153. Polynômes d'endomorphismes : indications de solutions

1. a) D'après les rappels de l'énoncés, on a $\chi_u = P_1...P_r$ et $\pi_u = P_r$, mais comme tous les P_i divisent P_r, les facteurs irréductibles de χ_u sont déjà présents dans π_u. Bien entendu, la multiplicité de ces facteurs dans χ_u peut être plus grande que dans π_u.

b) Les invariants de similitude sont les mêmes pour une matrice A de $M_n(K)$ si on la regarde dans $M_n(L)$, par unicité de la suite de polynômes $P_1, ..., P_r$ de $L[X]$ vérifiant les propriétés : $P_1|...|P_r$ et A est semblable à $\mathrm{Diag}(C(P_1), ..., C(P_r))$ dans $M_n(L)$. Le résultat découle alors de ce que deux matrices de $M_n(K)$ sont semblables (dans $M_n(K)$) si et seulement si elles ont les mêmes invariants de similitude.

c) Il est facile de voir (en mettant les vecteurs de la base canonique dans l'autre sens) qu'une matrice compagnon est semblable à sa transposée. On conclut avec l'existence d'une base $\mathcal{B}$ telle que la matrice considérée soit semblable à $\mathrm{Diag}(C(P_1), ...C(P_r))$.

d) Soit J_r le bloc de Jordan de taille r. Pour tout $\lambda \in K$, la matrice $\lambda I + J_r$ est semblable à la matrice compagnon $C((X-\lambda)^r)$ car elle représente un endomorphisme cyclique de polynôme caractéristique $(X-\lambda)^r$. Par ailleurs si P et Q sont premiers entre eux, on voit que $\mathrm{Diag}(C(P), C(Q))$ a pour polynôme caractéristique et pour polynôme minimal PQ, donc est semblable à $C(PQ)$. Ainsi, à partir de la décomposition en sous-espaces cycliques, on obtient la réduction de Jordan en factorisant les polynômes $P_1, ..., P_r$, puis en regroupant les facteurs de degré 1 identiques. Par exemple la matrice $\mathrm{Diag}(C(X^2), C(X^2(X-1)^3)$ est semblable à la matrice $\mathrm{Diag}(C(X^2), C(X^2), C((X-1)^3))$, ou encore à $\mathrm{Diag}(J_2, J_2, I + J_3)$.

Ceci est tout à fait analogue au passage de l'écriture d'un groupe abélien sous la forme $\mathbf{Z}/d_1\mathbf{Z} \times ... \times \mathbf{Z}/d_r\mathbf{Z}$ en une écriture suivant les composantes p-primaires pour p premier, par exemple $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$ est isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} = (\mathbf{Z}/3\mathbf{Z})^2 \times \mathbf{Z}/2^2\mathbf{Z}$. Bien entendu, les deux cas relèvent de la théorie des modules sur les anneaux principaux, qui permet par

exemple aussi de voir que les invariants de similitude $P_1, ..., P_r$ d'une matrice A s'obtiennent en posant $B = A - XI_n \in M_n(K[X])$, puis en calculant : P_1 comme le p.g.c.d. dans $K[X]$ des coefficients de B, P_1P_2 comme le p.g.c.d. des mineurs d'ordre 2 de B, ...jusqu'à $P_1...P_r$ qui est bien le déterminant de B.

2. a) Posons $P = \pi_M$. Le polynôme P est scindé sur L, il suffit donc de montrer qu'il est à racines simples (puisqu'il annule M), ou encore que P et P' sont premiers entre eux (rappelons que le pgcd de deux polynômes de $K[X]$ reste le même dans $L[X]$). Or, comme P est irréductible, ses seuls diviseurs à une constante près sont P et 1, il suffit donc de voir que P ne divise pas P'. Or, ceci résulte de ce que P' est de degré $< \deg P$ *et* P' *est non nul* car P est non constant et on est en caractéristique zéro.

b) D'après ce qu'on a vu, il faut juste vérifier que P' est non nul. Or, en caractéristique p, un polynôme P tel que $P' = 0$ s'écrit

$$P = a_0 + a_1X^p + ... + a_rX^{pr},$$

avec les a_i dans K. Mais si K est parfait, on peut écrire $a_i = b_i^p$ avec $b_i \in K$, d'où

$$P = (b_0 + ... + b_rX^r)^p,$$

qui n'est pas irréductible.

Si par contre K est de caractéristique p et $a \in K$ n'est pas une puissance p-ième dans K, alors le polynôme $P = X^p - a$ a une dérivée nulle, donc il n'a qu'une racine b (de multiplicité p) dans toute extension L de K dans laquelle P est scindé. Pourtant P est irréductible dans $K[X]$, sinon comme il ne peut pas avoir deux facteurs irréductibles premiers entre eux (parce que sur L ces deux facteurs auraient b comme racine commune), P serait de la forme Q^p avec $Q \in K[X]$; alors a serait la puissance p-ième du terme constant de Q.

3. On sait que M est semblable à un tableau diagonal de matrices qui sont toutes de la forme $\lambda I + N$ avec N nilpotente et $\lambda \neq 0$ (vu que M est supposée inversible). On se ramène donc à M de cette forme. On peut aussi supposer $\lambda = 1$ en observant que $\lambda I + N = \lambda(I + \frac{N}{\lambda})$, avec $\frac{N}{\lambda}$ nilpotente et λ de la forme $\mu^k, \mu \in \mathbf{C}$ (car $\mathbf{C}$ est algébriquement clos).

Maintenant, on écrit le DSE de $(1 + x)^{1/k}$, ce qui donne une série entière $\sum_{n\geq 0} a_nx^n$ (avec $a_n \in \mathbf{Q}$) vérifiant

$$(\sum_{n\geq 0} a_nx^n)^k = 1 + x$$

pour tout x réel avec $|x| < 1$. Soit alors F la série formelle de $\mathbf{C}[[X]]$ définie par $F = \sum_{n\geq 0} a_n x^n$. Comme le produit de Cauchy de deux séries entières s'obtient en faisant le produit des séries formelles correspondantes, l'unicité du DSE montre que la série formelle F^k est égale à la série formelle $1 + X$ (en effet les séries entières correspondantes coïncident au voisinage de 0). En particulier $F(N)^k = I + N$ en substituant la matrice N dans chaque série formelle, ce qui est licite puisque comme N est nilpotente, on obtient bien des séries convergentes. Ainsi $F(N)$ est solution du problème cherché. Le même type d'argument (en utilisant la série de $\ln(1 + x)$) donne qu'il existe une matrice A telle que $\exp A = I + N$. Noter par contre que si par exemple A est une matrice $(2, 2)$ nilpotente non nulle, elle ne s'écrit pas $A = B^2$, sinon B serait aussi nilpotente et on aurait $B^2 = 0$. L'hypothèse M inversible était donc importante dans cet exercice.

Pour des rappels sur les séries formelles, on pourra consulter la section 7.4. du tome 1 (algèbre) du *Cours de mathématiques spéciales* de Ramis, Deschamps et Odoux.

4. a) Supposons par l'absurde que $P = \pi_u$ s'écrive $P = P_1^r Q$ avec $r \geq 2$, P_1 irréductible et Q premier avec P. Alors le sous-espace $F = \ker(P_1(u))$ est stable par u, montrons qu'il n'a pas de supplémentaire G stable. Si G existait, la restriction de $P_1(u)$ à G serait inversible vu que $F \cap G = \{0\}$. Le polynôme minimal R de la restriction de u à G ne serait donc pas divisible par P_1, et comme $(P_1 R)(u) = 0$ (vu que $P_1(u)R(u)$ s'annule sur F et G), ceci contredirait le fait que le polynôme minimal de P est divisible par P_1^r.

b) Soit F un sous-espace stable par u. On applique le lemme des noyaux à E et F, ce qui donne

$$E = \bigoplus \ker P_i(u);\ F = \bigoplus (\ker P_i(u) \cap F).$$

Si on sait traiter le cas où le polynôme minimal est irréductible, il suffit alors de l'appliquer à chaque $(\ker P_i(u) \cap F) \subset \ker P_i(u)$, puisque le polynôme minimal de la restriction de u à $\ker P_i(u)$ est P_i. On prend ensuite la somme directe des supplémentaires stables de chaque $(\ker P_i(u) \cap F)$ dans $\ker P_i(u)$.

c) Comme $x \notin F$, l'idéal I ne contient pas 1. Soit Q le générateur unitaire de I; comme $P_1(u) = 0$, le polynôme Q divise P_1 et comme P_1 est irréductible on obtient $Q = P_1$. Ainsi, on a $P(u)(x) \in F \Rightarrow P(u) = 0$, ce qui donne que $F \cap G = \{0\}$ comme on voulait.

d) On conclut par récurrence sur $\dim F$, car $F \oplus G$ est de dimension $> \dim F$ et G est stable par u.

e) D'après ce qu'on vient de voir, ce sont ceux dont le polynôme minimal est scindé à racines simples, donc les endomorphismes diagonalisables.

f) En caractéristique 0, chaque facteur irréductible de π_u reste à racines simples dans L (cf. exercice 2), donc M semi-simple est équivalent à M diagonalisable dans $M_n(L)$. Cela reste vrai sur un corps parfait de caractéristique $p > 0$, mais pas sur un corps imparfait d'après ce qu'on a vu dans l'exercice 2 : dans ce cas l'implication "diagonalisable dans $M_n(L)$ implique semi-simple" reste vraie mais pas la réciproque.