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 $\mathrm{Diag}(C(P_1), ..., C(P_r))$ via le théorème de réduction de Frobenius. A fortiori, A est semblable sur $M_n(L)$ à $\mathrm{Diag}(C(P_1), ..., C(P_r))$, 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) 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 $\sum d_i = n$.

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 $C(PQ)$ (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

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

f) Si u a un espace stable autre que $\{0\}$ et E, il est immédiat (par exemple en écrivant la matrice par blocs de u) que le polynôme caractéristique P n'est pas irréductible. Supposons réciproquement que u n'ait pas de sous-espaces stables non triviaux. La réduction de Frobenius donne alors immédiatement que u est cyclique, de matrice $C(P)$ dans une certaine base. On a vu en d) que si $P = QR$ avec Q et R deux à deux premiers entre eux, alors $C(P)$ est semblable à $\mathrm{Diag}(C(Q), C(R))$, ce qui montre que P ne peut pas avoir deux facteurs irréductibles distincts, sinon il y aurait un sous-espace stable non trivial pour u. Reste à écarter le cas où $P = Q^r$ avec Q irréductible et $r \geq 2$, mais dans ce cas $\ker(Q(u))$ est un sous-espace stable non trivial puisque $Q(u)$ est non inversible (vu que $P(u) = 0$) et distinct de E (puisque $Q(u) \neq 0$, le minimal de u étant Q^r).

2. Il suffit de prendre une matrice compagnon $C(P)$, avec P irréductible mais tel que P acquiert des racines multiples sur son corps de décomposition L, vu que P est le minimal de $C(P)$. Ici $P = X^2 - T$ convient : en effet $P' = 0$ (donc sur L, P a une racine double) mais P est irréductible vu qu'il est de degré 2 sans racine dans K (un élément de $\mathbf{Z}/2\mathbf{Z}(T)$ qui est un

carré est de degré pair). Ce phénomène ne peut se produire que si on a des polynômes irréductibles P (donc non constants) qui vérifient $P' = 0$, il ne se rencontre donc pas en caractéristique zéro, ni même sur un corps parfait de caractéristique $p > 0$ car un tel polynôme s'écrirait

$$P = a_0 + a_1 X^p + ... + a_n X^{np},$$

avec chaque a_i de la forme $a_i = \alpha_i^p$, $\alpha_i \in K$ (le corps K étant parfait), d'où $P = (\alpha_0 + ... + \alpha_n X^n)^p$ ne peut pas être irréductible.

3. 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.

4. 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.

5. 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.