154. Sous-espaces stables : Indications de solutions

1. a) C'est une question assez classique, mais dont il faut formuler la réponse précisément, un argument vague du genre "les invariants de similitude sont les mêmes" étant insuffisant. On observe d'abord que pour toute matrice A de $M_n(K)$ d'invariants de similitude $(P_1, ..., P_r)$, la matrice A est semblable sur $M_n(K)$ à $\text{Diag}(C(P_1), ..., C(P_r))$ via le théorème de réduction de Frobenius. A fortiori, A est semblable sur $M_n(L)$ à $\text{Diag}(C(P_1), ..., C(P_r))$, ce qui montre que ses invariants de similitude en tant que matrice de $M_n(L)$ restent $(P_1, ..., P_r)$. On peut alors dire que si A et B sont semblables sur $M_n(L)$, leurs invariants de similitude en tant que matrices de $M_n(K)$ sont les mêmes (puisque ces invariants ne changent pas par passage de $M_n(K)$ à $M_n(L)$), et elles sont donc bien semblables dans $M_n(K)$.

Si on connaît ici la théorie des modules sur un anneau principal (en l'occurrence $K[X]$), on peut aussi dire que le polynôme $P_1....P_i$ pour $1 \leq i \leq r$ se calcule en prenant le pgcd dans $K[X]$ des mineurs d'ordre i de la matrice $A - XI$, ce qui permet de retrouver que les invariants de similitude ne changent pas par extension du corps de base.

b) Via la réduction de Frobenius, il suffit de le faire pour une matrice compagnon $C(P)$. Or, la transposée de $C(P)$ garde pour polynôme minimal et polynôme caractéristique P, ce qui montre (toujours d'après la réduction de Frobenius) qu'elle est semblable à $C(P)$.

Une autre méthode consiste à observer qu'un bloc de Jordan J est semblable à ${}^tJ$ (considérer le changement de base de la base canonique $(e_1, ..., e_n)$ à la base $(e_n, ..., e_1)$), ce qui permet via la réduction de Jordan de voir qu'une matrice dont le polynôme caractéristique est scindé est semblable à sa transposée. On conclut alors avec a) en prenant pour L le corps de décomposition de ce polynôme caractéristique.

c) C'est une conséquence immédiate de ce que dans une certaine base, la matrice de u s'écrit $\text{Diag}(C(P_1), ..., C(P_r))$ avec $P_1 | P_2 ... | P_r$. En effet, on a alors $\pi_u = P_r$ et $\chi_u = P_1 ... P_r$.

d) On observe que le commutant d'une matrice compagnon A de taille d est de dimension d (c'est l'espace des polynômes en A). Toute matrice M est semblable à une matrice diagonale par blocs du type $\mathrm{Diag}(C(P_1), ..., C(P_r))$, chaque bloc étant une matrice compagnon de taille d_i (avec $\sum d_i = n$). Le commutant d'une telle matrice contient au moins les matrices diagonales par blocs $\mathrm{Diag}(M_1, ..., M_r)$ où chaque M_i est dans le commutant de $C(P_i)$. Ainsi la dimension du commutant de M est au moins $\sum d_i = n$.

e) 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 $C(PQ)$ (on peut aussi utiliser le lemme des noyaux). 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

2. Soit $(.,.)$ un produit scalaire quelconque sur V. Il suffit alors de poser

$$\langle x, y \rangle := \sum_{s \in G} (\rho_s(x), \rho_s(y)).$$

Maintenant, si W est un sous-espace de V stable par ρ, l'orthogonal de W pour le nouveau produit scalaire $\langle , \rangle$ est aussi stable, puisque tous les endomorphismes $\rho_g, g \in G$ sont alors des isométries pour ce produit scalaire. On termine alors comme dans le cours sur les représentations.

3. Soient $E_1, ..., E_r$ les espaces propres de u. Si F est stable par u, alors comme la restriction de u à F est diagonalisable, on a

$$F = \bigoplus (E_i \cap F),$$

puisque le sous-espace propre de cette restriction associé à une valeur propre λ est $E(\lambda) \cap F$, où $E(\lambda)$ est le sous-espace propre de u associé à λ. Ainsi F est somme directe de sous-espaces des espaces propres $E_1, ..., E_r$; réciproquement une somme directe de sous-espaces des E_i est clairement stable par u.

4. Comme A a trois valeurs propres distinctes 2, 9, et 5, elle est semblable à $B := \mathrm{Diag}(2,9,5)$. Pour P inversible, l'application $X \mapsto PXP^{-1}$ est un automorphisme de l'algèbre $M_n(K)$, ce qui permet de ramener la question à l'équation $X^2 = B$. Une telle X commute avec B, donc laisse stable ses sous-espaces propres, donc est elle-même diagonale, ce qui donne $X = \mathrm{Diag}(\pm\sqrt{2}, \pm 3, \pm\sqrt{5})$. Réciproquement, ces X conviennent. Il y a donc 8 solutions.

5. 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 $(P_1R)(u) = 0$ (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.

Noter que si K est de caractéristique 0, chaque facteur irréductible de π_u reste à racines simples dans toute extension L de K (exercice classique), donc u semi-simple est équivalent à $M := \mathrm{Mat}(u)$ diagonalisable dans $M_n(L)$, où L est tel que le polynôme caractéristique de u soit scindé sur L. Cela reste vrai sur un corps parfait de caractéristique $p > 0$, mais pas sur un corps imparfait (prendre la matrice compagnon du polynôme $X^p - T$ sur le corps $K = \mathbf{Z}/p\mathbf{Z}(T)$). Dans ce cas l'implication "diagonalisable dans $M_n(L)$ implique semi-simple" reste vraie mais pas la réciproque.