X-ENS 2025

Épreuve de mathématiques A, MP & MPI, quatre heures
(corrigé)

1 Questions préliminaires

1. **Restriction d'un endomorphisme diagonalisable à un sous-espace stable.**
Comme h est diagonalisable, par le critère polynomial de diagonalisation h admet un polynôme de $\mathbb{C}[X]$ annulateur scindé et à racines simples, que notons P. Par restriction des scalaires, $P(h)$ est nul sur W, et on vérifie aisément que l'endomorphisme induit par $P(h)$ sur W (qui existe bien par stabilité de W par h) est $P(h_W)$. Ainsi $P(h_W)$ est identiquement nul, donc h_W admet un polynôme annulateur scindé et à racines simples. À nouveau par le critère polynomial de diagonalisation, on en déduit que h_W est diagonalisable.

2. **Un invariant matriciel.**
   (a) Si M et M' sont semblables, alors M^k et $(M')^k$ sont semblables pour tout entier naturel k (élever à la puissance k une relation de similitude $M = PM'P^{-1}$), donc en particulier leurs noyaux ont même dimension. Le résultat en découle immédiatement : $\delta_k(M) = \delta_k(M')$.

   (b) Soient $(e_1, \ldots, e_r)$ la base canonique de $\mathbb{C}^n$ et j_r l'endomorphisme de $\mathbb{C}^r$ canoniquement associé à J_r. La définition de cette matrice implique par récurrence :
$$\forall k \in \mathbb{N},\ \forall i \in [\![1, r]\!], \quad j_r^k(e_i) = \begin{cases} e_{i+k} & \text{si } i \leqslant r - k, \\ 0 & \text{si } i > r - k, \end{cases}$$
et donc pour tout $k \in [\![0, r]\!]$ le rang de la famille $\left(j_r^k(e_1), \ldots, j_r^k(e_r)\right)$ est celui de la famille $(e_{k+1}, \ldots, e_r)$, qui vaut $r - k$; si $k > r$ alors j_r^k est nul. Ainsi :
$$\forall k \in \mathbb{N}, \quad \operatorname{rang}(J_r^k) = \operatorname{rang}(j_r^k) = \begin{cases} n - k & \text{si } k \leqslant r - 1, \\ 0 & \text{si } k \geqslant r. \end{cases}$$
On en déduit, par le théorème du rang :
$$\forall k \in \mathbb{N}, \quad \dim(\ker(J_r^{k+1})) - \dim(\ker(J_r^k)) = \operatorname{rang}(J_r^k) - \operatorname{rang}(J_r^{k+1}) = \begin{cases} 1 & \text{si } k \leqslant r - 1, \\ 0 & \text{si } k \geqslant r. \end{cases}$$
Pour tout $k \in \mathbb{N} \setminus \{0\}$, en distinguant selon que k soit supérieur ou inférieur à r, on a donc :
$$\begin{aligned} \delta_k(J_r) &= \left(\dim(\ker(J_r^k)) - \dim(\ker(J_r^{k+1}))\right) - \left(\dim(\ker(J_r^{k-1})) - \dim(\ker(J_r^k))\right) \\ &= \begin{cases} 0 & \text{si } k \geqslant r + 1, \\ 1 & \text{si } k = r, \\ 0 & \text{si } k \leqslant r - 1, \end{cases} \end{aligned}$$
d'où le résultat.

   (c) Soient n_1 et n_2 les tailles de M_1 et M_2, et $r_{1,k}$ et $r_{2,k}$ les rangs de M_1^k et M_2^k, respectivement. Pour tout $i \in \{1, 2\}$ et tout $r \in [\![1, n_i]\!]$, notons $J_{r,n_i} = \operatorname{diag}\left(\mathrm{I}_r, 0_{n_i - r}\right)$ (cette matrice n'a rien à voir avec les matrices J_r de l'énoncé). Pour tout $i \in \{1, 2\}$ et tout $k \in \mathbb{N}$, comme M_i^k est de rang $r_{i,k}$, il existe $(P_{i,k}, Q_{i,k}) \in \mathrm{GL}_{n_i}(\mathbb{C})^2$ tel que : $M_i^k = P_{i,k} J_{r_{i,k}, n_i} Q_{i,k}$. Alors :
$$\forall k \in \mathbb{N}, \quad M^k = \begin{pmatrix} M_1^k & 0 \\ 0 & M_2^k \end{pmatrix} = \begin{pmatrix} P_{1,k} & 0 \\ 0 & P_{2,k} \end{pmatrix} \begin{pmatrix} J_{r_{1,k}, n_1} & 0 \\ 0 & J_{r_{2,k}, n_2} \end{pmatrix} \begin{pmatrix} Q_{1,k} & 0 \\ 0 & Q_{2,k} \end{pmatrix},$$

et les deux matrices aux extrémités du produit sont évidemment inversibles (par exemple l'inverse de $\begin{pmatrix} P_{1,k} & 0 \\ 0 & P_{2,k} \end{pmatrix}$ est $\begin{pmatrix} P_{1,k}^{-1} & 0 \\ 0 & P_{2,k}^{-1} \end{pmatrix}$). Par invariance du rang par relation d'équivalence, on a donc pour tout $k \in \mathbb{N}$:

$$\operatorname{rang}(M^k) = \operatorname{rang}\left(\begin{pmatrix} J_{r_{1,k},n_1} & 0 \\ 0 & J_{r_{2,k},n_2} \end{pmatrix}\right) = r_{1,k} + r_{2,k} = \operatorname{rang}(M_1^k) + \operatorname{rang}(M_2^k)$$

(pour la première égalité, il suffit de remarquer que l'espace vectoriel engendré par les colonnes de $\begin{pmatrix} J_{r_{1,k},n_1} & 0 \\ 0 & J_{r_{2,k},n_2} \end{pmatrix}$ est celui engendré par $r_1 + r_2$ vecteurs extraits de la base canonique). Par le théorème du rang, on a pour tout $k \in \mathbb{N}$:

$$\begin{aligned} \dim(\ker(M^k)) &= 2n - \operatorname{rang}(M^k) \\ &= \left(n - \operatorname{rang}(M_1^k)\right) + \left(n - \operatorname{rang}(M_2^k)\right) \\ &= \dim(\ker(M_1^k)) + \dim(\ker(M_2^k)). \end{aligned}$$

On en déduit aisément l'égalité attendue $\delta_k(M) = \delta_k(M_1) + \delta_k(M_2)$.

Esquisse d'une autre démonstration plus géométrique. On peut aussi introduire l'endomorphisme f de $\mathbb{C}^{n_1+n_2}$ canoniquement associé à M et noter qu'il laisse stable les espaces vectoriels engendrés par $(e_1, \ldots, e_{n_1})$ et $(e_{n_1+1}, \ldots, e_{n_2})$ respectivement. Si l'on note f_1 et f_2 les deux endomorphismes induits sur les espaces précités, et p_1, p_2 les projecteurs associés à la décomposition $\mathbb{C}^{n_1+n_2} = \operatorname{Vect}\left((e_1, \ldots, e_{n_1})\right) \oplus \operatorname{Vect}\left((e_{n_1+1}, \ldots, e_{n_2})\right)$, on a : $\forall k \in \mathbb{N}$, $f^k = f_1^k \circ p_1 + f_2^k \circ p_2$, ce dont on peut déduire l'égalité : $\operatorname{im}(f^k) = \operatorname{im}(f_1^k) \oplus \operatorname{im}(f_2^k)$. Le résultat en découle facilement.

2 Algèbre linéaire sur les polynômes de Laurent

3. **L'application linéaire $\widehat{\xi}$ et l'endomorphisme ξ.**

(a) Comme $\widehat{\xi} \circ \Pi$ et $\widehat{\xi}$ sont linéaires, ces deux applications sont égales si et seulement si elles coïncident sur une partie génératrice. Comparons donc leurs évaluations en les polynômes de Laurent de la forme X^k avec $k \in \mathbb{Z}$. Soit $k \in \mathbb{Z}$. On a :

$$\widehat{\xi}(X^k) = \Pi(X^{k+1})$$

et :

$$\widehat{\xi}(\Pi(X^k)) = \Pi(X\Pi(X^k)) = \begin{cases} \Pi(X \cdot X^k) = \Pi(X^{k+1}) & \text{si } k \leqslant -1, \\ \Pi(X \cdot 0) = 0 = \Pi(X^{k+1}) & \text{si } k \in \mathbb{N}. \end{cases}$$

Dans tous les cas : $\widehat{\xi}(\Pi(X^k)) = \widehat{\xi}(X^k)$. Ceci vaut pour tout $k \in \mathbb{Z}$, donc par l'argument ci-dessus on a bien : $\widehat{\xi} \circ \Pi = \widehat{\xi}$.

(b) Comme $P \mapsto P(\xi)(F)$ et $P \mapsto \Pi(PF)$ sont linéaires sur $\mathbb{C}[X]$ (cela tient essentiellement à la linéarité de l'évaluation en ξ et de Π), démontrer qu'elles sont égales revient à démontrer qu'elles coïncident sur une partie génératrice de $\mathbb{C}[X]$. Nous considérons la base canonique. Soit $k \in \mathbb{N} \setminus \{0\}$. L'égalité de la question précédente implique, par restriction à $\mathcal{D}$, l'égalité : $\xi \circ \Pi = \xi$. Composons-la par ξ^{k-1} et évaluons-la en XG avec $G \in \mathcal{D}$. On obtient :

$$\forall G \in \mathcal{D}, \quad \xi^{k+1}(G) = \xi^k(\xi(G)) = \xi^k(\Pi(XG)) = \xi^k(XG).$$

Ceci vaut pour tout $k \in \mathbb{N} \setminus \{0\}$. Par récurrence, on en déduit :

$$\forall k \in \mathbb{N} \setminus \{0\}, \ \forall G \in \mathcal{D}, \quad \xi^k(G) = \xi(X^{k-1}G) = \Pi(X^k G).$$

On remarque que cette identité reste valable pour $k = 0$. En posant $G = F$, on obtient donc l'égalité $P(\xi)(F) = \Pi(PF)$ pour tout P de la forme X^k avec $k \in \mathbb{N}$, et donc pour tout $P \in \mathbb{C}[X]$, par linéarité.

4. **Image et noyau des puissances de ξ.**
Notons que X^{-j-n} appartient à $\mathcal{D}$ pour tout $j \in \mathbb{N} \setminus \{0\}$. D'après l'égalité de la question précédente, on a pour tout $j \in \mathbb{N} \setminus \{0\}$:
$$\xi^n(X^{-j-n}) = \Pi(X^{-j}) = X^{-j}.$$
Ceci démontre que X^{-j} appartient à l'image de ξ^n pour tout $j \in \mathbb{N} \setminus \{0\}$, et comme ces monômes engendrent $\mathcal{D}$ on en déduit : $\mathcal{D} \subseteq \mathrm{im}(\xi^n)$. L'inclusion réciproque est immédiate par définition de ξ, d'où l'égalité :
$$\mathrm{im}(\xi^n) = \mathcal{D},$$
démontrant que ξ^n est surjective de $\mathcal{D}$ dans lui-même. Pour une base du noyau, notons que Π étant un projecteur parallèlement à $\mathbb{C}[X]$, on a : $\ker(\Pi) = \mathbb{C}[X]$. Comme $F \mapsto X^n F$ est une bijection de $X^{-n}\mathbb{C}[X]$ dans $\mathbb{C}[X]$, on en déduit, toujours grâce à l'expression de la question précédente :
$$\ker(\xi^n) = X^{-n}\mathbb{C}[X] \cap \mathcal{D} = \mathrm{Vect}\left(\left(X^{-n}, X^{-n+1}, \ldots, X^{-1}\right)\right).$$
Une base de $\ker(\xi^n)$ est donc $\emptyset$ si $n = 0$, et $(X^{-n}, X^{-n+1}, \ldots, X^{-1})$ si $n \geqslant 1$.

5. **Sous-espaces cycliques.**
Nous allons démontrer :
$$\mathcal{D}_r = \mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right).$$
Le fait que $\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}$ soit une base de $\mathcal{D}_r$ en découlera immédiatement.
Pour l'inclusion réciproque, on note que ξ stabilise $\mathcal{D}_r$ et donc, par récurrence : $\forall k \in \mathbb{N}$, $\xi^k(X^{-r}) \in \mathcal{D}_r$. Par la question 3.(b), cela signifie : $\forall k \in \mathbb{N}$, $\Pi(X^{k-r}) \in \mathcal{D}_r$. En particulier, pour $k \in [\![0, r-1]\!]$, on a $k - r \leqslant -1$ et donc X^{k-r} appartient à $\mathcal{D}_r$, d'où : $\forall k \in [\![0, r-1]\!]$, $X^{k-r} \in \mathcal{D}_r$. Un espace vectoriel étant stable par combinaison linéaire, on a l'inclusion : $\mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right) \subseteq \mathcal{D}_r$.
Réciproquement, le sous-espace vectoriel $\mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right)$ contient X^{-r} et est stable par ξ. En effet, pour tout $k \in [\![0, r-2]\!]$ on a $1 + k - r \leqslant -1$, et donc :
$$\forall k \in [\![0, r-2]\!], \quad \xi\left(X^{k-r}\right) = \Pi(X^{1+k-r}) = X^{1+k-r} \in \mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right),$$
et :
$$\xi(X^{(r-1)-r}) = \Pi\left(1\right) = 0 \in \mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right).$$
Par linéarité, $\mathrm{Vect}\left(\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}\right)$ est bien stable par ξ. Par minimalité de $\mathcal{D}_r$, on a donc bien l'inclusion réciproque puis l'égalité annoncée, et $\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}$ est une base de $\mathcal{D}_r$.
Le calcul des images de X^{k-j} par ξ, effectué ci-dessus, donne immédiatement pour matrice :
$$\mathrm{M}_{\left(X^{k-r}\right)_{0\leqslant k\leqslant r-1}}\left(\xi_{\mathcal{D}_r}\right) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} = J_r.$$

3 Prolongements compatibles

6. **Prolongement compatible avec u donné par un vecteur.**

(a) L'ensemble $\mathcal{J}$ est un groupe pour l'addition puisqu'il contient 0 (en effet W contient le vecteur nul) et W est stable par combinaison linéaire. Vérifions la propriété d'absorption : soient $Q \in \mathbb{C}[X]$ et $P \in \mathcal{J}$. Alors $P(u)(v)$ appartient à W par définition de $\mathcal{J}$, et comme W est stable par u on a :

$$\forall k \in \mathbb{N}, \quad u^k\left(P(u)(v)\right) \in W.$$

En décomposant Q dans la base canonique de $\mathbb{C}[X]$ on a donc, par linéarité et par stabilité par combinaison linéaire de W :

$$(QP)(u)(v) = Q(u)(P(u)(v)) \in W,$$

d'où le résultat. Ainsi $\mathcal{J}$ est un idéal de $\mathbb{C}[X]$.

(b) Comme u est nilpotent, il existe $n \in \mathbb{N}$ tel que u^n soit nul. En prenant $P = X^n$, on a alors : $P(u)(v) = u^n(v) = 0 \in W$, d'où le résultat : $X^n \in \mathcal{J}$.

Comme les idéaux de $\mathbb{C}[X]$ sont principaux, par la question précédente il existe $\pi \in \mathbb{C}[X]$ tel que : $\mathcal{J} = \pi\mathbb{C}[X]$. Le calcul ci-dessus démontre que X^n appartient à $\pi\mathbb{C}[X]$, donc π divise X^n : on en déduit l'existence de $r \in [\![0, n]\!]$ tel que $\pi = X^r$. D'où le résultat :

$$\mathcal{J} = \pi\mathbb{C}[X] = X^r\mathbb{C}[X].$$

Remarque. On a $r \neq 0$. En effet, dans le cas contraire, on aurait $1 \in \mathcal{J}$, et donc : $1(u)(v) \in W$. C'est impossible puisque : $1(u)(v) = \mathrm{Id}_V(v) = v$, et par hypothèse v n'est pas dans V.

(c) Prendre $P = 0 \in \mathbb{C}[X]$ dans la description de W' donne l'inclusion $W \subseteq W'$, et prendre $(P, w) = (1, 0)$ donne l'appartenance de v à W'. Démontrons la stabilité par u. Soit $x \in W'$. Il existe $(P, w) \in \mathbb{C}[X] \times W$ tel que : $x = P(u)(v) + w$. Comme u laisse stable W, on a $u(w) \in W$. On en déduit que si l'on pose $Q = XP \in \mathbb{C}[X]$, on a par linéarité de u :

$$u(x) = u \circ P(u)(v) + u(w) = Q(u)(v) + u(w) \in W'.$$

Ceci vaut pour tout $x \in W'$, d'où le résultat.

Remarque. On en aura besoin dans la question 7 : l'inclusion de W dans W' est *stricte* puisque W' contient v, au contraire de W.

(d) On a vu à la question 4 que ξ^r est une surjection de $\mathcal{D}$ dans lui-même. Comme $G_v = \varphi(u^r(v))$ est dans l'image de φ, qui est incluse dans $\mathcal{D}$, l'existence de $F_v \in \mathcal{D}$ tel que $G_v = \xi^r(F_v)$ en découle aisément.

(e) Rappelons que l'on a : $\xi \circ \varphi = \varphi \circ u_W$. On en déduit par récurrence sur k :

$$\forall k \in \mathbb{N}, \quad \xi^k \circ \varphi = \varphi \circ u_W^k.$$

Le cas $k = 0$ est trivial, et si $k \in \mathbb{N}$ vérifie : $\xi^k \circ \varphi = \varphi \circ u_W^k$, alors :

$$\xi^{k+1} \circ \varphi = \xi \circ \xi^k \circ \varphi = \xi \circ \varphi \circ u_W^k = \varphi \circ u_W \circ u_W^k = \varphi \circ u_W^{k+1},$$

d'où l'hérédité. Par principe de récurrence, on a le résultat. Ainsi les applications linéaires $P \mapsto P(\xi) \circ \varphi$ et $P \mapsto \varphi \circ P(u_W)$ coïncident sur $\left(X^k\right)_{k \in \mathbb{N}}$, donc sur l'espace engendré sur cette famille. On en déduit :

$$\forall Q \in \mathbb{C}[X], \quad Q(\xi) \circ \varphi = \varphi \circ Q(u_W). \qquad (*)$$

Déduisons-en le résultat voulu. Supposons : $P(u)(v) = w$. Alors $P(u)(v)$ appartient à W, donc : $P \in \mathcal{J} = X^r\mathbb{C}[X]$ (question 6.(b)). On en déduit l'existence de $Q \in \mathbb{C}[X]$ tel que : $P = X^rQ$. Comme $u^r(v)$ appartient à W par définition de r, on en déduit :

$$\begin{aligned} \varphi(w) = \varphi(P(u)(v)) = \varphi(Q(u)(u^r(v))) &= Q(\xi) \circ \varphi(u^r(v)) && (*) \\ &= Q(\xi)(G_v) \\ &= Q(\xi) \circ \xi^r(F_v) && (q.\,6.(d)) \\ &= (X^rQ)(\xi)(F_v) \\ &= P(\xi)(F_v), \end{aligned}$$

d'où le résultat.

(f) Notons que si $0 = P(u)(v) + w$, alors nécessairement on a $P(\xi)(F_v) + \varphi(w) = 0$ d'après la question précédente (à ceci près qu'on remplace P par $-P$), ce qui assure que $\varphi'(0)$ est correctement défini (et égal à 0).

On en déduit que si $x = P(u)(v) + w = Q(u)(v) + w'$ sont deux représentations de x dans W' (avec $Q \in \mathbb{C}[X]$ et $w' \in W$), alors : $0 = (P - Q)(u)(v) + (w - w')$, avec $P - Q \in \mathbb{C}[X]$ et $w - w' \in W$. Par le paragraphe précédent, on a : $0 = (P - Q)(\xi)(v) + \varphi(w - w')$, donc par linéarité de φ et de l'évaluation en v on en déduit :

$$P(\xi)(F_v) + \varphi(w) = Q(\xi)(F_v) + \varphi(w'),$$

ce qui assure que $\varphi'(x)$ ne dépend que de x et pas du choix de P et w.

On note que φ' est bien à valeurs dans $\mathcal{D}$ car φ et ξ le sont. Soit $w \in W$. On a : $w = 0(u)(v)+w$, donc par définition de φ' on a : $\varphi'(w) = 0(\xi)(F_v)+\varphi(w) = \varphi(w)$. Ceci démontre que $\varphi' : W' \to \mathcal{D}$ est bien un prolongement de φ. Vérifions la compatibilité avec u. Soit $x \in W'$. Il existe $(P, w) \in \mathbb{C}[X] \times W$ tel que : $x = P(u)(v) + w$. On a alors, par linéarité de ξ et hypothèse sur φ :

$$\xi(\varphi'(x)) = \xi(P(\xi)(F_v)) + \xi(\varphi(w)) = (XP)(\xi)(F_v) + \varphi(u(w)).$$

Pour calculer $\varphi'(u(x))$, par définition de cette application on doit décomposer $u(x)$ dans W'. Or :

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

avec $u(w) \in W$ par stabilité de ce sous-espace par W. Par définition de φ' on a donc :

$$\varphi'(u(x)) = (XP)(\xi)(F_v) + \varphi(u(w)).$$

On retrouve l'expression ci-dessus, d'où : $\xi(\varphi'(x)) = \varphi'(u(x))$. Ceci vaut pour tout $x \in W'$, donc : $\xi \circ \varphi' = \varphi' \circ u_{W'}$, démontrant la compatibilité de φ' avec u.

7. **Prolongement à V compatible avec u.**

Soit $\mathcal{S}$ l'ensemble des sous-espaces vectoriels de V contenant W, et soit $W' \in \mathcal{S}$ un sous-espace vectoriel tel que :

$$\dim(W') = \max\left\{\dim(W'') \mid W'' \in \mathcal{S},\ \varphi \text{ se prolonge en } \varphi' : W'' \to \mathcal{D} \text{ compatible avec } u\right\}.$$

Ce maximum existe, puisque c'est celui d'une partie de $\mathbb{N}$ non vide (considérer $W'' = W$) et majorée (par $\dim(V)$). Raisonnons par l'absurde et supposons : $W' \neq V$. Soit $\varphi' : W' \to \mathcal{D}$ un prolongement de φ compatible avec u. Par l'hypothèse absurde, W' est strictement inclus dans V, donc par les questions précédentes il existe $W'' \in \mathcal{S}$ contenant W' strictement (donc $\dim(W') < \dim(W'')$) et $\varphi'' : W'' \to \mathcal{D}$ prolongeant φ' en étant compatible avec u ; c'est en particulier un prolongement de φ compatible avec u, donc W'' contredit la propriété de maximalité de W'.

Par l'absurde : $W' = V$, donc φ admet un prolongement ψ à V compatible avec u.

4 Théorème de décomposition pour les endomorphismes nilpotents

8. **Scindage d'un sous-espace cyclique maximal.**

(a) Soit $(a_0, \dots, a_{n-1}) \in \mathbb{C}^n$ tel que : $\sum\limits_{i=0}^{n-1} a_i u^i(v_0) = 0$. Raisonnons par l'absurde et supposons que $(a_0, \dots, a_{n-1})$ est différent du n-uplet nul. Soit alors $j \in [\![0, n-1]\!]$ le plus petit indice tel que $a_j \neq 0$. L'égalité précédente devient : $\sum\limits_{i=j}^{n-1} a_i u^i(v_0) = 0$. En prenant l'image par u^{n-j-1} dans cette égalité, on obtient, comme u^{n-j-1} est linéaire et $n-i-j-1 \geqslant n$ pour $i \geqslant j+1$ (rappelons que u^n est nul, donc toutes les puissances supérieures de u également) :

$$0 = a_j u^{n-1}(v_0) + \sum_{i=j+1}^{n-1} a_i u^{n-i-j-1}(v_0) = a_j u^{n-1}(v_0).$$

Comme $u^{n-1}(v_0) \neq 0$ par définition de v_0, il en résulte : $a_j = 0$. C'est absurde.
Par l'absurde, on a démontré : $(a_0, \dots, a_{n-1}) = (0, \dots, 0)$, obtenant ainsi la liberté de la famille $(v_0, u(v_0), \dots, u^{n-1}(v_0))$.
La stabilité de $W = \mathrm{Vect}\left((v_0, u(v_0), \dots, u^{n-1}(v_0))\right)$ par u se vérifie immédiatement sur la partie génératrice naturelle :

$$\forall j \in [\![0, n-2]\!],\ u\left(u^j(v_0)\right) = u^{j+1}(v_0) \in \left(v_0, u(v_0), \dots, u^{n-1}(v_0)\right) \subseteq W,$$

et :

$$u\left(u^{n-1}(v_0)\right) = u^n(v_0) = 0 \in W,$$

donc par linéarité on a la stabilité de W par u. Ce calcul donne immédiatement :

$$\mathrm{M}_{(v_0, u(v_0), \dots, u^{n-1}(v_0))}(u_W) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} = J_n.$$

(b) Soit $\varphi : W \to \mathcal{D}$ l'application linéaire définie sur la base de la question précédente (que l'on note $\mathcal{B}$ dans ce qui suit) par : $\forall j \in [\![0, n-1]\!]$, $\varphi(u^j(v_0)) = X^{j-n}$. Par la question 5, l'image par φ de la base $\mathcal{B}$ de W est la base $(X^{j-n})_{0 \leqslant j \leqslant n-1}$ de $\mathcal{D}_n$, donc φ induit un isomorphisme de W dans $\mathcal{D}_n$, noté $\tilde{\varphi}$ par la suite ; en particulier φ est une application linéaire injective. De plus, par la question 5 et la question précédente, les matrices de u_W dans $\mathcal{B}$ et de $\xi_{\mathcal{D}_n}$ dans $(X^{j-n})_{0 \leqslant j \leqslant n-1} = \varphi(\mathcal{B})$ sont égales, donc celles de u_W et $\tilde{\varphi}^{-1} \circ \xi \circ \tilde{\varphi}$ dans $\mathcal{B}$ le sont aussi (utiliser la formule du changement de base). Il y a donc égalité : $u_W = \tilde{\varphi}^{-1} \circ \xi \circ \tilde{\varphi}$. D'où le résultat en composant à gauche de chaque membre de l'égalité par $\tilde{\varphi}$.

(c) En reprenant le raisonnement en début de résolution de la question 6.(e), on a :

$$\forall k \in \mathbb{N}, \quad \xi^k \circ \psi = \psi \circ u^k. \tag{†}$$

En prenant $k = n$, on a par nilpotence de u l'égalité : $\xi^n \circ \psi = 0$, donc : $\mathrm{im}(\psi) \subseteq \ker(\xi^n)$.

(d) Pour tout $x \in \ker(\psi)$, on a :

$$\psi(u(x)) = \xi(\psi(x)) = \xi(0) = 0,$$

donc : $u(x) \in \ker(\psi)$. Ceci démontre déjà la stabilité par u du noyau de ψ. Démontrons à présent que c'est un supplémentaire de W, en commençant par démontrer que W et $\ker(\psi)$ sont en somme directe. Comme ψ est un prolongement de φ, on a :

$$\ker(\psi) \cap W = \ker(\varphi) = \{0\}$$

car φ est injective. Ceci démontre que W et $\ker(\psi)$ sont en somme directe. Il reste à démontrer que la somme de leurs dimensions égale la dimension de V. L'image de ψ est incluse dans le noyau de ξ^n, donc :

$$\operatorname{rang}(\psi) \leqslant \dim\left(\ker\left(\xi^n\right)\right) \overset{(q.\,4)}{=} n,$$

et par le théorème du rang : $\dim(\ker(\psi)) \geqslant \dim(V) - n$. On en déduit :

$$\dim(V) \geqslant \dim(W \oplus \ker(\psi)) = \dim(W) + \dim(\ker(\psi)) = n + \dim(\ker(\psi)) \geqslant \dim(V).$$

Par antisymétrie : $\dim(W \oplus \ker(\psi)) = \dim(V)$, d'où le résultat : W et $\ker(\psi)$ sont supplémentaires et ce noyau est stable par u.

9. **Théorème de décomposition : existence.**
On raisonne par récurrence, le prédicat à démontrer étant pour tout $k \in \mathbb{N} \setminus \{0\}$:

   P_k : « Pour tout espace vectoriel V non nul de dimension au plus k et pour tout endomorphisme nilpotent u de V, il existe une base de V, un entier naturel s et des entiers naturels non nuls $r_1, \cdots, r_s$ dans laquelle la matrice de u est $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$. »

   Pour $k = 1$ il n'y a rien à raconter, puisqu'un endomorphisme nilpotent d'un espace de dimension 1 est toujours nul : sa matrice dans toute base est $(0) = J_1$. D'où P_1.

   Soit $k \in \mathbb{N} \setminus \{0\}$. On suppose P_k. Soient V un espace vectoriel de dimension $k+1$ et u un endomorphisme nilpotent de V. Soit n son indice de nilpotence. Si $n = k+1$, alors par la question 8.(a) on a immédiatement $\mathrm{M}_{(v_0, u(v_0), \ldots, u^{n-1}(v_0))}(u) = J_{k+1}$ pour un bon choix de vecteur v_0 (qui existe par définition de l'indice de nilpotence), ce qui conclut avec $s = 1$ et $r_1 = k+1$.

   Supposons à présent $n < k+1$. On introduit les sous-espaces vectoriels W et $\ker(\psi)$ des questions précédentes, avec les mêmes notations, et l'on rappelle que l'on a : $\mathrm{M}_{(v_0, u(v_0), \ldots, u^{n-1}(v_0))}(u_W) = J_n$. Posons $E = \ker(\psi)$ pour alléger les notations. Le sous-espace E est stable par u d'après la question précédente, et l'endomorphisme induit par u sur E reste nilpotent. De plus : comme $W \notin \{\{0\}, V\}$, la supplémentarité de W et E implique que E est non nul et de dimension strictement inférieure à $k+1$. On peut donc appliquer l'hypothèse de récurrence à l'espace vectoriel E muni de l'endomorphisme nilpotent u_E : il existe une base $\mathcal{B}$ de E telle que la matrice de u_E dans $\mathcal{B}$ soit de la forme $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$.

   Dans la concaténation des bases $\left(v_0, u\left(v_0\right), \ldots, u^{n-1}\left(v_0\right)\right)$ et $\mathcal{B}$, qui donne bien une base de V d'après la somme directe $V = W \oplus E$, la matrice de u est $\operatorname{diag}(J_n, J_{r_1}, \ldots, J_{r_s})$, d'où P_{k+1}.

   Par principe de récurrence, on a le résultat voulu pour tout entier naturel k non nul. Quitte à réarranger la base, on peut ordonner les r_i pour avoir $r_1 \geqslant \cdots \geqslant r_s$, ce qui conclut.

10. **Théorème de décomposition : unicité de la taille des blocs.**
Supposons que u admet, dans des bases adaptées, pour matrices $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$ et $\operatorname{diag}(J_{r'_1}, \ldots, J_{r'_t})$ respectivement (ainsi le nombre de blocs est s dans le premier cas et t dans le second). Par la formule du changement de base, ces deux matrices sont semblables, donc elles ont le même rang. Or J_r est de rang $r-1$ pour tout $r \in \mathbb{N} \setminus \{0\}$, donc la forme diagonale par blocs permet, par un raisonnement semblable à celui de la question 2.(c), d'en déduire :

$$\operatorname{rang}\left(\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})\right) = \sum_{i=1}^{s} (r_i - 1) = \sum_{i=1}^{s} r_i - s = n - s.$$

   De même : $\operatorname{rang}\left(\operatorname{diag}(J_{r'_1}, \ldots, J_{r'_t})\right) = n - t$. L'égalité des rangs permet donc de conclure que $s = t$.

De plus, par la question 2.(a), ces deux matrices semblables vérifient :

$$\forall k \in \mathbb{N} \setminus \{0\}, \quad \delta_k\left(\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})\right) = \delta_k\left(\operatorname{diag}(J_{r'_1}, \ldots, J_{r'_s})\right).$$

Par la question 2.(c), on a donc :

$$\forall k \in \mathbb{N} \setminus \{0\}, \quad \sum_{i=1}^{s} \delta_k\left(J_{r_i}\right) = \sum_{i=1}^{s} \delta_k\left(J_{r'_i}\right).$$

On simplifie ces deux membres grâce à la question 2.(b) enfin, et on obtient :

$$\forall k \in \mathbb{N} \setminus \{0\}, \quad \operatorname{card}\left(\{i \in [\![1, s]\!] \mid r_i = k\}\right) = \operatorname{card}\left(\{i \in [\![1, s]\!] \mid r'_i = k\}\right).$$

Autrement dit, il y a autant de blocs de taille k dans $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$ et $\operatorname{diag}(J_{r'_1}, \ldots, J_{r'_s})$, et ce pour tout $k \in \mathbb{N} \setminus \{0\}$. Puisque chaque entier apparaît autant de fois dans les suites $(r_1, \ldots, r_s)$ et $(r'_1, \ldots, r'_s)$, et que ces deux suites sont décroissantes, on a : $(r_1, \ldots, r_s) = (r'_1, \ldots, r'_s)$, ce qu'il fallait démontrer (on pouvait aussi déduire l'égalité $s = t$ d'une utilisation plus soignée de l'égalité ci-dessus).

5 Version « graduée » du théorème de décomposition

11. **Propriétés de h.**
   (a) L'endomorphisme h admet $X^N - 1 \in \mathbb{C}[X]$ pour polynôme annulateur, qui est scindé et à racines simples sur $\mathbb{C}$ (on a : $X^N - 1 = \prod_{j=0}^{N-1}(X - \zeta^j)$), donc h est diagonalisable par le critère polynomial de diagonalisation.
   (b) Remarquons que $\zeta^N = 1$, si bien que finalement : $V_N = V_0 = \ker(h - \zeta^N \mathrm{id}_V)$. Cela permet d'uniformiser les notations.
   Soit $x \in V_j$. On a par définition : $h(x) = \zeta^j x$, donc par hypothèse de l'énoncé (qui peut se réécrire $h \circ u = \zeta\, u \circ h$) :

$$h(u(x)) = \zeta\, u(h(x)) = \zeta \cdot \zeta^j u(x) = \zeta^{j+1} u(x),$$

   donc : $u(x) \in V_{j+1}$. Ceci démontre l'inclusion voulue : $u\left(V_j\right) \subseteq V_{j+1}$.
   (c) Notons d'abord que $h^{\pm k}$ existe pour tout entier relatif k parce que h est inversible.
   Soit $k \in \mathbb{Z}$. On va calculer $h^k \circ u \circ h^{-k}$ restreint aux sous-espaces propres V_j. Soient $j \in [\![0, N-1]\!]$ et $x \in V_j$. On a $h(x) = \zeta^j x$ et donc : $h^k(x) = \left(\zeta^j\right)^k x = \zeta^{jk} x$. Pour k positif, c'est du cours et cela se démontre par récurrence. Pour k négatif, on écrit $h^{-k}(x) = \zeta^{-jk} x$ (ce qui est licite par ce qui précède puisque $-k \geqslant 0$) et on compose cette égalité par h^k, qui est l'inverse de h^{-k}.
   Ce raisonnement vaut pour tous k, j et x, donc aussi pour $-k$, $j+1$ et $u(x) \in V_{j+1}$. D'où :

$$h^k \circ u \circ h^{-k}(x) = h^k \circ u\left(\zeta^{-jk} x\right) = \zeta^{-jk} h^k\left(u\left(x\right)\right) = \zeta^{-jk} \cdot \zeta^{(j+1)k} u(x) = \zeta^k u(x).$$

   Ainsi les endomorphismes $h^k \circ u \circ h^{-k}$ et $\zeta^k u$ coïncident sur V_j pour tout $j \in [\![0, N-1]\!]$, donc aussi sur $V = \bigoplus_{j=0}^{N-1} V_j$ (car h est diagonalisable). En résumé :

$$\forall k \in \mathbb{Z}, \quad h^k \circ u \circ h^{-k} = \zeta^k u.$$

   Pour tout $\ell \in \mathbb{N}$, on a directement :

$$h \circ u^\ell \circ h^{-1} = \left(h \circ u \circ h^{-1}\right)^\ell = (\zeta u)^\ell = \zeta^\ell u^\ell.$$

12. **Recherche d'un supplémentaire stable.**

(a) Si $x \in W$ alors, comme p est un projecteur sur W, on a : $p(x) = x$. Notons de plus que u laisse stable W, donc $u(x) \in W$ et par le même argument : $p(u(x)) = u(x)$. Ainsi :

$$p \circ u(x) = u(x) = u(p(x)) = u \circ p(x).$$

On raisonne de même avec W' (qui est également stable), à ceci près que $p(x) = 0$ et $p(u(x)) = 0$:

$$p \circ u(x) = 0 = u(0) = u \circ p(x).$$

Ainsi $p \circ u$ et $u \circ p$ sont linéaires et coïncident sur W et W', donc sur $V = W \oplus W'$, d'où le résultat : $u \circ p = p \circ u$.

(b) On a pour tout $k \in [\![0, N-1]\!]$, par stabilité de W par h, l'inclusion : $h^k(W) \subseteq W$.

On a mieux et cela nous servira ensuite. On a l'égalité : $h(W) = W$ (en effet h est un isomorphisme de V dans lui-même, donc il préserve les dimensions ; l'inclusion $h(W) \subseteq W$ implique l'égalité). On en déduit qu'on a aussi : $h^{-1}(W) = W$. Une récurrence permet d'étendre l'égalité à tout exposant de h, positif comme négatif.

On a donc : $h^k \circ p \circ h^{-k}(V) \subseteq h^k \circ p(V) = h^k(W) \subseteq W$. Comme W est stable par combinaison linéaire, l'image de $\bar{p} = \frac{1}{N} \sum_{k=0}^{N-1} h^k \circ p \circ h^{-k}$ est incluse dans W.

Soit $w \in W$. Comme p fixe les éléments de W et que h^{-k} laisse stable W (voir ci-dessus), on a $h^{-k}(w) \in W$ et donc :

$$\bar{p}(w) = \frac{1}{N} \sum_{k=0}^{N-1} h^k(h^{-k}(w)) = \frac{1}{N} \sum_{k=0}^{N-1} w = w,$$

d'où le résultat.

(c) On a :

$$\bar{p}^2 = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{\ell=0}^{N-1} h^k \circ p \circ h^{-k+\ell} \circ p \circ h^{-\ell}.$$

Or l'image de p est incluse dans W d'après la question précédente, et donc celle de $h^{-k+\ell} \circ p$ aussi puisque h laisse stable W (voir la question précédente pour l'extension de cette propriété de stabilité à toutes les puissances, y compris négatives). Comme p est un projecteur sur W, on en déduit que p fixe les images de $h^{-k+\ell} \circ p$, c'est-à-dire : $p \circ h^{-k+\ell} \circ p = h^{-k+\ell} \circ p$. Ainsi :

$$\bar{p}^2 = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{\ell=0}^{N-1} h^k \circ h^{-k+\ell} \circ p \circ h^{-\ell} = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{\ell=0}^{N-1} h^\ell \circ p \circ h^{-\ell} = \frac{1}{N} \sum_{k=0}^{N-1} \bar{p} = \bar{p}.$$

Ceci démontre que $\bar{p}$ est un projecteur. Pour obtenir son image, notons que pour un projecteur on a : $\mathrm{im}(\bar{p}) = \ker(\bar{p} - \mathrm{id}_V)$, et que la question précédente démontre les deux inclusions : $\mathrm{im}(\bar{p}) \subseteq W \subseteq \ker(\bar{p} - \mathrm{id}_V)$. D'où l'égalité.

Autre moyen d'obtenir l'image. On peut obtenir le rang de $\bar{p}$ grâce à sa trace. Comme la trace est invariante par similitude, la définition de $\bar{p}$ donne immédiatement : $\mathrm{rang}(\bar{p}) = \mathrm{tr}(\bar{p}) = \mathrm{tr}(p) = \mathrm{rang}(p) = \dim(W)$. Ayant une inclusion de $\mathrm{im}(\bar{p})$ dans W, on a aussi l'égalité.

(d) On a par linéarité de u et la question 11.(c) (où l'on change k en $-k \in \mathbb{Z}$) :

$$u \circ \bar{p} = \frac{1}{N} \sum_{k=0}^{N-1} u \circ h^k \circ p \circ h^{-k} \overset{(q.\,11.(c))}{=} \frac{\zeta^{-k}}{N} \sum_{k=0}^{N-1} h^k \circ u \circ p \circ h^{-k}.$$

Les endomorphismes p et u commutent d'après la question 12.(a), donc :

$$u \circ \bar{p} = \frac{\zeta^{-k}}{N} \sum_{k=0}^{N-1} h^k \circ p \circ u \circ h^{-k} \overset{(q.\,11.(c))}{=} \frac{\zeta^{-k}\zeta^k}{N} \sum_{k=0}^{N-1} h^k \circ p \circ h^{-k} \circ u = \bar{p} \circ u,$$

donc u et $\bar{p}$ commutent. Pour h, notons $\langle h \rangle$ le sous-groupe de $\mathrm{GL}(V)$ engendré par h et r son ordre, qui divise N par hypothèse sur h. On a facilement :

$$\bar{p} = \frac{1}{r} \sum_{g \in \langle h \rangle} g \circ p \circ g^{-1}.$$

On en déduit :

$$h \circ \bar{p} \circ h^{-1} = \frac{1}{r} \sum_{g \in \langle h \rangle} h \circ g \circ p \circ g^{-1} \circ h^{-1} = \frac{1}{r} \sum_{g \in \langle h \rangle} (h \circ g) \circ p \circ (h \circ g)^{-1},$$

or l'application $g \mapsto h \circ g$ est une permutation de $\langle h \rangle$, sa bijection réciproque étant $g \mapsto h^{-1} \circ g$. D'où :

$$h \circ \bar{p} \circ h^{-1} = \frac{1}{r} \sum_{g \in \langle h \rangle} g \circ p \circ g^{-1} = \bar{p},$$

donc : $h \circ \bar{p} = \bar{p} \circ h$, et $\bar{p}$ commute avec h. D'où le résultat.

(e) Comme $\bar{p}$ commute avec u et h, son noyau est stable par u et h. Il est supplémentaire de W, puisque l'image et le noyau d'un projecteur sont supplémentaires et qu'on a démontré que l'image de $\bar{p}$ est W dans la question 12.(c) : d'où le résultat.

13. **Version « graduée » du théorème de décomposition.**

(a) Raisonnons par l'absurde et supposons que pour tout vecteur propre v de h, on a : $u^{n-1}(v) = 0$. Alors la restriction de u^{n-1} à V_j est nulle pour tout $j \in [\![0, N-1]\!]$ et comme h est diagonalisable on a : $V = \bigoplus_{j=0}^{N-1} V_j$, donc u^{n-1} est nulle sur V : cela contredit la définition de l'indice de nilpotence n.

Par l'absurde, il existe un vecteur propre v de h tel que : $u^{n-1}(v) \neq 0$.

(b) On démontre le résultat voulu par récurrence sur la dimension, en suivant une démarche semblable à celle de la question 9.

Si V est de dimension 1, alors l'endomorphisme nilpotent u est nécessairement nul (donc de matrice J_1 dans toute base) et la matrice de h dans toute base est d'ordre 1 donc diagonale. L'étude de ses éléments propres (question 11.(a)) démontre que son unique coefficient est de la forme ζ^a avec $a \in [\![0, N-1]\!]$. Cela initialise la récurrence.

À présent, soit $k \in \mathbb{N} \setminus \{0\}$. Supposons le résultat vrai pour tout espace vectoriel V de dimension au plus k et tous endomorphismes u et h de V vérifiant les propriétés de cette partie. Soit V un espace vectoriel de dimension $k+1$, et soient u et h vérifiant les propriétés de cette partie. Soit n l'indice de nilpotence de u. On introduit v un vecteur propre de h tel que $u^{n-1}(v) \neq 0$ (il en existe par la question précédente) et on pose $W = \mathrm{Vect}\left((v, u(v), \ldots, u^{n-1}(v))\right)$. Par la question 8.(a), c'est un sous-espace stable par u et la matrice de u_W dans $(v, u(v), \ldots, u^{n-1}(v))$ est J_n. De plus, comme v est un vecteur propre de h, et que les valeurs propres de h sont de la forme ζ^a avec $a \in [\![0, N-1]\!]$ (question 11.(a)), on a : $h(v) = \zeta^a v$. On en déduit, par la deuxième identité de la question 11.(c) :

$$\forall \ell \in [\![0, n-1]\!], \quad h(u^\ell(v)) = \zeta^\ell u^\ell(h(v)) = \zeta^\ell u^\ell(\zeta^a v) = \zeta^{a+\ell} u^\ell(v).$$

Cela démontre à la fois que h laisse stable W (on l'a vérifié sur une base), et que la matrice de h_W relativement à la base $(v, u(v), \ldots, u^{n-1}(v))$ est :

$$\begin{pmatrix} \zeta^a & & & \mathbf{0} \\ & \zeta^{a+1} & & \\ & & \ddots & \\ \mathbf{0} & & & \zeta^{a+n-1} \end{pmatrix} = D_{n,a}.$$

Si $n = \dim(V)$, alors ce qu'on vient de faire assure que le résultat est démontré pour u et h. Sinon, on introduit un supplémentaire W' de W dans V stable par u et h, dont l'existence a été établie dans la question 12. Il est distinct de $\{0\}$ et V puisque c'est le cas de W, et la stabilité par u et h assure qu'on peut appliquer l'hypothèse de récurrence aux endomorphismes $u_{W'}$ et $h_{W'}$ de W', qui vérifient les mêmes propriétés que u et h (elles restent valables tout simplement par restriction des identités vectorielles). On en déduit l'existence d'une base $\mathcal{B}$ de W' telle que les matrices de $u_{W'}$ et $h_{W'}$ dans cette base soient simultanément $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$ et $\operatorname{diag}(D_{r_1,a_1}, \ldots, D_{r_s,a_s})$ pour des r_i et a_i adéquats. En concaténant $(v, u(v), \ldots, u^{n-1}(v))$ et $\mathcal{B}$, on obtient une base de V dans laquelle les matrices de u et h sont respectivement $\operatorname{diag}(J_n, J_{r_1}, \ldots, J_{r_s})$ et $\operatorname{diag}(D_{n,a}, D_{r_1,a_1}, \ldots, D_{r_s,a_s})$: d'où l'hérédité.

Par principe de récurrence, le résultat est démontré.

Remarque. Réciproquement, on vérifie la relation : $D_{r,a} J_r D_{r,a}^{-1} = \zeta J_r$, qui assure que tous endomorphismes se réduisant comme dans cette question vérifient les hypothèses $h^N = \mathrm{id}_V$ et $h \circ u \circ h^{-1} = \zeta u$.

14. **Un exemple.**

(a) Par la question 11.(b) on a : $u^3(V_1) \subseteq u^2(V_2) \subseteq u(V_3) \subseteq V_4 = V_0 = \{0\}$. On en déduit que u^3 est nul sur V_1 et on raisonne de même sur V_2 et V_3. Comme $V_1 \oplus V_2 \oplus V_3 = V$ par diagonalisabilité de h (question 11.(a) plus précisément), on a le résultat : $u^3 = 0$.

(b) On a ici $\zeta = e^{\frac{2i\pi}{4}} = i$. Nous cherchons pour u et h des endomorphismes dont les matrices dans une base donnée sont $\operatorname{diag}(J_{r_1}, \ldots, J_{r_s})$ et $\operatorname{diag}(D_{r_1,a_1}, \ldots, D_{r_s,a_s})$ respectivement, avec les a_i dans $[\![1,3]\!]$ (le cas $a_i = 0$ est exclu car 1 n'est pas valeur propre de h). Le fait que u^3 soit nul impose de prendre des blocs de taille au plus 3, puisqu'on démontre facilement que $\max(r_1, \ldots, r_s)$ est l'indice de nilpotence de u. Ainsi les types possibles sont dans $[\![1,3]\!]^2$.

Cependant tous les couples de $[\![1,3]\!]^2$ ne se réalisent pas, à cause de l'inclusion : $u(V_3) \subseteq V_4 = \{0\}$: ceci impose que si i^3 apparaît sur la diagonale de D_{r_i,a_i}, la colonne correspondante de J_{r_i} doit être nulle. Or la seule colonne nulle de J_{r_i} est sa dernière, donc *si* i^3 apparaît sur la diagonale de D_{r_i,a_i}, alors il doit être son dernier coefficient diagonal. Les couples réalisant ceci sont :

$$(1,1), \quad (1,2), \quad (1,3), \quad (2,1), \quad (2,2), \quad (3,1).$$

Réciproquement, tous ces types peuvent se réaliser. Il suffit en effet de prendre pour (u,h) les endomorphismes représentant canoniquement les matrices suivantes (on ne donne des exemples qu'en petite dimension ; mais en dimension quelconque, il suffit de prendre des matrices diagonales par blocs dont les blocs sont ceux ci-dessous) :

$$\Big(\begin{pmatrix}0\end{pmatrix}, \begin{pmatrix}i\end{pmatrix}\Big), \qquad \Big(\begin{pmatrix}0\end{pmatrix}, \begin{pmatrix}i^2\end{pmatrix}\Big), \qquad \Big(\begin{pmatrix}0\end{pmatrix}, \begin{pmatrix}i^3\end{pmatrix}\Big),$$

$$\left(\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}i & 0\\ 0 & i^2\end{pmatrix}\right), \quad \left(\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}i^2 & 0\\ 0 & i^3\end{pmatrix}\right), \quad \left(\begin{pmatrix}0 & 0 & 0\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}, \begin{pmatrix}i & 0 & 0\\ 0 & i^2 & 0\\ 0 & 0 & i^3\end{pmatrix}\right).$$

La remarque de la question précédente assure que ces couples vérifient bien les hypothèses $h^4 = \mathrm{id}_V$ et $h \circ u \circ h^{-1} = iu$.

(c) On remarque que pour les six types de la question précédente, les différentes dimensions se lisent matriciellement et nous avons :

type	mult. de i	mult. de i^2	mult. de i^3	r_1	r_2	$r_{2,1}$
$(1,1)$	1	0	0	0	0	0
$(1,2)$	0	1	0	0	0	0
$(1,3)$	0	0	1	0	0	0
$(2,1)$	1	1	0	1	0	0
$(2,2)$	0	1	1	0	1	0
$(3,1)$	1	1	1	1	1	1

Si u et h ont pour matrices $\operatorname{diag}(J_{r_1}, \dots, J_{r_s})$ et $\operatorname{diag}(D_{r_1,a_1}, \dots, D_{r_s,a_s})$ dans une base donnée, les différentes données ci-dessus s'additionnent. Plus précisément, si l'on note $n(r,a)$ le nombre de couples de type (r,a) dans la réduction ci-avant, et ce pour tout (r,a), alors on a d'après ce tableau :

$$\begin{aligned}
\dim(V_1) &= n(1,1) + n(2,1) + n(3,1),\\
\dim(V_2) &= n(1,2) + n(2,1) + n(2,2) + n(3,1),\\
\dim(V_3) &= n(1,3) + n(2,2) + n(3,1),\\
r_1 &= n(2,1) + n(3,1),\\
r_2 &= n(2,2) + n(3,1),\\
r_{2,1} &= n(3,1).
\end{aligned}$$

En résolvant ce système linéaire vérifié par les $n(r,a)$, on obtient après calculs :

$$\begin{aligned}
n(1,1) &= \dim(V_1) - r_1,\\
n(1,2) &= \dim(V_2) - r_1 - r_2 + r_{2,1},\\
n(1,3) &= \dim(V_3) - r_2,\\
n(2,1) &= r_1 - r_{2,1},\\
n(2,2) &= r_2 - r_{2,1},\\
n(3,1) &= r_{2,1},
\end{aligned}$$

d'où le résultat.

Remarque. Tel que la question est formulée, ces expressions exactes ne sont pas attendues et il suffit de démontrer que le système est inversible. C'est moins calculatoire, puisqu'il suffit pour cela de démontrer que le déterminant suivant est non nul, ce qui est immédiat :

$$\begin{vmatrix} 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix} = 1 \neq 0.$$

Remarque. Cette question assure que dans ce cas particulier, il y a unicité dans le théorème de décomposition graduée.

6 Classification des couples de matrices rectangulaires

15. **Une réduction.**
Supposons que (A,B) et (A',B') sont simultanément équivalents. Soient $\mathbf{e}$, $\mathbf{e}'$ des bases de $\mathbb{C}^m$ et $\mathbf{f}$, $\mathbf{f}'$ des bases de $\mathbb{C}^n$ telles que, pour des applications linéaires $\alpha : \mathbb{C}^m \to \mathbb{C}^n$ et $\beta : \mathbb{C}^n \to \mathbb{C}^m$ adaptées, on ait :

$$A = \mathrm{M}_{\mathbf{f}}(\alpha(\mathbf{e})),\ A' = \mathrm{M}_{\mathbf{f}'}(\alpha(\mathbf{e}')), \quad \text{et :} \quad B = \mathrm{M}_{\mathbf{e}}(\beta(\mathbf{f})),\ B' = \mathrm{M}_{\mathbf{e}'}(\beta(\mathbf{f}')).$$

Par la formule du changement de base, on a alors :

$$A' = \mathrm{M}_{\mathbf{f}'}(\mathbf{f})\mathrm{M}_{\mathbf{f}}(\alpha(\mathbf{e}))\mathrm{M}_{\mathbf{e}}(\mathbf{e}'), \quad \text{et :} \quad B' = \mathrm{M}_{\mathbf{e}'}(\mathbf{e})\mathrm{M}_{\mathbf{f}}(\beta(\mathbf{e}))\mathrm{M}_{\mathbf{f}}(\mathbf{f}').$$

On a donc (ii) en posant $P = \mathrm{M}_{\mathbf{e}'}(\mathbf{e})$ et $Q = \mathrm{M}_{\mathbf{f}'}(\mathbf{f})$, qui sont bien inversibles en tant que matrices de passage (entre deux bases). Ainsi (i) implique (ii).
Supposons l'existence de $P \in \mathrm{GL}_m(\mathbb{C})$ et $Q \in \mathrm{GL}_n(\mathbb{C})$ telles que $A' = QAP^{-1}$ et $B' = PBQ^{-1}$. On a :

$$\begin{aligned}
M_{A',B'} &= \begin{pmatrix} 0_{m,n} & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{pmatrix} \begin{pmatrix} A' & 0_n \\ 0_m & B' \end{pmatrix} \\
&= \begin{pmatrix} 0_{m,n} & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{pmatrix} \begin{pmatrix} Q & 0_{n,m} \\ 0_{m,n} & P \end{pmatrix} \begin{pmatrix} A & 0_n \\ 0_m & B \end{pmatrix} \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 0_{m,n} & \mathrm{I}_m \\ \mathrm{I}_n & 0_{n,m} \end{pmatrix} \begin{pmatrix} Q & 0_{n,m} \\ 0_{m,n} & P \end{pmatrix} \begin{pmatrix} 0_{n,m} & \mathrm{I}_n \\ \mathrm{I}_m & 0_{m,n} \end{pmatrix} \begin{pmatrix} 0_m & B \\ A & 0_n \end{pmatrix} \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix}^{-1} \\
&= \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix} \begin{pmatrix} 0_m & B \\ A & 0_n \end{pmatrix} \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix}^{-1}.
\end{aligned}$$

Posons alors $R = \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix}$, qui est bien carrée d'ordre $m+n$ et inversible puisque son déterminant est $\det(P)\det(Q) \neq 0$. Les égalités ci-dessus démontrent que l'on a $M_{A',B'} = RM_{A,B}R^{-1}$. De plus :

$$RHR^{-1} = \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix} \begin{pmatrix} \mathrm{I}_m & 0_{m,n} \\ 0_{n,m} & -\mathrm{I}_n \end{pmatrix} \begin{pmatrix} P^{-1} & 0_{m,n} \\ 0_{n,m} & Q^{-1} \end{pmatrix} = \begin{pmatrix} PP^{-1} & 0_{m,n} \\ 0_{n,m} & -QQ^{-1} \end{pmatrix} = H,$$

donc (ii) implique bien (iii).
Enfin, supposons qu'il existe $R \in \mathrm{GL}_{m+n}(\mathbb{C})$ telle que $M_{A',B'} = RM_{A,B}R^{-1}$ et $H = RHR^{-1}$. L'implication précédente indique que R devrait être diagonale par blocs, ce que nous allons commencer par démontrer. Notons $R = \begin{pmatrix} P & T \\ S & Q \end{pmatrix}$ avec $P \in \mathrm{M}_m(\mathbb{C})$, $Q \in \mathrm{M}_n(\mathbb{C})$, $T \in \mathrm{M}_{m,n}(\mathbb{C})$ et $S \in \mathrm{M}_{n,m}(\mathbb{C})$. On a : $HR = RH$, ce qu'on peut réécrire ainsi :

$$\begin{pmatrix} P & T \\ -S & -Q \end{pmatrix} = \begin{pmatrix} P & -T \\ S & -Q \end{pmatrix}$$

donc : $T = -T$, et : $S = -S$. Ceci implique la nullité des matrices T et S, donc : $R = \begin{pmatrix} P & 0_{m,n} \\ 0_{n,m} & Q \end{pmatrix}$. L'inversibilité de R implique celle de P et Q, puisque : $\det(P)\det(Q) = \det(R) \neq 0$ (on peut aussi raisonner avec l'endomorphisme canoniquement associé à R, qui reste injectif par restriction à des sous-espaces stables). On a en outre : $R^{-1} = \begin{pmatrix} P^{-1} & 0_{m,n} \\ 0_{n,m} & Q^{-1} \end{pmatrix}$. L'égalité $M_{A',B'} = RM_{A,B}R^{-1}$ équivaut alors, par identification des blocs, à :

$$A' = QAP^{-1}, \quad \text{et :} \quad B' = PBQ^{-1}.$$

Cela démontre (ii) en passant, mais notre véritable but est de démontrer que (iii) implique (i). La démonstration que (i) implique (ii) inspire ce qui suit. Introduisons :
— les bases canoniques de $\mathbb{C}^m$ et $\mathbb{C}^n$, notées $\mathbf{e}$ et $\mathbf{f}$ respectivement ;
— les applications linéaires $\alpha : \mathbb{C}^m \to \mathbb{C}^n$ et $\beta : \mathbb{C}^n \to \mathbb{C}^m$ canoniquement associées à A et B ;
— les colonnes de Q^{-1} et P^{-1}, notées $\mathbf{e}'$ et $\mathbf{f}'$ respectivement.

Par définition de α et β, on a : $A = \mathrm{M}_{\mathbf{f}}(\alpha(\mathbf{e}))$, et : $B = \mathrm{M}_{\mathbf{e}}(\beta(\mathbf{f}))$, et les relations ci-dessus entre A, A', B et B' signifient, grâce à la formule du changement de base :

$$A' = \mathrm{M}_{\mathbf{f}'}(\mathbf{f})\mathrm{M}_{\mathbf{f}}(\alpha(\mathbf{e}))\mathrm{M}_{\mathbf{e}}(\mathbf{e}') = \mathrm{M}_{\mathbf{f}'}(\alpha(\mathbf{e}')).$$

De même pour B', ce qui démontre que (A, B) et (A', B') sont simultanément équivalents : ainsi (iii) implique (i), ce qui achève de démontrer l'équivalence des trois propositions.

16. **Deux applications linéaires : décomposition.**

(a) On a immédiatement : $H^2 = \mathrm{I}_{m+n}$, et : $HMH^{-1} = -M$. En élevant la relation précédente à la puissance k, on en déduit :

$$\forall k \in \mathbb{N}, \quad HM^kH^{-1} = \left(HMH^{-1}\right)^k = (-M)^k.$$

Les applications linéaires $P \mapsto HP(M)H^{-1}$ et $P \mapsto P(-M)$ coïncident sur $\left(X^k\right)_{k\in\mathbb{N}}$ qui engendre $\mathbb{C}[X]$, donc elles sont égales :

$$\forall P \in \mathbb{C}[X], \quad HP(M)H^{-1} = P(-M).$$

(b) Soit x un nombre complexe non nul. On a :

$$\begin{pmatrix} \mathrm{I}_m & 0_{m,n} \\ \frac{1}{x}A & \mathrm{I}_n \end{pmatrix} (x\mathrm{I}_{m+n} - M) = \begin{pmatrix} \mathrm{I}_m & 0_{m,n} \\ \frac{1}{x}A & \mathrm{I}_n \end{pmatrix} \begin{pmatrix} x\mathrm{I}_m & -B \\ -A & x\mathrm{I}_n \end{pmatrix} = \begin{pmatrix} x\mathrm{I}_m & -B \\ 0_{n,m} & x\mathrm{I}_n - \frac{1}{x}AB \end{pmatrix}.$$

Comme le déterminant est multiplicatif, et que le déterminant d'une matrice triangulaire par blocs est le produit des déterminants des blocs diagonaux, cette égalité donne :

$$\det(\mathrm{I}_m)\det(\mathrm{I}_n)\chi_M(x) = \det(x\mathrm{I}_m)\det\left(x\mathrm{I}_n - \frac{1}{x}AB\right) = x^m \cdot \frac{1}{x^n}\det(x^2\mathrm{I}_n - AB).$$

Autrement dit :

$$\chi_M(x) = x^{m-n}\chi_{AB}(x^2).$$

Quitte à multiplier par x^{n-m}, nous avons là une égalité polynomiale valable en une infinité de nombres complexes, donc l'égalité se relève dans $\mathbb{C}[X]$ (ou $\mathbb{C}(X)$). On a démontré :

$$X^{n-m}\chi_M = \chi_{AB}(X^2).$$

Comme le membre de droite est un polynôme pair, si λ est une racine d'ordre k de $\chi_{AB}(X^2)$ alors $-\lambda$ l'est aussi (écrire $\chi_{AB}(X^2) = \chi_{AB}((-X)^2)$ et comparer les ordres de multiplicité des facteurs irréductibles $X - \lambda$ et $X + \lambda$ dans chaque membre de l'égalité : ils doivent être égaux par unicité de la décomposition). Il en est de même pour les racines de χ_M, où il faut simplement traiter le cas $\lambda = 0$ à part à cause du facteur X^{n-m} ; mais dans ce cas $\lambda = -\lambda$ et il est donc trivial que λ et $-\lambda$ sont racines de même ordre de multiplicité. D'où le résultat, puisque les racines de χ_M sont les valeurs propres de M.

(c) Comme $Q(0) \neq 0$, le polynôme irréductible X ne divise pas Q et donc X^r et Q sont premiers entre eux. L'égalité $\mathbb{C}^{m+n} = \ker(M^r) \oplus \ker(Q(M))$ découle alors du lemme de décomposition des noyaux.

Démontrons que ces deux noyaux sont stables par H. Soit $X \in \ker(M^r)$. Par la question 16.(a) on a :

$$M^r(HX) \overset{(q.\,16.(a))}{=} H^{-1}(-M)^rH^2X \overset{(q.\,16.(a))}{=} (-1)^rH^{-1}M^rX = 0,$$

donc $HX \in \ker(M^r)$, démontrant la stabilité par H de $\ker(M^r)$.

Pour la stabilité du noyau de $Q(M)$, on note que si Q est un polynôme constant (nécessairement non nul par hypothèse) alors il n'y a rien à raconter, puisque dans ce cas $\ker(Q(M)) = \{0\}$ est évidemment stable par tout endomorphisme. Si Q n'est pas constant, alors par le théorème fondamental de l'algèbre il est scindé sur $\mathbb{C}$. Plus précisément, la relation $\chi_M = X^r Q$ indique que l'on a :

$$Q = \prod_{\lambda \in \mathrm{Sp}_{\mathbb{C}}(M) \setminus \{0\}} (X - \lambda)^{m_\lambda},$$

où les m_λ sont les ordres de multiplicité des valeurs propres λ. Par la question précédente, en regroupant chaque valeur propre avec son opposée qui a même ordre de multiplicité, on a :

$$Q = \prod_{\substack{\lambda \in \mathrm{Sp}_{\mathbb{C}}(M) \\ \mathrm{Re}(\lambda) > 0}} (X^2 - \lambda^2)^{m_\lambda}.$$

De cette égalité, il résulte que Q est un polynôme pair, et donc : $Q(-M) = Q(M)$. On en déduit que par la question 16.(a) on a : $HQ(M)H^{-1} = Q(M)$, et donc H et $Q(M)$ commutent et on en déduit que $\ker(Q(M))$ est stable par H : d'où le résultat.

17. **Deux applications linéaires : cas nilpotent.**
Nous allons appliquer le théorème de décomposition graduée. Comme $H^2 = \mathrm{I}_n$, et :

$$HMH^{-1} = -M = e^{\frac{2i\pi}{2}} M$$

avec M nilpotente, on peut appliquer ce théorème avec $N = 2$. Dans une même base convenable, les applications $X \mapsto MX$ et $X \mapsto HX$ ont respectivement pour matrices :

$$\mathrm{diag}\left(J_{r_1}, \ldots, J_{r_s}\right), \quad \text{et :} \quad \mathrm{diag}\left(D_{r_1,a_1}, \ldots, D_{r_s,a_s}\right),$$

avec $r_1, \ldots, r_s$ et $a_1, \ldots, a_s \in \{0, 1\}$ des entiers convenables. Les coefficients diagonaux sont une alternance de -1 et de 1 (commençant par -1 si $a_i = 1$, par 1 si $a_i = 0$).
Pour obtenir la décomposition de l'énoncé, nous allons faire un changement de base qui regroupe les 1 et les -1. Pour alléger la rédaction, nous nous contenterons de réduire simultanément J_n et $D_{n,1}$ avec n un entier naturel non nul : nous indiquerons brièvement comment traiter le cas de J_n et $D_{n,0}$ puis conviendrons que la réduction des matrices diagonales par blocs en découle immédiatement.
Soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$. Supposons d'abord que n est pair, de la forme $n = 2r$ avec r un entier non nul. Considérons la famille :

$$\mathcal{F} = \left(e_2, \ldots, e_{2r}, e_1, \ldots, e_{2r-1}\right).$$

C'est une base de $\mathbb{C}^n$, puisque nous n'avons fait que permuter les vecteurs de $\mathcal{B}$. On a par définition de $D_{r,1}$:

$$\forall i \in [\![1, r]\!], \quad D_{n,1}(e_{2i}) = 1, \quad D_{n,1}(e_{2i-1}) = -1.$$

Si l'on note P la matrice de passage de $\mathcal{B}$ dans $\mathcal{F}$, la formule du changement de base donne donc :

$$D_{n,1} = P \begin{pmatrix} \mathrm{I}_r & 0_r \\ 0_r & -\mathrm{I}_r \end{pmatrix} P^{-1}.$$

On a ici $s = r$ (qui vérifie bien sûr $|r - s| \leqslant 1$). De plus :

$$\forall i \in [\![1, r]\!], \quad J_n(e_{2i}) = \begin{cases} e_{2i+1} & \text{si } i < r, \\ 0 & \text{si } i = r, \end{cases} \qquad J_n(e_{2i-1}) = e_{2i}.$$

La formule du changement de base donne donc : $J_n = P\begin{pmatrix} 0_r & B_0 \\ A_0 & 0_r \end{pmatrix} P^{-1}$, avec : $A_0 = J_r$, et : $B_0 = \mathrm{I}_r$: c'est la troisième configuration proposée. D'où le résultat pour J_n et $D_{n,1}$ lorsque n est pair.

Supposons à présent que n est impair, de la forme $n = 2r+1$ avec r entier naturel. On considère cette fois-ci la base :

$$\mathcal{F} = (e_2, \dots, e_{2r}, e_1, \dots, e_{2r+1})\,.$$

Le même calcul donne : $D_{n,1} = P\begin{pmatrix} \mathrm{I}_r & 0_{r,r+1} \\ 0_{r+1,r} & -\mathrm{I}_{r+1} \end{pmatrix} P^{-1}$. De plus :

$$\forall i \in [\![1, r]\!],\ J_n(e_{2i}) = e_{2i+1}, \quad \text{et} : \quad \forall i \in [\![1, r+1]\!],\ J_n(e_{2i-1}) = \begin{cases} e_{2i} & \text{si } i < r+1, \\ 0 & \text{si } i = r+1. \end{cases}$$

La formule du changement de base donne donc : $J_n = P\begin{pmatrix} 0_r & B_0 \\ A_0 & 0_{r+1} \end{pmatrix} P^{-1}$, avec :

$$A_0 = \begin{pmatrix} 0 & \cdots & \cdots & 0 \\ 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathrm{M}_{r+1,r}(\mathbb{C}), \quad \text{et} : \quad B_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \in \mathrm{M}_{r,r+1}(\mathbb{C}).$$

C'est la quatrième configuration proposée. D'où le résultat en posant cette fois-ci $s = r+1$.

Le cas de la coréduction de J_n et $D_{n,1}$ est achevé. Voici comment adapter l'étude avec $D_{n,0}$:

- si n est pair, on prend $\mathcal{F} = (e_1, \dots, e_{2r-1}, e_2, \dots, e_{2r})$ et on obtient la deuxième configuration de l'énoncé ;
- si n est impair, on prend $\mathcal{F} = (e_1, \dots, e_{2r+1}, e_2, \dots, e_{2r})$ et on obtient la première configuration de l'énoncé.

Ceci conclut l'étude de cette question.

18. **Deux applications linéaires : cas inversible.**

 (a) On a : $M^2 = \begin{pmatrix} BA & 0_{m,n} \\ 0_{n,m} & AB \end{pmatrix}$, et donc : $\det(AB)\det(BA) = \det(M^2) \neq 0$. On en déduit que les matrices AB et BA sont inversibles et donc de rang maximal, n dans le premier cas et m dans le second. Or :

 $$\mathrm{rang}(AB) \leqslant \min(\mathrm{rang}(A), \mathrm{rang}(B)), \quad \mathrm{rang}(BA) \leqslant \min(\mathrm{rang}(A), \mathrm{rang}(B)).$$

 Si par exemple $n < m$, alors A et B sont de rang au plus n, et donc la deuxième inégalité donne $m \leqslant n$, ce qui est absurde. C'est la première inégalité qui fournit une contradiction si $m < n$, d'où l'égalité $m = n$. L'inversibilité de A et B découle alors de la multiplicativité du déterminant, puisque : $\det(A)\det(B) = \det(AB) \neq 0$.

 Autre démonstration que l'inversibilité de AB et BA implique celle de A et B. Puisque AB et BA sont inversibles, il existe $M \in \mathrm{M}_n(\mathbb{C})$ et $N \in \mathrm{M}_m(\mathbb{C})$ telles que : $ABM = \mathrm{I}_n$, et : $NBA = \mathrm{I}_m$. La première égalité implique l'existence d'un inverse de A à droite et la seconde celle d'un inverse de A à gauche. On en déduit que A admet un inverse, par ailleurs égal aux inverses à gauche et à droite, d'où le résultat.

 (b) Soit $P = \begin{pmatrix} \mathrm{I}_n & 0_n \\ 0_n & A \end{pmatrix}$, qui est inversible d'après la question précédente. On a :

 $$M = P\begin{pmatrix} 0_n & BA \\ \mathrm{I}_n & 0_n \end{pmatrix} P^{-1}, \quad \text{et} : \quad H = PHP^{-1},$$

Comme la relation « être simultanément semblable » est clairement une relation transitive, il suffit donc de démontrer que le couple $\left(\begin{pmatrix} 0_n & BA \\ \mathrm{I}_n & 0_n \end{pmatrix}, H\right)$ est simultanément semblable au couple suggéré dans l'énoncé pour conclure.

Notons N la matrice $\begin{pmatrix} 0_n & BA \\ \mathrm{I}_n & 0_n \end{pmatrix}$. Pour obtenir une base dans laquelle la matrice de $X \mapsto NX$ revêt la forme de l'énoncé, on remarque que si $(u_1, \ldots, u_{2r})$ est une famille libre donnant le bloc $\begin{pmatrix} 0_r & \lambda \mathrm{I}_r + J_r \\ \mathrm{I}_r & 0_r \end{pmatrix}$, alors on doit avoir $N^2 u_i = \lambda u_i + u_{i+1}$ pour tout $i < r$, $N^2 u_r = u_r$, et enfin $u_i = N u_{i-r}$ pour $i > r$: cela conduit à la recherche d'une réduction de Jordan de N^2. Comme : $N^2 = \begin{pmatrix} BA & 0_n \\ 0_n & BA \end{pmatrix}$, cela revient à chercher une réduction de Jordan de BA.

Faisons. En appliquant le théorème de réduction de Jordan (démontré à la question 9) aux endomorphismes induits par $X \mapsto (BA - \lambda \mathrm{I}_n)X$ sur les sous-espaces caractéristiques (ils sont effectivement nilpotents par définition même de ces sous-espaces), on a l'existence de $Q \in \mathrm{GL}_n(\mathbb{C})$ telle que :

$$BA = Q \mathrm{diag}\left(\lambda_1 \mathrm{I}_{r_1} + J_{r_1}, \ldots, \lambda_s \mathrm{I}_{r_s} + J_{r_s}\right) Q^{-1},$$

où les λ_i sont les valeurs propres de BA (avec répétitions éventuelles) et les r_i des entiers naturels non nuls convenables.

Notons $J = \mathrm{diag}\left(\lambda_1 \mathrm{I}_{r_1} + J_{r_1}, \ldots, \lambda_s \mathrm{I}_{r_s} + J_{r_s}\right)$. On vérifie par un calcul matriciel brut (bien sûr motivé par les observations ci-dessus) que l'on a :

$$N = \begin{pmatrix} Q & 0_n \\ 0_n & Q \end{pmatrix} \begin{pmatrix} 0_n & J \\ \mathrm{I}_n & 0_n \end{pmatrix} \begin{pmatrix} Q & 0_n \\ 0_n & Q \end{pmatrix}^{-1}, \quad H = \begin{pmatrix} Q & 0_n \\ 0_n & Q \end{pmatrix} H \begin{pmatrix} Q & 0_n \\ 0_n & Q \end{pmatrix}^{-1},$$

donc le couple (N, H) est simultanément semblable à $\left(\begin{pmatrix} 0_n & J \\ \mathrm{I}_n & 0_n \end{pmatrix}, H\right)$.

Pour enfin démontrer que $\left(\begin{pmatrix} 0_n & J \\ \mathrm{I}_n & 0_n \end{pmatrix}, H\right)$ est simultanément semblable à un couple de matrices diagonales par blocs tels que décrit dans l'énoncé : notons $(e_1, \ldots, e_{2n})$ la base canonique de $\mathbb{C}^{2n}$ et permutons les vecteurs de cette base ainsi :

$$\mathcal{F} = (e_1, \ldots, e_{r_1}, e_{n+1}, \ldots, e_{n+r_1}, e_{r_1+1}, \ldots, e_{r_1+r_2}, e_{n+r_1+1}, \ldots, e_{n+r_1+r_2}, \ldots).$$

La description des deux matrices du couple démontre que par la formule du changement de base, appliquée entre la base canonique et $\mathcal{F}$, on a :

$$\begin{pmatrix} 0_n & J \\ \mathrm{I}_n & 0_n \end{pmatrix} = R \,\mathrm{diag}\left(\begin{pmatrix} 0_{r_1} & \lambda_1 \mathrm{I}_{r_1} + J_{r_1} \\ \mathrm{I}_{r_1} & 0_{r_1} \end{pmatrix}, \ldots, \begin{pmatrix} 0_{r_s} & \lambda_s \mathrm{I}_{r_s} + J_{r_s} \\ \mathrm{I}_{r_s} & 0_{r_s} \end{pmatrix}\right) R^{-1},$$

et :

$$H = R \,\mathrm{diag}(\mathrm{I}_{r_1}, -\mathrm{I}_{r_1}, \mathrm{I}_{r_2}, \ldots, -\mathrm{I}_{r_2}, \ldots, \mathrm{I}_{r_s}, -\mathrm{I}_{r_s}) R^{-1}.$$

où R est la matrice de passage de la base canonique dans $\mathcal{F}$. Ceci achève de démontrer, par transitivité, que (M, H) est simultanément semblable à un couple de matrices diagonales par blocs dont les blocs sont respectivement de la forme $\begin{pmatrix} 0_r & \lambda \mathrm{I}_r + J_r \\ \mathrm{I}_r & 0_r \end{pmatrix}$ et $\begin{pmatrix} \mathrm{I}_r & 0_r \\ 0_r & -\mathrm{I}_r \end{pmatrix}$. D'où le résultat.

Remarque. Le sujet semble tronqué. Je pensais que la décomposition $\mathbb{C}^{m+n} = \ker(M^r) \oplus \ker(Q(M))$ de la question 16.(c) servait à traiter le cas général à l'aide du cas nilpotent (correspondant à l'étude des endomorphismes induits sur $\ker(M^r)$) et du cas inversible (de même sur $\ker(Q(M))$).