(2) - \lambda_r(1)$ et on a bien $\boxed{\alpha_1(\lambda_1 - \lambda_r)e_1 + \cdots + \alpha_{r-1}(\lambda_{r-1} - \lambda_r)e_{r-1} = 0.}$

2 Si on avait $\alpha_1 = \cdots = \alpha_{r-1} = 0$, on aurait $\alpha_r e_r = 0$ donc $\alpha_r = 0$ et la famille $(\alpha_1, \cdots, \alpha_r) \in \mathbb{R}^r$ serait nulle contrairement à l'énoncé. Ainsi, comme $\lambda_1 - \lambda_r \neq 0, \cdots, \lambda_{r-1} - \lambda_r \neq 0$, la famille $(e_1, \cdots, e_{r-1})$ serait liée ce qui contredit encore la définition de r. Par conséquent, $\boxed{(e_1, \cdots, e_n) \text{ est libre et c'est donc une base de } E.}$

3 Par une récurrence facile : $\boxed{\forall k \in \mathbb{N},\ u^k(x_0) = \lambda_1^k e_1 + \cdots + \lambda_n^k e_n.}$

4 Il suffit de montrer que $\big(x_0, \cdots, u^{n-1}(x_0)\big)$ est libre pour justifier que c'est une base de E (son cardinal est égal à la dimension de E). Prenons donc $\big(\alpha_0, \cdots, \alpha_{n-1}\big) \in \mathbb{R}^n$ tel que $\sum\limits_{k=0}^{n-1} \alpha_k u^k(x_0) = 0$. On a alors $\sum\limits_{k=0}^{n-1} \alpha_k \sum\limits_{i=1}^{n} \lambda_i^k e_i = 0$ d'après 2.3. On inverse la somme double et $\sum\limits_{i=1}^{n} \Big(\sum\limits_{k=0}^{n-1} \alpha_k \lambda_i^k\Big) e_i = 0 = \sum\limits_{i=1}^{n} P(\lambda_i) e_i$ en posant $P = \sum\limits_{k=0}^{n-1} \alpha_k X^k \in \mathbb{R}_{n-1}[X]$. Mais comme $(e_1, \cdots, e_n)$ est une base, on a $\forall i \in [\![1;n]\!],\ P(\lambda_i) = 0$ donc $P = 0$ car il possède n racines distinctes deux à deux et $\deg(P) \leqslant n - 1$.
Ainsi, $\alpha_0 = \cdots = \alpha_{n-1} = 0$ et on déduit que $\boxed{\big(x_0, \cdots, u^{n-1}(x_0)\big) \text{ est une base de } E \text{ et } u \text{ est cyclique.}}$

PARTIE 3 : POLYNÔMES ANNULATEURS

1 Polynôme minimal d'un endomorphisme cyclique

1.1 $\boxed{Ann(u) \text{ est un idéal de } \mathbb{R}[X].}$ La famille $(\mathrm{id}_E, u, \cdots, u^{n^2})$ comporte n^2 vecteurs dans $\mathcal{L}(E)$ de dimension n^2, elle est donc liée et $\exists(\alpha_0, \cdots, \alpha_{n^2}) \neq (0, \cdots, 0) \in \mathbb{R}^{n^2+1}$, $\sum\limits_{k=0}^{n^2} \alpha_k f^k = 0$ donc $P = \sum\limits_{k=0}^{n^2} \alpha_k X^k \neq 0$ est un polynôme annulateur de u. L'idéal $Ann(u)$ est principal donc engendré par un polynôme unitaire π_u (diviser par le coefficient dominant). Soit Q unitaire tel que $Ann(u) = \pi_u \mathbb{R}[X] = Q\,\mathbb{R}[X]$, alors $Q \in \pi_u \mathbb{R}[X]$ donc π_u divise Q ; de même, $\pi_u \in Q\,\mathbb{R}[X]$ donc Q divise π_u et comme les deux polynômes sont unitaires : $Q = \pi_u$. Ainsi, $\boxed{\text{il existe un unique polynôme } \pi_u \text{ non nul unitaire tel que } Ann(u) = \pi_u\,\mathbb{R}[X].}$

1.2 Il suffit d'écrire $u^n(x_0)$ dans la base $\big(x_0, \cdots, u^{n-1}(x_0)\big)$: $u^n(x_0) = \beta_{n-1} u^{n-1}(x_0) + \cdots + \beta_1 u(x_0) + \beta_0 x_0$ et de poser, $\forall k \in [\![0;n]\!],\ \alpha_k = -\beta_k$. $\boxed{\exists(\alpha_0, \cdots, \alpha_{n-1}) \in \mathbb{K}^n,\ u^n(x_0) + \alpha_{n-1} u^{n-1}(x_0) + \cdots + \alpha_0 x_0 = 0.}$

1.3 Posons $Q = X^n + \sum\limits_{k=0}^{n-1} \alpha_k X^k$, on a $Q(u)(x_0) = 0$ d'après 3.1.2. On compose par u et on obtient ainsi $(u \circ Q(u))(x_0) = (Q(u) \circ u)(x_0) = Q(u)(u(x_0)) = 0$. On continue à composer par u (par récurrence sur k) et $\forall k \in [\![0;n]\!],\ Q(u)(u^k(x_0)) = 0$ donc l'endomorphisme $Q(u)$ s'annule sur tous les vecteurs de la base $\big(x_0, \cdots, u^{n-1}(x_0)\big)$. Ainsi, $Q(u) = 0$ donc π_u divise Q. S'il existait un polynôme $U = \sum\limits_{k=0}^{d} a_k X^k$ non nul de degré strictement inférieur à n dans $\mathrm{Ann}(u)$, en évaluant en x_0 on aurait $U(u)(x_0) = \sum_{k=0}^{d} a_k u^k(x_0) = 0$ avec $d < n$ donc la famille $\big(x_0, \cdots, , u^{n-1}(x_0)\big)$ serait liée, ce qui est absurde. Alors, $\boxed{\pi_u = X^n + \sum_{k=0}^{n-1} \alpha_k X^k.}$

1.4 Clairement $\mathbb{R}_{n-1}[u] \subset \mathbb{R}[u]$ car si $P \in \mathbb{R}_{n-1}[X]$, alors $P \in \mathbb{R}[X]$. Réciproquement, si $v \in \mathbb{R}[u]$, alors il existe $P \in \mathbb{R}[X]$ tel que $v = P(u)$. On effectue la division euclidienne de P par π_u et on a donc $R \in \mathbb{R}_{n-1}[X]$ et $Q \in \mathbb{R}[X]$ tels que $P = Q\pi_u + R$. Mais alors $v = P(u) = Q(u) \circ \pi_u(u) + R(u)$ par les propriétés des polynômes d'endomorphismes. Ainsi, $v = P(u) = R(u) \in \mathbb{R}_{n-1}[u]$ car $\pi_u(u) = 0$, $\boxed{\mathbb{R}[u] = \mathbb{R}_{n-1}[u].}$

Ainsi, la famille $\big(\mathrm{id}_E, u, \cdots, u^{n-1}\big)$ est génératrice de $\mathbb{R}[u]$. De plus, si elle était liée, il existerait un polynôme annulateur de u de degré strictement inférieur à n ce qui est absurde car π_u est de degré n, ainsi $\boxed{\big(\mathrm{id}_E, u, \cdots, u^{n-1}\big) \text{ est une base de } \mathbb{R}[u].}$

2 Réunion de sous-espaces

2.1 Si F est une droite et si $F = \bigcup_{k=1}^{r} G_k$ avec G_k des sous-espaces de F, si tous les G_k étaient réduits à $\{0\}$, on aurait $F = \{0\}$ NON ! Ainsi, $\exists k \in [\![1;r]\!]$, $G_k \neq \{0\}$ et puisque $\dim(F) = 1$, on a $G_k = F$ et $\boxed{\mathcal{P}_1 \text{ est vraie.}}$

Soit $m \geqslant 2$ et $(f_1, \cdots, f_m)$ une base de F, $\lambda \in \mathbb{R}$ et $H_\lambda = \mathrm{Ker}(\varphi_\lambda)$ avec $\varphi_\lambda\Big(\sum_{k=1}^{m} x_k f_k\Big) = x_1 + \lambda x_2$. Les $(\varphi_\lambda)_{\lambda\in\mathbb{R}}$ sont des formes linéaires non nulles car $\varphi_\lambda(e_1) = 1 \neq 0$, les $(H_\lambda)_{\lambda\in\mathbb{R}}$ des hyperplans de F distincts 2 à 2 car le vecteur $-\lambda f_1 + f_2$ appartient à H_λ mais pas aux H_μ si $\lambda \neq \mu$.

Par conséquent, $\boxed{\text{tout espace de dimension finie } m \geqslant 2 \text{ possède une infinité d'hyperplans.}}$

2.2 Soit $m \geqslant 1$, F de dimension $m+1$, on suppose $\mathcal{P}_m$ vraie. Si $F = \bigcup_{k=1}^{r} G_k$ avec G_k des sous-espaces stricts (non égaux à F) de F et si H est un hyperplan de F, alors $H = H \cap F = \bigcup_{k=1}^{r} (H \cap G_k)$ donc il existe $k \in [\![1;r]\!]$ tel que $H \cap G_k = H$ (d'après $\mathcal{P}_m$) puis $G_k = H$ avec les dimensions. Ainsi chaque hyperplan de F est l'un des sous-espaces $G_1, \cdots, G_r$ ce qui est impossible puisqu'il en existe une infinité car $m+1 \geqslant 2$. Il existe donc un des G_k qui n'est pas strict donc égal à F et $\mathcal{P}_{m+1}$ est donc aussi vraie.

Par principe de récurrence, $\boxed{\forall m \geqslant 1,\ \mathcal{P}_m \text{ est vraie.}}$

3 Réciproque

3.1 Le polynôme nul est dans A_x. De plus, si $(P,Q) \in (A_x)^2$, alors $(P-Q)(u)(x) = P(u)(x) - Q(u)(x) = 0 - 0 = 0$ donc $P - Q \in A_x$. Si $P \in A_x$ et $U \in \mathbb{R}[X]$, $(UP)(u)(x) = \big(U(u) \circ P(u)\big)(x) = U(u)\big(P(u)(x)\big) = U(u)(0) = 0$ donc $UP \in A_x$. On en déduit que $\boxed{A_x \text{ est un idéal de } \mathbb{R}[X].}$

Comme $A_x \neq \{0\}$ puisque $\pi_u \in A_x$, $\boxed{\text{il existe un unique polynôme unitaire } \pi_x \text{ tel que } A_x = \pi_x\,\mathbb{R}[X]}$ car tout idéal de $\mathbb{R}[X]$ est principal (unicité comme au 3.1.1). De plus $\pi_u \in A_x = \pi_x\,\mathbb{R}[X]$ donc $\boxed{\pi_x \text{ divise } \pi_u.}$

3.2 Par unicité de la décomposition en produit de polynômes irréductibles, les diviseurs réels unitaires de π_u sont les $\prod_{k=1}^{r} (X - \alpha_k)^{m'_k} \prod_{k=1}^{s} (X^2 + \beta_k X + \gamma_k)^{n'_k}$ avec $m'_k \leqslant m_k$, $n'_k \leqslant n_k$, $\boxed{\text{il y en a } \prod_{k=1}^{r} (m_k + 1) \prod_{k=1}^{s} (n_k + 1).}$

Notons A l'ensemble de ces diviseurs unitaires de π_u et $\theta : \mathsf{E} \setminus \{0\} \to \mathsf{A}$ l'application définie par $\theta(x) = \pi_x$; il suffit de prendre un vecteur v_i pour chaque polynôme P_i de $\mathrm{Im}\,(\theta) = \{\mathsf{P}_1, \cdots, \mathsf{P}_p\}$ (avec $p = \mathrm{card}\,\big(\mathrm{Im}\,(\theta)\big)$), ainsi $\boxed{\text{il existe } p \geqslant 1 \text{ et } v_1, \cdots, v_p \text{ tels que pour tout } x \in \mathsf{E} \text{ non nul, } \pi_x \in \{\pi_{v_1}, \cdots, \pi_{v_p}\}.}$

3.3 $0_\mathsf{E} \in \bigcup\limits_{k=1}^{p} \mathsf{Ker}\,\big(\pi_{v_k}(u)\big)$. Si $x \neq 0$, alors il existe $k \in [\![1;p]\!]$ tel que $\pi_x = \pi_{v_k}$ donc $\pi_{v_k}(u)(x) = 0$ et on a donc $x \in \mathsf{Ker}\,\big(\pi_{v_k}(u)\big)$. Au final, $\boxed{\mathsf{E} = \bigcup\limits_{k=1}^{p} \mathsf{Ker}\,\big(\pi_{v_k}(u)\big).}$ D'après 3.2, $\boxed{\exists k \in [\![1;p]\!] \text{ tel que } \mathsf{E} = \mathsf{Ker}\,\big(\pi_{v_k}(u)\big).}$

3.4 Soit donc k un entier tel que $\mathsf{E} = \mathsf{F}_k = \mathsf{Ker}(\pi_{v_k}(u))$; on a donc $\forall x \in \mathsf{E},\ x \in \mathsf{F}_k \iff \pi_{v_k}(u)(x) = 0$ d'où $\pi_{v_k}(u) = 0$ ce qui montre que π_u divise π_{v_k}. Mais on sait déjà que π_{v_k} divise π_u d'après la question 3.3.1, on en déduit que $\boxed{\pi_u = \pi_{v_k}.}$ π_{v_k} est donc de degré n et la famille $\big(v_k, \cdots, u^{n-1}(v_k)\big)$ est donc libre (sinon il existerait un polynôme de degré strictement inférieur à n dans A_{v_k}), comme elle possède n vecteurs, c'est une base de E et $\boxed{u \text{ est un endomorphisme cyclique.}}$

PARTIE 4 : COMMUTANT DES CYCLIQUES

1 $\mathrm{id}_\mathsf{E} \in \mathcal{C}(u)$ (clair). Si $\lambda \in \mathbb{R}$ et $(v, w) \in \big(\mathcal{C}(u)\big)^2$, alors $(\lambda v + w) \circ u = \lambda v \circ u + w \circ u = \lambda u \circ v + u \circ w = u \circ (\lambda v + w)$ donc $\lambda v + w \in \mathcal{C}(u)$. De plus, $(v \circ w) \circ u = v \circ (w \circ u) = v \circ (u \circ w) = (v \circ u) \circ w = (u \circ v) \circ w = u \circ (v \circ w)$ donc $v \circ w \in \mathcal{C}(u)$. Par conséquent, $\boxed{\mathcal{C}(u) \text{ est un sous-anneau de } \mathcal{L}(\mathsf{E}).}$

On a vu en 3.1.4 que $\dim\big(\mathbb{R}[u]\big) = n$ or $\mathbb{R}[u] \subset \mathcal{C}(u)$ donc $\dim\big(\mathcal{C}(u)\big) \geqslant n$. De plus, comme $\mathcal{C}(u) \subset \mathcal{L}(\mathsf{E})$, on a $\dim\big(\mathcal{C}(u)\big) \leqslant n^2$. Au final, $\boxed{n \leqslant \dim\big(\mathcal{C}(u)\big) \leqslant n^2.}$

2 **Base et dimension de $\mathcal{C}(u)$**

2.1 Il suffit de décomposer le vecteur $v(x_0)$ de E dans la base $\big(x_0, u(x_0), \cdots, u^{n-1}(x_0)\big)$ de E ce qui justifie $\boxed{\text{l'existence de } (\alpha_0, \cdots, \alpha_{n-1}) \in \mathbb{R}^n \text{ tel que } v(x_0) = \alpha_0 x_0 + \alpha_1 u(x_0) + \cdots + \alpha_{n-1} u^{n-1}(x_0).}$

2.2 On a $v \circ \mathrm{id}_\mathsf{E} = \mathrm{id}_\mathsf{E} \circ v$ et $v \circ u = u \circ v$. Si on suppose pour un entier $k \geqslant 1$ que $v \circ u^k = u^k \circ v$, alors en composant par u à droite, $v \circ u^{k+1} = (u^k \circ v) \circ u = u^k \circ (v \circ u) = u^k \circ (u \circ v) = u^{k+1} \circ v$. Par principe de récurrence, on a même $\boxed{\forall k \in \mathbb{N},\ v \circ u^k = u^k \circ v.}$

2.3 On a $v(x_0) = \alpha_0 x_0 + \alpha_1 u(x_0) + \cdots + \alpha_{n-1} u^{n-1}(x_0)$ qu'on compose, pour $k \in [\![0; n-1]\!]$, par u^k pour obtenir avec 4.2.2, $\forall k \in [\![0; n-1]\!]$, $u^k\big(v(x_0)\big) = v\big(u^k(x_0)\big) = \sum\limits_{j=0}^{n-1} \alpha_j u^k\big(u^j(x_0)\big) = \sum\limits_{j=0}^{n-1} \alpha_j u^j\big(u^k(x_0)\big)$. Si on pose $w = \sum\limits_{j=0}^{n-1} \alpha_j u^j$, ce qui précède justifie que les endomorphismes w et v coïncident sur les vecteurs de la base $\big(x_0, u(x_0), \cdots, u^{n-1}(x_0)\big)$, ils sont donc égaux, $\boxed{v = \alpha_0 \mathrm{id}_\mathsf{E} + \alpha_1 u + \cdots \alpha_{n-1} u^{n-1}.}$

2.4 On savait déjà que $\mathbb{R}[u] = \mathbb{R}_{n-1}[u] \subset \mathcal{C}(u)$ mais on vient de voir que $\mathcal{C}(u) \subset \mathbb{R}_{n-1}[u]$. Par conséquent, $\mathcal{C}(u) = \mathbb{R}_{n-1}[u] = \mathbb{R}[u]$ et on a, d'après 3.1.4, $\boxed{\dim \mathcal{C}(u) = n \text{ car } \big(\mathrm{id}_\mathsf{E}, u, \cdots, u^{n-1}\big) \text{ est une base de } \mathcal{C}(u).}$