Devoir Surveillé n° 9

Correction du problème – Invariants de similitude et réduction de Frobenius

Question préliminaire

Soit $x \in E$.

- Soit $P = 0$ le polynôme nul. Alors $P(u)(x) = 0$, donc $0 \in E_{u,x}$.
- Soit y et z dans $E_{u,x}$ et $\lambda \in \mathbb{K}$. Il existe donc deux polynômes A et B tels que $y = A(u)(x)$ et $z = B(u)(x)$. On a alors
$$\lambda y + z = (\lambda A(u) + B(u))(x) = (\lambda A + B)(u)(x).$$
Comme $\lambda A + B \in \mathbb{K}[X]$, cela montre bien que $\lambda y + z \in E_{u,x}$.

Ainsi, $\boxed{E_{u,x} \text{ est un sous-espace vectoriel de } E}$.

Partie I – Lemme des noyaux

Soit P et Q deux polynômes premiers entre eux.

1. Soit $x \in \mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u))$. On a donc :
$$P(u)(x) = 0 \qquad \text{et} \qquad Q(u)(x) = 0.$$
D'après le théorème de Bézout, il existe U et V deux polynômes tels que $UP + VQ = 1$. On obtient donc :
$$x = \mathrm{id}(x) = 1(u)(x) = U(u)(P(u)(x)) + V(u)(Q(u))(x) = U(u)(0) + V(u)(0) = 0.$$
Par conséquent, $\mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u)) = \{0\}$, donc la somme $\boxed{\mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u)) \text{ est directe}}$.
2. Soit $x \in \mathrm{Ker}(PQ(u))$. On a donc :
$$PQ(u)(x) = 0 \qquad \text{donc:} \qquad Q(u)(P(u)(x)) = Q(u) \circ P(u)(x) = (QP)(u)(x) = 0.$$
Ainsi, $\boxed{P(u)(x) \in \mathrm{Ker}(Q(u)).}$
3. - On a déjà montré que la somme est directe.
   - Soit $x \in \mathrm{Ker}(PQ(u))$. D'après la question précédente, $P(u)(x) \in \mathrm{Ker}(Q(u))$ et de la même manière, $Q(u)(x) \in \mathrm{Ker}(P(u)(x))$ Par conséquent,
$$Q(u) \circ U(u) \circ P(u)(x) = U(u) \circ Q(u) \circ P(u)(x) = 0.$$
On en déduit que $U(u) \circ P(u)(x) \in \mathrm{Ker}(Q(u))$ et de même $V(u) \circ Q(u)(x) \in \mathrm{Ker}(P(u))$. La relation de Bézout donne donc une décomposition de x dans la somme $\mathrm{Ker}(P(u)) + \mathrm{Ker}(Q(u))$. On en déduit que
$$\mathrm{Ker}(PQ(u)) \subset \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u))$$
   - Soit $x \in \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u))$. On peut donc écrire $x = y + z$, avec $y \in \mathrm{Ker}(P(u))$ et $z \in \mathrm{Ker}(Q(u))$. Ainsi,
$$PQ(u)(x) = Q(u)(P(u)(y)) + P(u)(Q(u)(z)) = Q(u)(0) + P(u)(0) = 0.$$
Donc $x \in \mathrm{Ker}(PQ(u))$. Par conséquent, $\mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u)) \subset \mathrm{Ker}(PQ(u))$.

   On en conclut que $\boxed{\mathrm{Ker}(PQ(u)) = \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u))}$ (lemme des noyaux)

4. On montre par récurrence sur n que si $P_1, \dots, P_n$ sont 2 à 2 premiers entre eux, alors

$$\mathrm{Ker}((P_1 \cdots P_n)(u)) = \bigoplus_{i=1}^{n} \mathrm{Ker}(P_i(u)).$$

Le cas $n = 1$ est trivial et le cas $n = 2$ a été démontré dans la question précédente.
Soit $n \geqslant 2$ tel que la formule soit vérifiée pour toute famille de n polynômes premiers entre eux deux à deux. On considère $P_1, \dots, P_{n+1}$ premiers entre eux deux à deux. Alors $P_1 \cdots P_n$ et P_{n+1} sont premiers entre eux (P_{n+1} n'ayant aucun facteur irréductible en commun avec les P_i, $i \leqslant n$, il n'en a pas nonn plus avec leur produit). On applique le cas $n = 2$ à ces deux polynômes :

$$\mathrm{Ker}(P_1 \cdots P_{n+1}(u)) = \mathrm{Ker}(P_1 \dots P_n(u)) \oplus \mathrm{Ker}(P_{n+1}(u)).$$

L'hypothèse de récurrence amène alors :

$$\mathrm{Ker}(P_1 \cdots P_{n+1}(u)) = \bigoplus_{i=1}^{n} \mathrm{Ker}(P_i(u)) \oplus \mathrm{Ker}(P_{n+1}(u)) = \bigoplus_{i=1}^{n+1} \mathrm{Ker}(P_i(u)).$$

D'après le principe de récurrence, pour tout $n \in \mathbb{N}^*$,

$$\boxed{\mathrm{Ker}((P_1 \cdots P_n)(u)) = \bigoplus_{i=1}^{n} \mathrm{Ker}(P_i(u))}.$$

Partie II – Polynôme minimal ponctuel et polynôme minimal

1. Soit $\mathrm{Ann}(u)$ le sous-ensemble de $\mathbb{K}[X]$ constitué des polynômes P tels que $P(u) = 0$.
   (a) La famille $(u^0, \dots, u^{n^2})$ est une famille de cardinal $n^2 + 1$ de $\mathcal{L}(E)$ dont la dimension est n^2. Elle est donc liée. Une relation non triviale entre les termes de cette famille fournit un polynôme annulateur non nul de u. Ainsi, $\boxed{\mathrm{Ann}(u) \neq \{0\}}$.
   (b)
   - Le polynôme nul est clairement un polynôme annulateur de u.
   - Si P et Q sont deux polynômes annulateurs de u, alors

   $$(P - Q)(u) = P(u) - Q(u) = 0,$$

   donc $P - Q \in \mathrm{Ann}(u)$. On en déduit, à l'aide du point précédent, que $\mathrm{Ann}(u)$ est un sous-groupe (additif) de $\mathbb{K}[X]$.
   - Soit $P \in \mathrm{Ann}(u)$ et $Q \in \mathbb{K}[X]$. Alors

   $$(PQ)(u) = Q(u) \circ P(u) = Q(u) \circ 0 = 0.$$

   Ainsi, $PQ \in \mathrm{Ann}(u)$.

   On en déduit que $\boxed{\mathrm{Ann}(u) \text{ est un idéal}}$. Comme $\mathbb{K}[X]$ est principal, $\mathrm{Ann}(u)$ est un idéal principal, engendré par un polynôme $Q_{u,x}$ non nul (d'après la question 1), qu'on peut choisir unitaire (quitte à diviser un générateur queconque par son coefficient dominant). Puisque $\mathrm{Ann}(u) = (Q_u)$, tout autre élément non nul de $\mathrm{Ann}(u)$ s'écrit sous la forme RQ_u, avec $R \neq 0$, donc est de degré supérieur ou égal à Q_u.
   Ainsi, Q_u est bien un $\boxed{\text{polynôme annulateur non nul de degré minimal}}$.
2. Soit $x \in E$.
   (a) De même, notons $\mathrm{Ann}_x(u) = \{P \in \mathbb{K}[X] \mid P(u)(x) = 0_E.\}$. Ce sous-ensemble de $\mathbb{K}[X]$ est non réduit à 0, puisqu'il contient en particulier Q_u. De plus, tout comme $\mathrm{Ann}(u)$, il s'agit d'un idéal. En effet :
   - Le polynôme nul est clairement dans $\mathrm{Ann}_x(u)$.
   - Si P et Q sont deux éléments de $\mathrm{Ann}_x(u)$, alors

   $$(P - Q)(u)(x) = P(u)(x) - Q(u)(x) = 0,$$

   donc $P - Q \in \mathrm{Ann}_x(u)$. On en déduit, à l'aide du point précédent, que $\mathrm{Ann}_x(u)$ est un sous-groupe (additif) de $\mathbb{K}[X]$.

- Soit $P \in \mathrm{Ann}(u)$ et $Q \in \mathbb{K}[X]$. Alors

$$(PQ)(u)(x) = Q(u) \circ P(u)(x) = Q(u)(0) = 0.$$

Ainsi, $PQ \in \mathrm{Ann}_x(u)$.

Comme dans la question précédente, $\mathrm{Ann}_x(u)$ est engendré par un $\boxed{\text{polynôme unitaire } Q_{u,x}}$, qui est alors le polynôme non nul de plus petit degré de $\mathrm{Ann}_x(u)$.

(b) La famille $(u^0(x), \dots, u^n(x))$ est une famille de cardinal $n+1$ de l'espace E de dimension n. Elle est donc liée. Une relation non triviale entre ces vecteurs fournit un polynôme Q de degré au plus n tel que $Q(u)(x) = 0$, donc $Q \in \mathrm{Ann}_x(u)$. Par minimalité du degré de $Q_{u,x}$, on en déduit que $\boxed{\deg(Q_{u,x}) \leqslant n}$

(c) Comme on l'a déjà constaté, $Q_u \in \mathrm{Ann}_x(u) = (Q_{u,x})$. Ainsi, par déscription de l'idéal engendré par $(Q_{u,x})$, $\boxed{Q_{u,x} \mid Q_u}$.

3. Soit $a_1, \dots, a_p$ des éléments de E tels que la somme $\bigoplus_{i=1}^{p} E_{u,a_i}$ soit directe. On pose $a = \sum_{i=1}^{p} a_i$.

(a) Par définition de $Q_{u,a}$,

$$0 = Q_{u,a}(u)(a) == Q_{u,a}(u)(a)(a_1 + \cdots + a_p) = Q_{u,a}(u)(a_1) + \cdots + Q_{u,a}(a_p).$$

Comme pour tout $i \in [\![1, p]\!]$, $Q_{u,a}(u)(a_i) \in E_{u,a_i}$, et comme ces espaces sont en somme directe, on en déduit que

$$\forall i \in [\![1, p]\!], \quad Q_{u,a}(u)(a_i) = 0.$$

Ainsi, $Q_{u,a} \in \mathrm{Ann}_{a_i}(u) = Q_{u,a_i}$, d'où il vient $\boxed{Q_{u,a_i} \mid Q_{u,a}}$.

(b) - De la question précédente, on déduit que

$$\bigvee_{i=1}^{p} Q_{u,a_i} \mid Q_{u,a}.$$

- Réciproquement, pour tout $j \in [\![1, p]\!]$, $\bigvee_{i=1}^{p} Q_{u,a_i}$ est un multiple de Q_{u,a_j}, donc est dans $\mathrm{Ann}_{a_j}(u)$. On en déduit que

$$\left(\bigvee_{i=1}^{p} Q_{u,a_i}\right)(u)(a_j) = 0.$$

Ainsi, par linéarité :

$$\left(\bigvee_{i=1}^{p} Q_{u,a_i}\right)(u)(a) = \sum_{j=1}^{n} \left(\bigvee_{i=1}^{p} Q_{u,a_i}\right)(u)(a_j) = 0.$$

On en déduit que $\bigvee_{i=1}^{p} Q_{u,a_i} \in \mathrm{Ann}_a(u) = (Q_{u,a})$, donc est un multiple de $Q_{u,a}$.

- Ainsi, $\bigvee_{i=1}^{p} Q_{u,a_i}$ et $Q_{u,a}$ sont associés et tous deux unitaires, donc

$$\boxed{\bigvee_{i=1}^{p} Q_{u,a_i} = Q_{u,a}}.$$

4. On montre dans cette question que le polynôme minimal de u peut être réalisé comme polynôme minimal ponctuel en un certain vecteur a.

Soit $Q_u = P_1^{a_1} \cdots P_r^{\alpha_r}$ la décomposition du polynôme minimal Q_u en facteurs irréductibles ($r \geqslant 1$, $\alpha_i \geqslant 1$).

(a) - Dans un premier temps, soit $x \in \mathrm{Ker}(P_i^{\alpha_i - 1}(u))$. Ainsi,

$$P_i^{\alpha_i - 1}(u)(x) = 0, \qquad \text{donc:} \qquad P_i^{\alpha_i}(u)(x) = P_i(u)(P_i^{\alpha_i - 1}(u)(x)) = P_i(u)(0) = 0.$$

On en déduit que $\boxed{\mathrm{Ker}(P_i^{\alpha_i - 1}(u)) \subset \mathrm{Ker}(P_i^{\alpha_i}(u))}$.

- Supposons qu'on ait l'égalité $\mathrm{Ker}(P_i^{\alpha_i-1}(u)) = \mathrm{Ker}(P_i^{\alpha_i}(u))$. Soit $x \in E$. Comme Q_u est un polynôme annulateur,

$$0 = Q_u(u)(x) = P_i^{\alpha_i}(u)\left(\left(\prod_{j\neq i} P_j^{\alpha_j}\right)(u)(x)\right).$$

Ainsi,

$$\left(\prod_{j\neq i} P_j^{\alpha_j}\right)(u)(x) \in \mathrm{Ker}(P_i^{\alpha_i}(u)) = \mathrm{Ker}(P_i^{\alpha_i-1}(u)).$$

On obtient donc

$$0 = P_i^{\alpha_i-1}(u)\left(\left(\prod_{j\neq i} P_j^{\alpha_j}\right)(u)(x)\right) = \left(\frac{Q_u}{P_i}\right)(u)(x).$$

Comme ceci est vrai pour tout x de E, on en déduit que le polynôme $\frac{Q_u}{P_i}$ est encore un polynôme annulateur de u, qui contredit la minimalité du degré de Q_u.
Ainsi, $\boxed{\mathrm{Ker}(P_i^{\alpha_i-1}(u)) \neq \mathrm{Ker}(P_i^{\alpha_i}(u))}$.

(b) Soit $a_i \in \mathrm{Ker}(P_i^{\alpha_i}(u)) \setminus \mathrm{Ker}(P_i^{\alpha_i-1}(u))$. On a donc $P_i^{\alpha_i}(u)(a_i) = 0$, donc $P_i^{\alpha_i} \in \mathrm{Ann}_{a_i}(u)$. On en déduit que $Q_{u,a_i} \mid P_i^{\alpha_i}$.
Puisque P_i est irréductible, Q_{u,a_i} est de la forme $P_i^{\beta_i}$, pour un $\beta_i \leqslant \alpha_i$.
Par ailleurs, $a_i \notin \mathrm{Ker}(P_i^{\alpha_i-1}(u))$, donc $P^{\alpha_i-1}(u)(a_i) \neq 0$, donc $P_i^{\alpha_i-1} \notin \mathrm{Ann}_{a_i}(x)$. Par conséquent, Q_{u,a_i} ne divise pas $P_i^{\alpha_i-1}$, donc $\beta_i > \alpha_i - 1$.
On en déduit que $\boxed{Q_{u,a_i} = P_i^{\alpha_i}}$.

(c)
- Pour tout $x \in E_{u,a_i}$, il existe P tel que $x = P(u)(a_i)$. On a alors :

$$Q_{u,a_i}(u)(x) = (Q_{u,a_i}P)(u)(a_i) = P(u)(Q_{u,a_i}(u)(a_i)) = P(u)(0) = 0.$$

Ainsi, $E_{u,a_i} \subset \mathrm{Ker}(Q_{u,a_i})(u) = \mathrm{Ker}(P_i^{\alpha_i}(u))$
- Les espaces $\mathrm{Ker}(P_i^{\alpha_i}(u))$ étant en somme directe d'après le lemme des noyaux, il en est de même des E_{u,a_i}. Ainsi, d'après la question 3, il existe a tel que

$$Q_{u,a} = \bigvee_{i=1}^{r} Q_{u,a_i}.$$

- Puisque pour tout $i \in [\![1, r]\!]$, $Q_{u,a_i} = P_i^{\alpha_i}$, et puisque ces polynômes sont premiers entre eux,

$$\bigvee_{i=1}^{r} Q_{u,a_i} = \prod_{i=1}^{r} P_i^{\alpha_i} = Q_u.$$

On en conclut que $\boxed{Q_{u,a} = Q_u}$.
On déduit en particulier, avec 2b, que $\boxed{\deg(Q_u) \leqslant n}$.

Partie III – Endomorphismes cycliques, sous-espaces u-monogènes

1. Soit u un endomorphisme cyclique de E et x tel que $E_{u,x} = E$. On note $d = \deg(Q_{u,x})$.

(a) Soit $y \in E = E_{u,x}$. On peut donc écrire $y = P(u)(x)$, pour un certain polynôme P. En effectuant la division euclidienne de P par $Q_{u,x}$, on trouve deux polynômes A et R, avec $\deg(R) < d$, tels que

$$y = (AQ_{u,x} + R)(u)(x) = A(u)(Q_{u,x}(u)(x)) + R(u)(x) = A(u)(0) + R(u)(x) = R(u)(x).$$

Puisque $\deg R < d$, on peut écrire $R = \sum_{i=0}^{d-1} a_i X^i$. Il vient alors :

$$y = \sum_{i=1}^{d} a_i u^i(x) \in \mathrm{Vect}(x, u(x), \ldots, u^{d-1}(x)).$$

Ceci étant vrai pour tout y, on en déduit que $\boxed{(x, u(x), \cdots, u^{d-1}(x)) \text{ est une famille génératrice de } E}$
Son cardinal est donc au moins égal à la dimension de E, à savoir n. Ainsi, $d \geqslant n$. La question II-2b amène alors $\boxed{d = n}$.

(b) Par ailleurs, on sait que $Q_{u,x} \mid Q_u$ et $\deg(Q_u) \leqslant n$ d'après II-4c. Ainsi, ces deux polynômes étant unitaires, et Q_u étant non nul, on obtient $\boxed{Q_{u,x} = Q_u}$.

(c) Puisque la famille $\boxed{\mathcal{B} = (b_1, \ldots, b_n) = (u^0(x), \ldots, u^{n-1}(x))}$ est génératrice de E et de cardinal $n = \dim(E)$, c'en est une base. En notant

$$Q_{u,x} = Q_u = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

il vient alors :

$$u(b_1) = b_2, \qquad u(b_2) = b_3, \qquad \ldots, \qquad u(b_{n-1}) = b_n, \qquad ,$$

et, puisque $Q_u(u)(x) = 0$

$$u(b_n) = u^n(x) = -\sum_{i=0}^{n-1} a_i u^i(x) = -\sum_{i=0}^{n-1} a_i b_i.$$

Les coordonnnées de $u(b_n)$ dans la base $\mathcal{B}$ sont donc bien la colonne des coefficients $-a_i$. On obtient donc bien la description de la matrice :

$$\boxed{\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},}$$

2. Soit F un sous-espace vectoriel u-monogène.

(a) Soit x tel que $F = E_{u,x}$. Soit $y \in F$. Il existe donc $P \in \mathbb{K}[X]$ tel que $y = P(u)(x)$. Ainsi, $u(y) = u \circ P(u)(x) = (XP)(u)(x)$. On en déduit que $u(y) \in F$. Ainsi, $\boxed{F \text{ est stable par } u.}$

(b) C'est à peu près par définition ! Puisque $F = E_{u,x}$, $x = \mathrm{id}(x) = 1(u)(x) \in E_{u,x} = F$. Par conséquent, on a aussi $E_{u,x} = E_{u_F,x}$, donc $F = E_{u_F,x}$. Par définition, on en déduit que $\boxed{u_F \text{ est cyclique}}$.

Partie IV – Théorème des invariants de similitude

1. Soit $d = \deg(Q_u)$. D'après la partie II, il existe $a \in E$ tel que $Q_u = Q_{u,a}$. Soit $F = E_{u,a}$. Par définition, F est u-monogène. De plus, d'après III-2, u induit un endomorphisme cyclique u_F sur F, et

$$Q_{u_F,a} = Q_{u,a} = Q_u.$$

De plus, d'après la question III-1a $\deg(Q_{u_F,a}) = \dim(F)$, d'où $\boxed{\dim F = d}$.

2. La famille $(u^0(a), \ldots, u^{d-1}(a))$ est donc une base de F. On peut la compléter en une base $(e_1, \ldots, e_n)$ de E.

(a) G est un sous-espace vectoriel de E en tant qu'intersection de sous-espaces. Soit $x \in E$. Ainsi, pour tout $i \in \mathbb{N}$,

$$e_d^* \circ u^i(x) = 0.$$

On en déduit que pour tout $i \in \mathbb{N}$, on a aussi

$$e_d^* \circ u^{i+1}(x) = 0 \qquad \text{donc:} \qquad e_d^* \circ u^i(u(x)) = 0.$$

Ainsi, $u(x) \in G$. Par conséquent, $\boxed{G \text{ est stable par } u}$.

(b) Soit $(\lambda_0, \dots, \lambda_{d-1})$ une famille de scalaires tels que

$$\sum_{i=0}^{d-1} \lambda_i e_d^* \circ u^i = 0.$$

On a donc

$$e_d^* \circ \left(\sum_{i=0}^{d-1} \lambda_i u^i \right) = 0$$

En évaluant en a, il vient :

$$0 = e_d^* \left(\sum_{i=0}^{d-1} \lambda_i u^i(a) \right) = e_d^* \left(\sum_{i=0}^{d-1} \lambda_i e_i \right) = \lambda_{d-1},$$

par définition de e_d^*. On peut alors évaluer en $u(a)$:

$$0 = e_d^* \left(\sum_{i=0}^{d-1} \lambda_i u^i(u(a)) \right) = e_d^* \left(\sum_{i=0}^{d-2} \lambda_i e_{i+1} \right) = \lambda_{i-1}.$$

En itérant ce procédé, on montre que $\lambda_0 = \dots = \lambda_{d-1} = 0$. Ainsi, $\boxed{\text{la famille } (e_d^* \circ u^i)_{i \in [\![0,d-1]\!]} \text{ est libre}}$.

(c) Soit $f_1, \dots, f_d$ des formes linéaires sur E de dimension n, linéairement indépendantes. Montrons que

$$\dim \left(\bigcap_{i=1}^{d} \mathrm{Ker}(f_i) \right) = n - d.$$

Soit $\mathcal{C}$ une base de E, et $L_i = \mathrm{Mat}_{\mathcal{C},(1)}(f_i)$ la matrice ligne représentant f_i dans cette base (on a choisi la base (1) à l'arrivée). Les lignes L_i forment une famille libre. Soit f l'application linéaire de E dans $\mathbb{K}^d$ définie par

$$f(x) = (f_1(x), \dots, f_d(x)).$$

Alors, $M = \mathrm{Mat}_{\mathcal{B},bc}(f)$ est la matrice dont les lignes sont les L_i. Ces d lignes formant une famille libre, $\mathrm{rg}(M) = d$, donc $\mathrm{rg}(f) = d$. D'après le théorème du rang, il vient donc $\dim(\mathrm{Ker}(f)) = n - d$.
Or $f(x) = 0$ si et seulement si pour tout $i \in [\![1, d]\!]$, $f_i(x) = 0$, donc

$$\mathrm{Ker}(f) = \bigcap_{i=1}^{d} \mathrm{Ker}(f_i).$$

On en déduit que

$$\dim \left(\bigcap_{i=1}^{d} \mathrm{Ker}(f_i) \right) = n - d.$$

Il suffit alors d'appliquer ce résultat à la famille $(e_d^* \circ u^i)_{i \in [\![0,d-1]\!]}$ pour obtenir $\dim G = n - d$.

(d)
- Soit $x \in F \cap G$. Alors il existe P un polynôme de degrén strictement inférieur à d tel que $x = P(u)(a)$. De plus, pour tout $i \in [\![1, d]\!]$, $e_d^* \circ u^i(x) = 0$. Notons $P = \sum_{k=0}^{d} a_k X^k$. On a alors :

$$e_d^* \circ u^i(x) = \sum_{k=0}^{d} a_k u^{k+i}(a).$$

  On utilise le même procédé que pour l'étude de la liberté en 2b : pour $i = 1$, on obtient, par définition de e_d^*, $a_d = 0$, puis a_{d-1} avec $i = 2$, etc. Ainsi, $P = 0$, puis $x = 0$. On en déduit que la somme $F \oplus G$ est directe.
- Par ailleurs, $\dim(F) + \dim(G) = \dim(E)$, d'après la question précédente, donc, puisque la somme est directe, $\boxed{F \oplus G = E}$.

(e) D'après III-1b, le polynôme minimal P_1 de l'endomorphisme cyclique est $Q_{u,a} = Q_u$. Puisque $Q_u(u) = 0$, on a aussi $Q_u(u_G) = 0$, donc Q_u est un polynôme annulateur de u_G. On en déduit que le polynôme minimal de u_G divise $Q_u = P_1$. Ainsi, $\boxed{P_2 \mid P_1}$.

3. On raisonne par réucurrence sur la dimension de E. On ajoute à la propriété de récurrence le fait que P_1 est le polynôme minimal de u.

- Si E est de dimension 1, tout endomorphisme non nul est cyclique ($E = E_{u,x}$, pour tout $x \neq 0$, puisque $E_{u,x}$ contient $u^0(x) = x$). De plus, puisque $F_1 = E$, P_1 est le polynôme minimal de u.
- Soit $n \geqslant 2$ tel que tout endomorphisme d'un espace de dimension strictement inférieure à n vérifie le théorème des invariants de similitude. Soit E un espace de dimension n, et u un endomorphisme de E. On construit F et G comme ci-dessus. Si $F = E$, alors u est cyclique, et vérifie donc trivialement le théorème (et comme dans l'initialisation, l'unique polynôme dans la suite des invariants de similitude est le polunôme minimal de u). Sinon, G est non nul, de dimension strictement inférieure à F. L'endomorphisme u_G vérifie donc le théorème. Il existe donc des sous-espaces u_G-monogènes $F_2, \dots, F_r$ (donc aussi u-monogènes), tels que les polynômes annulateurs des induits de u_G (qui sont aussi les induits de G) vérifient $P_r \mid \cdots \mid P_2$, et P_2 est le polynôme minimal de u_G. On pose alors $F_1 = F$, et on a la décomposition voulue. On remarque que $P_2 \mid P_1$ d'après la question précédente, et que la construction ci-dessus prouve bien que P_1 est le polynôme minimal de u.
- D'après le principe de récurrence, cela prouve le théorème des invariants de similitude.

4. Soit $(F_1, \dots, F_r)$ et $(G_1, \dots, G_s)$ deux suites de sous-espaces u-monogènes vérifiant les conditions du théorème des invariants de similitude, et $P_1, \dots, P_r$, $Q_1, \dots, Q_s$ les deux suites de polynômes associées. On suppose qu'elles ne sont pas égales, et on note j le plus grand indice tel que $P_i = Q_i$ pour tout $i \in [\![1, j-1]\!]$.

   (a) D'après les questions III-1a et III-1b, pour tout $i \in [\![1, r]\!]$, $\deg(P_i) = \dim(F_i)$. Comme la somme des F_i est directe, et égale à E, on a alors :

$$\boxed{n = \dim(E) = \sum_{i=1}^{r} \dim(F_i) = \sum_{i=1}^{r} \deg(P_i)}.$$

   Le même raisonnement avec la deuxième suite amène :

$$\boxed{n = \sum_{i=1}^{s} \deg(Q_i)}.$$

   (b) Pour tout $i \in [\![1, j-1]\!]$, on a $P_i = Q_i$, donc

$$\sum_{i=1}^{j-1} \deg(P_i) = \sum_{i=1}^{j-1} \deg(Q_j).$$

   Si $j > r$ ou $j > s$ (disons $j > r$ pour se fixer les idées), alors par définition de j, $r = j - 1$. Ainsi,

$$\sum_{i=1}^{j-1} \deg(Q_i) = \sum_{i=1}^{j-1} \deg(P_i) = \sum_{i=1}^{r} \deg(P_i) = n.$$

   Ainsi, d'après la question précédente,

$$\sum_{i=j}^{s} \dim(G_i) = 0 \qquad \text{donc:} \qquad \forall i \in [\![j, s]\!], \quad \dim(F_i) = \deg(P_i) = 0.$$

   Ceci contredit la non nullité des F_i. Par conséquent, $[\![j, s]\!] = \varnothing$, puis $r = s$. Les deux suites (P_i) et (Q_i) sont donc égales, ce qui contredit notre hypothèse de départ.
   Ainsi, $\boxed{j \leqslant r \text{ et } j \leqslant s}$.
   En d'autres termes, on n'est arrivé au bout d'aucune des deux suites.

   (c)
   - Les sous-espaces $P_j(u)(F_i)$ sont inclus dans F_i. Comme la somme des F_i est directe, il en découle que $\bigoplus_{i=1}^{j-1} P_j(u)(F_i)$ est directe.
   - De même pour la somme $\bigoplus_{i=1}^{s} P_j(u)(G_i)$.
   - Soit v un endomorphisme d'un espace E, E_1 et E_2 deux sous-espaces de E. Alors :
     * pour tout $y \in v(E_1 + E_2)$, il existe $x_1 \in E_1$ et $x_2 \in E_2$ tels que $y = v(x_1 + x_2)$. On a alors $y = v(x_1) + v(x_2) \in v(E_1) + v(E_2)$.
     * Réciproquement, si $y \in v(E_1) + v(E_2)$, il existe $x_1 \in E_1$ et $x_2 \in E_2$ tel que $y = v(x_1) + v(x_2) = v(x_1 + x_2) \in v(E_1 + E_2)$.

Ainsi, $v(E_1+E_2)=v(E_1)+v(E_2)$.

- On peut bien sûr itérer cela (récurrence immédiate), et cela reste vrai pour une somme d'un nombre fini quelconque de termes.
- Ainsi, puisque $E=G_1+\cdots+G_s$, et puisque la somme des images est directe, on obtient :

$$\boxed{P_j(u)(E)=\bigoplus_{i=1}^{s}P_j(u)(G_i)}.$$

- De la même manière,

$$P_j(u)(E)=\bigoplus_{i=1}^{r}P_j(u)(F_i).$$

Par ailleurs, pour tout $i\leqslant j$, $P_i\mid P_j$, donc P_j est un polynôme annulateur de u_{F_i}. On en déduit que

$$P_j(u)(F_i)=P_j(u_{F_i})(F_i)=\{0\}.$$

Ainsi,

$$\boxed{P_j(u)(E)=\bigoplus_{i=1}^{j-1}P_j(u)(F_i)}.$$

(d)
- Soit $i\in[\![1,j-1]\!]$. D'après III-1c, il existe deux bases $\mathcal{B}=(b_1,\dots,b_d)$ et $\mathcal{C}=(c_1,\dots,c_d)$ de F_i et G_i respectivement, telles que

$$\mathrm{Mat}_{\mathcal{B}}(u_{F_i})=C(P_i)=C(Q_i)=\mathrm{Mat}_{\mathcal{C}}(u_{G_i}).$$

Soit $v:F_i\to G_i$ l'application linéaire envoyant (dans le même ordre) les vecteurs de la base $\mathcal{B}$ sur les vecteurs de la base $\mathcal{C}$. Comme v envoie la base $\mathcal{B}$ sur une base, il s'agit d'un isomorphisme. En notant C_ℓ la ℓ-ième colonne de $\mathrm{Mat}_{\mathcal{C}}(u_{G_i})$, qui est aussi la ℓ-ième colonne de $\mathrm{Mat}_{\mathcal{B}}(u_{F_i})$, on a alors :

$$v^{-1}\circ u_{G_i}\circ v(b_\ell)=v^{-1}\circ u_{G_i}(c_\ell)=v^{-1}(\vec{v}_{\mathcal{C}}(C_\ell))=\vec{v}_{\mathcal{B}}(C_\ell)=u_{F_i}(b_\ell).$$

Ainsi, u_{F_i} et $v^{-1}\circ u_{G_i}\circ v$ coïncident sur les vecteurs d'une base, donc, par propriété de rigidité, $\boxed{u_{F_i}=v^{-1}\circ u_{G_i}\circ v}$

- En simplifiant les termes $v^{-1}\circ v$ intermédiaires, il vient alors, pour tout polynôme P,

$$P(u_{F_i})=v^{-1}\circ P(u_{G_i})\circ v.$$

Puisque v est un isomophisme , il vient alors :

$$\dim(P_j(u)(F_i))=\dim(P_j(u_{F_i})(F_i)=\dim(v^{-1}\circ P_j(u_{G_i})\circ v(F_i))=\dim(v^{-1}\circ P_j(u_{G_i})(G_i))=\dim(P_j(u_{G_i})(G_i)),$$

l'isomorphisme v^{-1} préservant la dimension. Ainsi, on obtient bien :

$$\boxed{\dim(P_j(u)(F_i))=\dim(P_j(u)(G_i))}.$$

(e) On a donc, d'après la question 4c,

$$\sum_{i=1}^{s}\dim(P_j(u)(G_i))=\dim P_j(u)(E)=\sum_{i=1}^{j-1}\dim(P_j(u)(G_i))=\sum_{i=1}^{j-1}\dim(P_j(u)(F_i)),$$

la dernière égalité découlant de la question précédente. Ainsi, en comparant le premier et le dernier terme, il vient :

$$\sum_{i=j}^{s}\dim(P_j(u)(G_i))=0,$$

donc, les dimensions étant positives, pour tout $i\in[\![j,s]\!]$, $\boxed{\dim(P_j(u)(G_i))=0}$.

(f) La relation précédente montre que $P_j(u)(G_j)=0$, donc que $P_j(u_{G_j})=0$. Ainsi, P_j est un polynôme annulateur de u_{G_j}. Comme son polynôme minimal est par définition Q_j, on en déduit que $Q_j\mid P_j$.
On peut dans tout cet argument (depuis 4c) inverser le rôle des P_i et Q_i. On obtient alors $P_j\mid Q_j$. Comme les deux polynômes sont unitaires on en déduit que $\boxed{P_j=Q_j}$.
Cela contredit la maximalité de la définition de j. Ainsi, l'hypothèse initiale est fausse. On en déduit que $(P_1,\dots,P_r)=(Q_1,\dots,Q_s)$ (en particulier, $r=s$). D'où $\boxed{\text{l'unicité de la suite des invariants de similitude.}}$

Partie V – Quelques applications

1. Réduction de Frobenius.

   Avec les notations précédentes, on considère pour tout $i \in [\![1, r]\!]$ une base $\mathcal{B}_i$ de F_i telle que la matrice de l'endomorphisme cyclique u_{F_i} dans cette base soit $C(P_i)$ (une telle base existe d'après la question III-1c).

   L'espace E étant la somme directe des F_i, on obtient une base $\mathcal{B}$ de E en juxtaposant (dans l'ordre) les bases $\mathcal{B}_i$. Dans cette base $\mathcal{B}$, la matrice de u est :

$$\boxed{\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix}.}$$

2. Réduction de Jordan.

   On suppose que le polynôme minimal Q_u est scindé.

   - Si u est nilpotente, alors $Q_u = X^d$ pour un certain entier d. La suite des invariants de similitude vérifie alors $P_r \mid \cdots \mid P_1 = X^d$. Donc, pour tout i, il existe d_i tel que $P_i = X^{d_i}$. On en déduit que la matrice compagnon $C(P_i)$ n'a que des coefficients nuls sur sa dernière colonne. En d'autres termes, $C(P_i)$ est la transposée d'une matrice de Jordan : la base $\mathcal{B}_i = (b_1, \ldots, b_{d_i})$ vérifie

$$u(b_1) = b_2, \ldots, u(b_{d_i - 1}) = b_{d_i}, \quad u(b_d) = 0.$$

     On définit alors la base $\mathcal{B}'_i$ sur F_i par :

$$\mathcal{B}'_i = (b_{d_1}, \ldots, b_1).$$

     La matrice de u_{F_1} dans $\mathcal{B}'$ est alors une matrice de Jordan (à diagonale nulle). La matrice de u dans la base $\mathcal{B}'$ obtenue en juxtaposant les $\mathcal{B}'_i$ est donc diagonale par blocs, les blocs diagonaux étant des matrices de Jordan à diagonale nulle. C'est bien la description attendue.

   - Dans le cas général, on factorise $Q_u = \prod_{i=1}^{m} (X - \lambda_i)^{\alpha_i}$, ce qui est possible, puisque Q_u est supposé scindé. D'après le lemme des noyaux, on a alors

$$E = \bigoplus_{i=1}^{m} \mathrm{Ker}((u - \lambda_i \mathrm{id})^{\alpha_i}).$$

     L'espace $H_i = \mathrm{Ker}((u - \lambda_i \mathrm{id})^{\alpha_i})$ est stable par u, et donc aussi par $u - \lambda_i \mathrm{id}$, et l'endomorphisme induit $u_{H_i} - \lambda_i \mathrm{id}$ est nilpotent. On peut trouver une base $\mathcal{C}_i$ de H_i dans laquelle $\mathrm{Mat}_{\mathcal{C}_i}(u_{H_i} - \lambda_i \mathrm{id})$ est diagonale par blocs, de blocs diagonaux égaux à des matrices de Jordan à diagonale nulle.

     Ainsi, $\mathrm{Mat}_{\mathcal{C}_i}(u_{H_i})$ est diagonale par blocs, de blocs diagonaux égaux à des matrices de Jordan à diagonale égale à λ_i.

   - Enfin, dans la base $\mathcal{C}$ obtenue en juxtaposant les $\mathcal{C}_i$, la matrice de u est diagonale par blocs, chaque bloc étant lui-même diagonal par blocs, avec des blocs de Jordan (de diagonale les λ_i. On obtient bien la description voulue :

$$\boxed{\mathrm{Mat}_{\mathcal{C}}(u) = \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_s \end{pmatrix}},$$

     où les J_i sont des blocs de Jordan :

$$J_i = \begin{pmatrix} \lambda_i & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \lambda_i \end{pmatrix}$$

   On peut remarquer que de plus, les λ_i sont les racines du polynôme minimal Q_u (une même racine pouvant apparaître plusieurs fois).

3. Caractérisation des classes de similitude.

   Notons u et v les endomorphismes de $\mathbb{K}^n$ canoniquement associés à A et B respectivement.

- Supposons A et B semblables. Soit $(P_1, \dots, P_r)$ la suite des invariants de similitude de A. D'après le théorème de réduction de Frobenius, il existe une base $\mathcal{B}$ de $\mathbb{K}^n$ dans laquelle la matrice de u est de la forme

$$\mathrm{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix} = M$$

(réduction de Frobenius). La matrice M est donc semblable à A, donc à B. Il existe donc une base $\mathcal{C}$ telle que

$$\mathrm{Mat}_{\mathcal{C}}(v) = M.$$

En considérant la partition de $\mathcal{C}$ en sous-familles libres $\mathcal{C}_1, \dots, \mathcal{C}_r$ correspondant aux blocs de la matrice M, et en notant $G_i = \mathrm{Vect}(\mathcal{C}_i)$, les G_i sont stables par v, et $\mathrm{Mat}_{\mathcal{C}_i}(v_{G_i}) = C(P_i)$, matrice compagnon de P_i. Alors, en notant $\mathcal{C}_i = (c_1, \dots, c_d)$,

$$(c_1, v(c_1), \dots, v^{d-1}(c_1)) = (c_1, \dots, c_d)$$

est une base de G_i. C'est donc en particulier une famille génératrice. On en déduit que

$$G_i = \mathbb{K}_{d-1}[u](c_1) \subset \mathbb{K}[u](c_1) \subset G_i,$$

où $\mathbb{K}[u](c)$ désigne tous les vecteurs obtenus en appliquant tous les polynômes en u au point c. La dernière inclusion est obtenue par stabilité. On a donc $G_i = \mathbb{K}[u](c_1)$, donc G_i est u-monogène.
La famille $(c_1, v(c_1), \dots, v^{d-1}(c_1))$ est aussi libre, Il n'existe donc pas de relation entre ces termes, ce qui implique que $\deg(Q_{v,c_1}) \geqslant d$. Mais son degré ne peut excéder la dimension de l'espace, donc $\deg(Q_{v,c_1}) = d$. De plus, $Q_{v,c_1} = Q_{v_{G_i},c_1}$, et divise donc $Q_{v_{G_i}}$, dont le degré est inférieur à d (II-4c). On en déduit que $Q_{v,c_1} = Q_{v_{G_i}}$.
Enfin, l'expression de $v(c_d)$ montre que $P_i(c_1) = 0$, donc Q_{v,c_1} divise P_1, et est unitaire de même degré. Donc $P_i = Q_{v,c_1}$.
Par conséquent, $G_1 \oplus \cdots \oplus G_r$ est une décomposition de E en sous-espaces cycliques sur lesquels les endomorphismes induits v_{G_i} sont cycliques de polynôme annulateur P_i, vérifiant bien toutes les conditions des invariants de similitude.
On en déduit que $(P_1, \dots, P_r)$ est la suite des invariants de similitude de v.
Ainsi, $\boxed{u \text{ et } v \text{ ont mêmes invariants de similitude.}}$
- Réciproquement, si u et v ont même invariants de similitude, A et B sont toutes les deux semblables à la matrice

$$\begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_r) \end{pmatrix},$$

d'après le théorème de réduction de Frobenius appliqué à u et à v. Ainsi $\boxed{A \text{ et } B \text{ sont semblables}}$.

4. Invariance de la similitude par restriction du corps de base.
Soit $\mathbb{K}$ un sous-corps d'un corps $\mathbb{L}$. Soit A et B dans $\mathcal{M}_n(\mathbb{K})$.
- Si A et B sont semblables dans $\mathcal{M}_n(\mathbb{K})$, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$. En particulier, P est aussi un élément de $\mathcal{M}_n(\mathbb{L})$, donc $\boxed{A \text{ et } B \text{ sont semblables dans } \mathcal{M}_n(\mathbb{L})}$.
- Si A et B sont semblables dans $\mathcal{M}_n(\mathbb{L})$, elles ont mêmes invariants de similitude sur $\mathbb{L}$.
Or, les invariants de similitude de matrice A sur $\mathbb{L}$ sont les mêmes que les invariants de similitude de A sur $\mathbb{K}$. En effet, d'après la preuve faite dans la question V-3, les invariants de similitude sont entièrement déterminés par les blocs d'une réduite de Frobenius. Or, une réduite de Frobenius dans $\mathcal{M}_n(\mathbb{K})$ de A est aussi une réduite de Frobenius de A dans $\mathcal{M}_n(\mathbb{L})$ (si A est semblable à une matrice de Frobenius M sur $\mathcal{M}_n(\mathbb{K})$, elle l'est aussi sur $\mathcal{M}_n(\mathbb{L})$, d'après le premier point).
Appliquant ceci aux deux matrices A et B, on en déduit que les matrices A et B ont mêmes invariants de similitude sur $\mathbb{K}$, donc $\boxed{A \text{ et } B \text{ sont semblables}}$ d'après V-3.