Corrigé de l'épreuve de Mathématiques A
Concours X-ENS 2025 (Filières MP-MPI)

1. Soit h un endomorphisme diagonalisable de V. Son polynôme minimal, noté π_h, est donc scindé à racines simples sur $\mathbb{C}$. Soit W un sous-espace vectoriel de V stable par h. Notons $h_W \in \mathcal{L}(W)$ l'endomorphisme induit. Pour tout vecteur $x \in W$, on a $h_W(x) = h(x)$. Par récurrence immédiate, pour tout entier $k \geq 0$, on a $(h_W)^k(x) = h^k(x)$. Par linéarité, pour tout polynôme $P \in \mathbb{C}[X]$, on a $P(h_W)(x) = P(h)(x)$. En particulier, puisque π_h annule h, on a $\pi_h(h_W)(x) = \pi_h(h)(x) = 0_V$ pour tout $x \in W$. Le polynôme π_h est donc un polynôme annulateur de h_W. Le polynôme minimal de h_W, noté π_{h_W}, divise par conséquent π_h. Puisque π_h est scindé à racines simples sur $\mathbb{C}$, ses diviseurs le sont également. π_{h_W} est donc scindé à racines simples, ce qui prouve que h_W est diagonalisable.

2.a) Soient M et M' deux matrices semblables de $\mathcal{M}_n(\mathbb{C})$. Il existe $P \in GL_n(\mathbb{C})$ telle que $M = PM'P^{-1}$. Pour tout entier $k \in \mathbb{N}$, on a $M^k = P(M')^kP^{-1}$. Les matrices M^k et $(M')^k$ étant équivalentes (et même semblables), elles ont le même rang. D'après le théorème du rang, elles ont donc la même dimension de noyau : $\dim\ker M^k = \dim\ker(M')^k$. La quantité $\delta_k(M)$ n'étant calculée qu'à partir de combinaisons linéaires des dimensions des noyaux des puissances de M, on a de manière immédiate $\delta_k(M) = \delta_k(M')$ pour tout entier $k \geq 1$.

2.b) Considérons l'endomorphisme u canoniquement associé à la matrice de Jordan J_r de taille $r \times r$ dans la base canonique $(e_1, \dots, e_r)$. L'action de u est : $u(e_i) = e_{i-1}$ pour $i \geq 2$, et $u(e_1) = 0$. Par itération, pour un entier $j \geq 1$, $\ker u^j = \mathrm{Vect}(e_1, \dots, e_{\min(j,r)})$. Ainsi, $\dim\ker J_r^j = \min(j, r)$. Calculons $\delta_k(J_r) = -\min(k-1, r) + 2\min(k, r) - \min(k+1, r)$:

— Si $k < r$, alors $k + 1 \leq r$. $\delta_k(J_r) = -(k-1) + 2k - (k+1) = 0$.

— Si $k = r$, alors $k - 1 = r - 1$, $k = r$, et $k + 1 > r$. $\delta_r(J_r) = -(r-1) + 2r - r = 1$.

— Si $k > r$, alors $k - 1 \geq r$. $\delta_k(J_r) = -r + 2r - r = 0$.

On a bien $\delta_k(J_r) = 1$ si $k = r$ et 0 sinon.

2.c) Soit $M = \mathrm{diag}(M_1, M_2)$. Pour un vecteur colonne bloc $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$, le calcul donne $MX = \begin{pmatrix} M_1X_1 \\ M_2X_2 \end{pmatrix}$. Ainsi, $MX = 0 \iff M_1X_1 = 0$ et $M_2X_2 = 0$. L'application qui à $X \in \ker M$ associe $(X_1, X_2) \in \ker M_1 \times \ker M_2$ est un isomorphisme. On en déduit que $\dim\ker M = \dim\ker M_1 + \dim\ker M_2$. Pour tout entier $j \in \mathbb{N}$, le produit par blocs donne $M^j = \mathrm{diag}(M_1^j, M_2^j)$, donc la relation précédente se généralise : $\dim\ker M^j = \dim\ker M_1^j + \dim\ker M_2^j$. En utilisant la linéarité de la combinaison définissant δ_k, on obtient :

$$\delta_k(M) = -(\dim\ker M_1^{k-1} + \dim\ker M_2^{k-1}) + 2(\dim\ker M_1^k + \dim\ker M_2^k) - (\dim\ker M_1^{k+1} + \dim\ker M_2^{k+1})$$

ce qui se regroupe en $\delta_k(M) = \delta_k(M_1) + \delta_k(M_2)$.

3.a) Tout élément $F \in \mathbb{C}[X^{\pm 1}]$ se décompose de manière unique sous la forme $F = D + P$ avec $D \in \mathcal{D}$ et $P \in \mathbb{C}[X]$. Par définition, $\Pi(F) = D$. On calcule le terme de gauche : $\xi(\Pi(F)) = \xi(D) = \hat{\xi}(D) = \Pi(XD)$. On calcule le terme de droite : $\hat{\xi}(F) = \Pi(XF) = \Pi(XD + XP)$. Or, comme $P \in \mathbb{C}[X]$, on a $XP \in \mathbb{C}[X]$. La projection de la partie polynomiale sur $\mathcal{D}$ étant nulle, $\Pi(XP) = 0$. Ainsi, $\Pi(XD + XP) = \Pi(XD)$. On conclut que $\xi(\Pi(F)) = \hat{\xi}(F)$.

3.b) Montrons par récurrence sur $k \in \mathbb{N}$ que $\xi^k(F) = \Pi(X^k F)$ pour tout $F \in \mathcal{D}$.

- Pour $k = 0$: $\xi^0(F) = F$. Puisque $F \in \mathcal{D}$, $\Pi(F) = F$. L'égalité est vraie.
- Supposons l'égalité vraie au rang k. $\xi^{k+1}(F) = \xi(\xi^k(F)) = \xi(\Pi(X^k F))$ d'après l'hypothèse de récurrence. En appliquant le résultat de la question 3.a) avec le polynôme de Laurent $X^k F$, on obtient : $\xi(\Pi(X^k F)) = \hat{\xi}(X^k F) = \Pi(X \cdot X^k F) = \Pi(X^{k+1} F)$. La propriété est donc héréditaire.

Ainsi, pour tout monôme X^k, on a $X^k(\xi)(F) = \Pi(X^k F)$. Par linéarité de Π et de l'évaluation polynomiale d'un endomorphisme, on a, pour tout $P \in \mathbb{C}[X]$, $P(\xi)(F) = \Pi(P \cdot F)$.

4. Soit $F \in \mathcal{D}$. Il s'écrit $F = \sum_{j=1}^{p} f_{-j} X^{-j}$. D'après 3.b), on a :

$$F \in \ker \xi^n \iff \Pi(X^n F) = 0 \iff X^n F \in \mathbb{C}[X]$$

Le produit vaut $X^n F = \sum_{j=1}^{p} f_{-j} X^{n-j}$. Pour que cette somme soit un polynôme usuel, il faut et il suffit que toutes les puissances soient positives ou nulles, c'est-à-dire que $n - j \geq 0$, soit $j \leq n$ pour tous les indices où $f_{-j} \neq 0$. Ainsi, $F \in \ker \xi^n \iff F = \sum_{j=1}^{n} f_{-j} X^{-j}$. Une base du noyau de ξ^n est donc la famille $(X^{-1}, X^{-2}, \ldots, X^{-n})$.

Pour démontrer la surjectivité, soit $G \in \mathcal{D}$. On cherche un antécédent $F \in \mathcal{D}$. Posons $F = X^{-n} G$. Puisque G ne possède que des monômes de degrés strictement négatifs, les multiplier par X^{-n} donne des monômes de degrés strictement inférieurs à $-n$. F appartient donc bien à $\mathcal{D}$. On calcule son image : $\xi^n(F) = \Pi(X^n F) = \Pi(X^n X^{-n} G) = \Pi(G)$. Puisque $G \in \mathcal{D}$, $\Pi(G) = G$. Donc ξ^n est surjectif.

5. Le plus petit sous-espace $\mathcal{D}_r$ contenant X^{-r} et stable par ξ est l'espace engendré par les images successives : $\mathrm{Vect}(\xi^k(X^{-r}))_{k \in \mathbb{N}}$. Or, d'après 3.b), $\xi^k(X^{-r}) = \Pi(X^{k-r})$.

- Si $0 \leq k \leq r - 1$, l'exposant $k - r$ est ≤ -1. Donc $X^{k-r} \in \mathcal{D}$, et $\Pi(X^{k-r}) = X^{k-r}$.
- Si $k \geq r$, l'exposant $k - r \geq 0$, donc $X^{k-r} \in \mathbb{C}[X]$. Sa projection est nulle : $\Pi(X^{k-r}) = 0$.

L'espace $\mathcal{D}_r$ est donc engendré par la famille $(X^{k-r})_{0 \leq k \leq r-1}$, c'est-à-dire $(X^{-r}, X^{-r+1}, \ldots, X^{-1})$. Les monômes étant de degrés distincts, cette famille génératrice est libre, c'est une base de $\mathcal{D}_r$. Notons les vecteurs de cette base $e_{k+1} = X^{-r+k}$ pour $0 \leq k \leq r - 1$. On a $\xi(e_i) = \xi(X^{-r+i-1}) = X^{-r+i} = e_{i+1}$ pour $1 \leq i \leq r - 1$. Et pour le dernier vecteur, $\xi(e_r) = \xi(X^{-1}) = \Pi(1) = 0$. Dans la base $(e_1, \ldots, e_r)$, l'image du i-ème vecteur est le $(i + 1)$-ème. La matrice associée est celle qui a des 1 sur la première sous-diagonale et des 0 ailleurs. C'est exactement le bloc de Jordan J_r.

6.a) On vérifie que $\mathcal{J}$ est un idéal de $\mathbb{C}[X]$:

- $\mathcal{J}$ est non vide car le polynôme nul 0 vérifie $0(u)(v) = 0_V \in W$.
- Si $P, Q \in \mathcal{J}$, $(P + Q)(u)(v) = P(u)(v) + Q(u)(v)$. Comme W est un espace vectoriel, cette somme appartient à W.
- Si $P \in \mathcal{J}$ et $A \in \mathbb{C}[X]$, $(AP)(u)(v) = A(u)(P(u)(v))$. Posons $w = P(u)(v) \in W$. Comme W est stable par u, il est stable par tout polynôme en u. Donc $A(u)(w) \in W$. On a bien $AP \in \mathcal{J}$.

6.b) u est nilpotent sur V (de dimension finie). Il existe donc $N \in \mathbb{N}^*$ tel que $u^N = 0$. On a alors $u^N(v) = 0_V \in W$, ce qui prouve que $X^N \in \mathcal{J}$. L'anneau $\mathbb{C}[X]$ étant principal et $\mathcal{J}$ un idéal non réduit à $\{0\}$, $\mathcal{J}$ est engendré par un unique polynôme unitaire P_0. Or $X^N \in \mathcal{J}$, donc P_0 divise X^N. P_0 est nécessairement de la forme X^r pour un certain entier naturel r. (On peut noter que $r \geq 1$ car $v \notin W$, donc $1 \notin \mathcal{J}$).

6.c) $W' = \{P(u)(v) + w \mid P \in \mathbb{C}[X], w \in W\}$. En prenant $P = 0$, on obtient que W' contient W. En prenant $P = 1$ et $w = 0$, on voit que $v \in W'$. Montrons la stabilité par u : soit $x = P(u)(v) + w \in W'$.

$$u(x) = u(P(u)(v)) + u(w) = (XP)(u)(v) + u(w)$$

Comme $XP \in \mathbb{C}[X]$ et que $u(w) \in W$ (car W est stable par u), $u(x)$ s'écrit bien sous la forme demandée, donc $u(x) \in W'$. W' est stable par u.

6.d) On a défini $G_v = \varphi(u^r(v))$. Par définition, φ arrive dans $\mathcal{D}$, donc $G_v \in \mathcal{D}$. D'après la question 4, l'endomorphisme ξ^r de $\mathcal{D}$ est surjectif. Il existe donc au moins un élément $F_v \in \mathcal{D}$ tel que $\xi^r(F_v) = G_v$.

6.e) Si $P(u)(v) = w \in W$, cela signifie que $P \in \mathcal{J}$. L'idéal $\mathcal{J}$ étant engendré par X^r, P est un multiple de X^r : il existe $A \in \mathbb{C}[X]$ tel que $P = AX^r$. On calcule alors $P(\xi)(F_v) = (AX^r)(\xi)(F_v) = A(\xi)(\xi^r(F_v)) = A(\xi)(G_v) = A(\xi)(\varphi(u^r(v)))$. L'hypothèse $\xi \circ \varphi = \varphi \circ u_W$ implique par itération que pour tout polynôme A, $A(\xi) \circ \varphi = \varphi \circ A(u_W)$. Donc $P(\xi)(F_v) = \varphi(A(u)(u^r(v))) = \varphi((AX^r)(u)(v)) = \varphi(P(u)(v)) = \varphi(w)$.

6.f) Pour montrer que $\varphi'(x)$ est bien défini, supposons que x admette deux décompositions : $x = P_1(u)(v) + w_1 = P_2(u)(v) + w_2$. Alors $(P_1 - P_2)(u)(v) = w_2 - w_1 \in W$. D'après la question 6.e) appliquée au polynôme $P_1 - P_2$, on a $(P_1 - P_2)(\xi)(F_v) = \varphi(w_2 - w_1)$. Par linéarité, $P_1(\xi)(F_v) - P_2(\xi)(F_v) = \varphi(w_2) - \varphi(w_1)$, ce qui donne $P_1(\xi)(F_v) + \varphi(w_1) = P_2(\xi)(F_v) + \varphi(w_2)$. L'image ne dépend donc pas du choix de P et w.

Vérifions que c'est un prolongement compatible :

— Si $x \in W$, on prend $P = 0$ et $w = x$. $\varphi'(x) = 0 + \varphi(x) = \varphi(x)$. Donc φ' prolonge bien φ.

— Pour la compatibilité, $\xi(\varphi'(x)) = \xi(P(\xi)(F_v) + \varphi(w)) = (XP)(\xi)(F_v) + \xi(\varphi(w))$. Grâce à la relation de compatibilité sur W, on a $\xi(\varphi(w)) = \varphi(u(w))$. D'autre part, $u(x) = u(P(u)(v) + w) = (XP)(u)(v) + u(w)$. En appliquant la définition de φ' à $u(x)$ (avec le polynôme XP et le vecteur $u(w) \in W$), on obtient $\varphi'(u(x)) = (XP)(\xi)(F_v) + \varphi(u(w))$. On a donc bien $\xi(\varphi'(x)) = \varphi'(u(x))$, ce qui montre que $\xi \circ \varphi' = \varphi' \circ u_{W'}$.

7. On procède par un argument de dimension. Si $W = V$, φ est déjà le prolongement cherché. Sinon, on peut choisir $v \in V \setminus W$ et construire un espace W_1 strictement plus grand que W, sur lequel φ se prolonge en φ_1 compatible avec u. Si $W_1 \neq V$, on recommence. La dimension de l'espace construit augmente strictement à chaque étape. V étant de dimension finie, cette procédure s'arrête au bout d'un nombre fini d'étapes (au plus $\dim V - \dim W$). L'application finale obtenue sur V est un prolongement de φ compatible avec u.

8.a) Considérons une combinaison linéaire nulle : $\sum_{k=0}^{n-1} \lambda_k u^k(v_0) = 0$. Appliquons u^{n-1} à cette égalité. Pour tout $k \geq 1$, $u^{n-1}(u^k(v_0)) = u^{n-1+k}(v_0) = 0$ car $n - 1 + k \geq n$ et $u^n = 0$. Il ne reste que $\lambda_0 u^{n-1}(v_0) = 0$. Or on a supposé $u^{n-1}(v_0) \neq 0$, donc $\lambda_0 = 0$. Par récurrence finie, en appliquant u^{n-2}, puis u^{n-3}, etc., on montre que tous les λ_k sont nuls. La famille est donc libre. Le sous-espace W engendré contient v_0 (pour $k = 0$). Il est stable par u car $u(u^k(v_0)) = u^{k+1}(v_0) \in W$ pour $k \leq n-2$, et $u(u^{n-1}(v_0)) = 0 \in W$. En ordonnant la base selon $\mathcal{B}_W = (u^{n-1}(v_0), u^{n-2}(v_0), \ldots, u(v_0), v_0)$, l'image du j-ème vecteur par u_W est le $(j-1)$-ème (avec 0 pour le premier). La matrice de u_W dans cette base est le bloc de Jordan J_n.

8.b) On définit $\varphi : W \to \mathcal{D}$ en imposant les images des vecteurs de base : $\varphi(u^{n-1-k}(v_0)) = X^{-k-1}$ pour $0 \leq k \leq n-1$ (autrement dit, l'image du monôme $u^j(v_0)$ est X^{j-n}). Cette application transforme une base de W en la famille libre $(X^{-n}, \ldots, X^{-1})$ de $\mathcal{D}$, elle est donc injective. On vérifie la compatibilité pour tout $j \in \{0, \ldots, n-2\}$: $\xi(\varphi(u^j(v_0))) = \xi(X^{j-n}) = X^{j+1-n} = \varphi(u^{j+1}(v_0))$. Et pour $j = n-1$: $\xi(\varphi(u^{n-1}(v_0))) = \xi(X^{-1}) = \Pi(1) = 0 = \varphi(u^n(v_0))$. Par linéarité, $\xi \circ \varphi = \varphi \circ u_W$.

8.c) Soit $\psi : V \to \mathcal{D}$ ce prolongement. On a $\xi \circ \psi = \psi \circ u$. Par récurrence immédiate, $\xi^n \circ \psi = \psi \circ u^n$. Or $u^n = 0$, donc $\xi^n \circ \psi = 0$. Ceci implique que pour tout vecteur $x \in V$, $\xi^n(\psi(x)) = 0$. L'image de ψ est donc contenue dans $\ker \xi^n$.

8.d) Par construction de φ, on a $\operatorname{Im} \varphi = \operatorname{Vect}(X^{-1}, \ldots, X^{-n}) = \ker \xi^n$. Puisque ψ prolonge φ, l'application ψ considérée comme allant de V dans $\ker \xi^n$ est surjective (son image contient au moins l'image de φ). D'après le théorème du rang, $\dim V = \dim \ker \psi + \dim \operatorname{Im} \psi = \dim \ker \psi + \dim(\ker \xi^n)$. Or $\dim(\ker \xi^n) = n = \dim W$, donc $\dim V = \dim \ker \psi + \dim W$. De plus, si $x \in W \cap \ker \psi$, alors $\psi(x) = 0$, donc $\varphi(x) = 0$. Comme φ est injective sur W, $x = 0$. La somme est donc directe : $V = W \oplus \ker \psi$. Enfin, si $x \in \ker \psi$, $\psi(u(x)) = \xi(\psi(x)) = \xi(0) = 0$, donc $u(x) \in \ker \psi$. Le supplémentaire est bien stable par u.

9. On procède par récurrence sur la dimension de l'espace. Si $\dim V = 1$, alors $u = 0$, et sa matrice est J_1. Le résultat est vrai. Supposons le résultat vrai pour tout espace de dimension strictement inférieure à $\dim V$. Soit u nilpotent. Si $u = 0$, la matrice est nulle, c'est une matrice diagonale par blocs formés de J_1. Si $u \neq 0$, notons n son indice de nilpotence. D'après la question 8, on peut décomposer $V = W \oplus \ker \psi$, où W est cyclique de dimension n avec u_W de matrice J_n, et $S = \ker \psi$ est stable par u. L'espace S étant de dimension $\dim V - n < \dim V$, l'hypothèse de récurrence s'applique à l'endomorphisme induit u_S. Il existe donc une base de S dans laquelle la matrice de u_S est diagonale par blocs de Jordan. La réunion de la base de W et de la base de S forme une base de V dans laquelle la matrice de u est diagonale par blocs de Jordan. Quitte à permuter les blocs de la base (ce qui revient à réordonner les sous-espaces), on peut classer les blocs de manière décroissante de tailles $r_1 \geq r_2 \geq \cdots \geq r_s$.

10. Soit M la matrice de u diagonale par blocs avec pour blocs $J_{r_1}, \ldots, J_{r_s}$. D'après la question 2.c), on a pour tout $k \geq 1$, $\delta_k(u) = \sum_{i=1}^{s} \delta_k(J_{r_i})$. D'après la question 2.b), $\delta_k(J_{r_i})$ vaut 1 si $r_i = k$ et 0 sinon. Par conséquent, la somme vaut exactement le nombre de blocs de Jordan de taille k. Or, les quantités $\delta_k(u)$ sont des invariants de l'endomorphisme u qui ne dépendent que des dimensions des noyaux de ses itérés (question 2.a). Le nombre de blocs de taille k est donc une constante fixée par u indépendamment du choix de la base. Les tailles et leur multiplicité (donc le nombre total s) sont uniques.

11.a) L'endomorphisme h vérifie $h^N - \mathrm{id}_V = 0$. Le polynôme $X^N - 1$ est donc un polynôme annulateur de h. Or, dans $\mathbb{C}[X]$, ce polynôme est scindé à racines simples (ses racines sont les racines N-ièmes de l'unité). Puisque h est annulé par un polynôme scindé à racines simples, h est diagonalisable.

11.b) Soit $x \in V_j = \ker(h - \zeta^j \,\mathrm{id}_V)$. Par définition, $h(x) = \zeta^j x$. Calculons l'image de $u(x)$ par h. L'égalité $h \circ u \circ h^{-1} = \zeta u$ s'écrit aussi $h \circ u = \zeta u \circ h$. Donc $h(u(x)) = \zeta u(h(x)) = \zeta u(\zeta^j x) = \zeta^{j+1} u(x)$. Le vecteur $u(x)$ est donc un vecteur propre de h pour la valeur propre ζ^{j+1} (ou le vecteur nul). Dans tous les cas, $u(x) \in V_{j+1}$. (La cyclicité est assurée par le fait que $\zeta^N = 1$, donc $V_N = V_0$).

11.c) Par hypothèse, $h \circ u \circ h^{-1} = \zeta u$. Par récurrence sur $k \in \mathbb{N}$, on montre que $h^k \circ u \circ h^{-k} = \zeta^k u$. (Pour $k = 0$, $u = u$. Hérédité : $h^{k+1} u h^{-k-1} = h(h^k u h^{-k}) h^{-1} = h(\zeta^k u) h^{-1} = \zeta^k (h u h^{-1}) = \zeta^{k+1} u$). Pour $k < 0$, on pose $k' = -k > 0$, l'inversion de la relation donne le même résultat. Donc $h^k \circ u \circ h^{-k} = \zeta^k u$ pour tout $k \in \mathbb{Z}$. Pour l'itération de u : on a $h \circ u^l \circ h^{-1} = (h \circ u \circ h^{-1})^l = (\zeta u)^l = \zeta^l u^l$.

12.a) Puisque W et W' sont tous deux stables par u, pour tout vecteur $x = x_W + x_{W'}$ avec $x_W \in W$ et $x_{W'} \in W'$, on a $u(x) = u(x_W) + u(x_{W'})$. Comme $u(x_W) \in W$ et $u(x_{W'}) \in W'$, la composante de $u(x)$ sur W est précisément $u(x_W)$. Donc $p(u(x)) = u(x_W) = u(p(x))$. Ainsi, u et p commutent.

12.b) Pour tout $x \in V$, $p(h^{-k}(x)) \in W$ car p projette sur W. Puisque W est stable par h (et donc par ses puissances), $h^k(p(h^{-k}(x))) \in W$. La moyenne de ces termes appartient donc à W, ce qui montre que $\mathrm{Im}(\overline{p}) \subset W$. Si $w \in W$, comme W est stable par h et dimension finie, il est stable par h^{-1}. Donc $h^{-k}(w) \in W$. Sa projection par p est lui-même : $p(h^{-k}(w)) = h^{-k}(w)$. Puis on applique h^k, ce qui donne $h^k(h^{-k}(w)) = w$. On somme N fois le vecteur w et on divise par N, d'où $\overline{p}(w) = w$.

12.c) D'après 12.b), pour tout $x \in V$, $\overline{p}(x) \in W$. Si on réapplique $\overline{p}$, on se trouve dans le cas du second point de 12.b) : $\overline{p}(\overline{p}(x)) = \overline{p}(x)$. L'endomorphisme $\overline{p}$ vérifie donc $\overline{p} \circ \overline{p} = \overline{p}$, c'est un projecteur. Puisque $\overline{p}(x) \in W$ et que pour tout $w \in W, \overline{p}(w) = w$, l'image de ce projecteur est exactement W.

12.d) Pour la commutation avec h : $h \circ \overline{p} \circ h^{-1} = \frac{1}{N} \sum_{k=0}^{N-1} h^{k+1} \circ p \circ h^{-k-1}$. En effectuant le changement d'indice $j = k + 1$, la somme s'étend de $j = 1$ à N. Or $h^N = \mathrm{id}_V$ et $h^0 = \mathrm{id}_V$, les termes extrêmes se raccordent, et on retrouve exactement la somme définissant $\overline{p}$. Ainsi $h \circ \overline{p} \circ h^{-1} = \overline{p}$, d'où $h \circ \overline{p} = \overline{p} \circ h$.

Pour la commutation avec u : $\overline{p} \circ u = \frac{1}{N} \sum_{k=0}^{N-1} h^k \circ p \circ h^{-k} \circ u$. On exploite 11.c : $h^{-k} \circ u = \zeta^{-k} u \circ h^{-k}$. Donc le terme de la somme s'écrit $h^k \circ p \circ \zeta^{-k} u \circ h^{-k}$. Comme p et u commutent, cela vaut $h^k \circ (\zeta^{-k} u) \circ p \circ h^{-k}$. Toujours d'après 11.c, $h^k \circ (\zeta^{-k} u) \circ h^{-k} = u$, donc en insérant $h^{-k} h^k$ au milieu, on trouve $h^k \circ (\zeta^{-k} u) \circ p \circ h^{-k} = (h^k \circ \zeta^{-k} u \circ h^{-k}) \circ h^k \circ p \circ h^{-k} = u \circ h^k \circ p \circ h^{-k}$. En passant u en facteur de la somme, on a bien $\overline{p} \circ u = u \circ \overline{p}$.

12.e) Puisque $\overline{p}$ est un projecteur d'image W, son noyau $\ker \overline{p}$ est un supplémentaire de W dans V. Soit $x \in \ker \overline{p}$. $\overline{p}(u(x)) = u(\overline{p}(x)) = u(0) = 0$, donc $u(x) \in \ker \overline{p}$. De même, $\overline{p}(h(x)) = h(\overline{p}(x)) = h(0) = 0$, donc $h(x) \in \ker \overline{p}$. Ce supplémentaire est bien stable par u et h.

13.a) u étant d'indice n, on a $u^{n-1} \neq 0$. Puisque h est diagonalisable, V se décompose en somme directe de ses sous-espaces propres associés aux valeurs propres de la forme ζ^j (certains peuvent être réduits à $\{0\}$). Si pour tous les j, u^{n-1} était nul sur V_j, il serait nul sur V, ce qui est exclu. Il existe donc au moins un indice j et un vecteur $v \in V_j$ tel que $u^{n-1}(v) \neq 0$. Ce vecteur v est bien propre pour h.

13.b) On procède par récurrence sur la dimension de V. On choisit v propre pour h (soit $h(v) = \zeta^a v$) tel que $u^{n-1}(v) \neq 0$. Le sous-espace $W = \mathrm{Vect}(u^{n-1}(v), \dots, u(v), v)$ est stable par u (question 8). Il est également stable par h car $h(u^k(v)) = \zeta^{a+k}u^k(v)$, chaque vecteur de cette base est donc un vecteur propre de h. Dans cette base ordonnée, la matrice de u_W est J_n, et celle de h_W est la matrice diagonale $D_{n,a} = \mathrm{diag}(\zeta^{a+n-1}, \dots, \zeta^{a+1}, \zeta^a)$. (Une réindexation adéquate donne la forme $D_{r,a}$ classique). D'après les questions 8 et 12, W admet un supplémentaire stable par u et par h. On conclut en appliquant l'hypothèse de récurrence à ce supplémentaire.

14.a) On a $V = V_1 \oplus V_2 \oplus V_3$ puisque $V_0 = \ker(h - \mathrm{id}_V) = \{0\}$. D'après 11.b), on a $u(V_1) \subset V_2$, $u(V_2) \subset V_3$, et $u(V_3) \subset V_0 = \{0\}$. Donc $u^3(V_1) \subset u^2(V_2) \subset u(V_3) = \{0\}$. Puisque u^3 est nul sur tous les sous-espaces composant V, l'endomorphisme u^3 est nul : $u^3 = 0$.

14.b) Un bloc correspond à une suite d'exposants de ζ de la forme $(a, a+1, \dots, a+r-1 \pmod 4)$. Comme $V_0 = \{0\}$, la valeur 0 ne peut pas apparaître dans la suite. La taille maximale d'une suite sans 0 est donc 3, et doit être exactement $(1, 2, 3)$.

- Taille 1 ($r = 1$) : Les indices possibles sont $\{1, 2, 3\}$. Cela donne 3 types : $(J_1, D_{1,1})$, $(J_1, D_{1,2})$, $(J_1, D_{1,3})$.
- Taille 2 ($r = 2$) : Les paires consécutives sans 0 sont $(1, 2)$ et $(2, 3)$. Cela donne 2 types : $(J_2, D_{2,1})$ et $(J_2, D_{2,2})$.
- Taille 3 ($r = 3$) : La seule suite est $(1, 2, 3)$. Cela donne 1 type : $(J_3, D_{3,1})$.

Il y a donc $3 + 2 + 1 = 6$ types de blocs possibles.

14.c) Notons $n_{r,a}$ le nombre de blocs de type $(J_r, D_{r,a})$. La dimension $d_j = \dim V_j$ correspond au nombre d'apparitions de ζ^j sur la diagonale des matrices de h. On a :

$$d_1 = n_{1,1} + n_{2,1} + n_{3,1}$$
$$d_2 = n_{1,2} + n_{2,1} + n_{2,2} + n_{3,1}$$
$$d_3 = n_{1,3} + n_{2,2} + n_{3,1}$$

Le rang de u_1 (qui va de V_1 vers V_2) correspond au nombre de transitions de 1 vers 2 dans les blocs, soit $r_1 = n_{2,1} + n_{3,1}$. Le rang de u_2 (de V_2 vers V_3) correspond au nombre de transitions de 2 vers 3, soit $r_2 = n_{2,2} + n_{3,1}$. Le rang de la composée $u_2 \circ u_1$ est le nombre de transitions de 1 jusqu'à 3, ce qui n'arrive que dans les blocs de taille 3 : $r_{21} = n_{3,1}$. Le système est triangulaire. On déduit $n_{3,1} = r_{21}$, puis $n_{2,1} = r_1 - r_{21}$ et $n_{2,2} = r_2 - r_{21}$. Ensuite, on trouve les $n_{1,j}$ à partir des d_j. Les nombres de blocs de chaque type sont donc déterminés de façon unique par ces dimensions et rangs.

15.

- (i) $\iff$ (ii) : Dire que (A, B) et (A', B') sont simultanément équivalents signifie que A' et A (resp. B' et B) représentent la même application avec les mêmes paires de bases de départ et d'arrivée interverties. Les formules de changement de base matriciel se traduisent directement par l'existence de matrices de passage inversibles P (pour $e \to e'$) et Q (pour $f \to f'$) telles que $A' = QAP^{-1}$ et $B' = PBQ^{-1}$.
- (ii) $\implies$ (iii) : Posons $R = \mathrm{diag}(P, Q) \in GL_{m+n}(\mathbb{C})$. On vérifie immédiatement que R commute avec H, donc $RHR^{-1} = H$. De plus, le calcul par blocs montre que

$$RM_{A,B}R^{-1} = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix} \begin{pmatrix} 0 & B \\ A & 0 \end{pmatrix} \begin{pmatrix} P^{-1} & 0 \\ 0 & Q^{-1} \end{pmatrix} = \begin{pmatrix} 0 & PBQ^{-1} \\ QAP^{-1} & 0 \end{pmatrix} = M_{A',B'}$$

L'assertion (iii) est prouvée.

— (iii) $\implies$ (ii) : Si (iii) est vraie, la relation $H = RHR^{-1}$ donne $HR = RH$. En notant $R = \begin{pmatrix} P & S \\ T & Q \end{pmatrix}$, l'égalité $HR = RH$ impose $\begin{pmatrix} P & S \\ -T & -Q \end{pmatrix} = \begin{pmatrix} P & -S \\ T & -Q \end{pmatrix}$, d'où $S = 0$ et $T = 0$. R est donc diagonale par blocs. Le calcul fait à l'étape précédente garantit alors que $A' = QAP^{-1}$ et $B' = PBQ^{-1}$.

16.a) On a $H^2 = \text{diag}(I_m, -I_n)^2 = \text{diag}(I_m, I_n) = I_{m+n}$. Le calcul de similitude donne :

$$HMH^{-1} = HMH = \begin{pmatrix} I_m & 0 \\ 0 & -I_n \end{pmatrix} \begin{pmatrix} 0 & B \\ A & 0 \end{pmatrix} \begin{pmatrix} I_m & 0 \\ 0 & -I_n \end{pmatrix} = \begin{pmatrix} 0 & B \\ -A & 0 \end{pmatrix} \begin{pmatrix} I_m & 0 \\ 0 & -I_n \end{pmatrix} = \begin{pmatrix} 0 & -B \\ -A & 0 \end{pmatrix} = -M$$

Par linéarité et par récurrence sur les puissances ($HM^kH^{-1} = (-M)^k$), on en déduit que pour tout polynôme $P \in \mathbb{C}[X]$, $HP(M)H^{-1} = P(-M)$.

16.b) La relation $HMH^{-1} = -M$ montre que les matrices M et $-M$ sont semblables. Elles ont par conséquent le même polynôme caractéristique, ce qui signifie que leurs valeurs propres ont les mêmes multiplicités. Si λ est racine du polynôme caractéristique de M, c'est aussi une racine de celui de $-M$, et donc $-\lambda$ est une valeur propre de M avec même multiplicité algébrique.

16.c) D'après le théorème de Cayley-Hamilton, le polynôme caractéristique χ_M annule M. On peut l'écrire $\chi_M = X^r Q$ où $Q(0) \neq 0$. Les polynômes X^r et Q n'ont aucune racine commune, ils sont donc premiers entre eux. D'après le lemme des noyaux, on a la somme directe $\mathbb{C}^{m+n} = \ker M^r \oplus \ker Q(M)$. Pour la stabilité : si $x \in \ker M^r$, alors $M^r(H(x)) = H((-M)^r(x)) = \pm H(M^r(x)) = 0$, donc $H(x) \in \ker M^r$. Un argument similaire avec Q montre que $\ker Q(M)$ est stable par H.

17. Si M est nilpotente, on applique le théorème "gradué" (partie V) avec $N = 2$ et $\zeta = -1$. Les blocs de M et H peuvent se réduire conjointement. H est diagonale, et les matrices de blocs sont soit paires (de type J_{2k}) et s'intercalent symétriquement entre la dimension m et n, soit impaires. La traduction des suites de valeurs propres alternées (ici $+1$ et -1) pour H donne l'allure des sous-matrices hors-diagonales de M. Les 4 cas correspondent aux façons dont un bloc de Jordan "biparti" peut commencer (en A ou en B) et s'achever. On obtient donc une décomposition en blocs de formes fondamentales avec des décalages de dimensions $|r - s| \leq 1$.

18.a) M^2 est diagonale par blocs : $M^2 = \text{diag}(BA, AB)$. Puisque M est inversible, M^2 l'est aussi, ce qui implique que AB et BA sont inversibles. La matrice $A \in \mathcal{M}_{n,m}$ admet un inverse à droite et un inverse à gauche, elle correspond donc à un endomorphisme injectif et surjectif. On en déduit que $m = n$, et que A et B sont inversibles.

18.b) Puisque A est inversible, le couple (A, B) est équivalent, via une base adaptée (par exemple en choisissant $Q = A^{-1}$ et $P = I_m$), au couple (I_n, BA). L'étude se réduit alors à la similitude de $B' = BA$. En appliquant la décomposition de Jordan classique à cette dernière (qui est inversible, donc on sépare les blocs associés à une valeur propre $\lambda \neq 0$), on récupère le couplage annoncé avec $A_1 = I_r$ et $B_1 = \lambda I_r + J_r$. La taille est paire $(2r)$ du fait de la symétrie bipartie de M.