Université de Rennes 1
Préparation à l'agrégation de mathématiques
Auteur du document :

M. Coste

Mathématiques générales 1995

Corrigé : Michel Coste

Première partie : Spectre des matrices positives.

Les notions de positivité, et de réductibilité pour les matrices, sont invariantes par permutation des coordonnées. On s'autorisera donc de telles permutations pour se mettre dans des situations plus faciles à décrire.

On utilisera la notation $x \leq y$, où x et y sont des vecteurs de $\mathbf{R}^n$, pour dire que $x_i \leq y_i$ pour $i = 1, \ldots, n$. Ceci définit une relation d'ordre (non total) sur $\mathbf{R}^n$, compatible avec l'addition, et préservée par multiplication à gauche par une matrice carrée positive.

1.

(a) On a $z_i = y_i + \sum_{j=1}^n a_{i,j} y_j \geq y_i$. Donc $z_i \geq 0$ pour tout i, et si $y_i > 0$, alors $z_i > 0$. Supposons que y a exactement p coordonnées nulles, $0 < p < n$. On peut supposer que ces coordonnées sont les p premières : $y_1 = \ldots = y_p = 0$, et $y_{p+1} > 0, \ldots, y_n > 0$. Si $z_1 = \ldots = z_p = 0$, c'est que pour tout couple i, j avec $1 \leq i \leq p$ et $p + 1 \leq j \leq n$, on a $a_{i,j} = 0$ et donc A est réductible contrairement à l'hypothèse. En conclusion z est un vecteur positif, et le nombre de ses coordonnées nulles est 0, ou est strictement inférieur au nombre de coordonnées nulles de y (l'énoncé de la question est formulé incorrectement).

(b) Le résultat précédent entraîne immédiatement que $(I+A)^{n-1}(y)$ ne peut pas avoir de coordonnée nulle.

(c) L'application du (b) au j-ème vecteur de la base canonique de $\mathbf{C}^n$ montre que la j-ème colonne de $(I + A)^{n-1}$ a toutes ses coordonnées strictement positives.

2.

(a) Par définition, $\rho \leq r(x)$ si et seulement si, pour $i = 1, \ldots, n$, on a $x_i = 0$ ou $\rho x_i \leq (Ax)_i$. Donc $r(x)$ est le plus grand réel ρ tel que $\rho x \leq Ax$.

(b) La fonction $(Ax)_i/x_i$ est continue sur Q^+, et l'inf de n fonctions continues est une fonction continue.

(c)(i) L'image F du compact E par la fonction continue $(I + A)^{n-1}$ est compacte (et bien sûr non vide), et 1(b) montre qu'elle est contenue dans Q^+.

(c)(ii) Si $\rho x \leq Ax$, alors

$$\rho(I + A)x = \rho x + A(\rho x) \leq Ax + A^2 x = A(I + A)x$$

et donc $r(x) \leq r((I+A)x)$. Si $y = (I+A)^{n-1}x$, on obtient en itérant $n-1$ fois $r(x) \leq r(y)$.

(c)(iii) La fonction $x \mapsto r(x)$, continue sur le compact F (par (b) et (c)(i)), y atteint sa borne supérieure r : $r = r(w)$ pour un $w \in F$. Par (c)(ii), r majore $r(E)$. Comme on a clairement $r = r(w/\|w\|)$ et que $w/\|w\| \in E$, r est aussi le plus grand élément de $r(E)$.

On peut remarquer que r est aussi la plus grande valeur de $r(x)$ pour x vecteur positif non nul de $\mathbf{R}^n$. En effet il est clair que $r(x) = r(x/\|x\|)$, et $x/\|x\|$ appartient à E.

(c)(iv) Notons comme ci-dessus w un élément de F tel que $r(w) = r$. On sait que w a toutes ses coordonnées strictement positives, et pour montrer $r > 0$ il suffit de vérifier que

Aw a toutes ses coordonnées strictement positives. Si ce n'est pas le cas, on peut supposer que $(Aw)_1 = 0$ et alors la première ligne de A est nulle, ce qui contredit l'hypothèse que A est irréductible.

(d) On sait que $rz \leq Az$. Si z n'est pas vecteur propre de A, de valeur propre r, alors $Az - rz$ est un vecteur positif non nul, et donc

$$At - rt = (A - rI)(I + A)^{n-1}z = (I + A)^{n-1}(A - rI)z$$

a toutes ses coordonnées strictement positives par 1(b). Ceci entraîne $r(t) > r$, ce qui est impossible par définition de r vu que $t \in F$.

(e) D'après 2(d) on a $Az = rz$, d'où $(I + A)^{n-1}z = (1 + r)^{n-1}z$. Par 1(b) on obtient que $(1+r)^{n-1}z$ a toutes ses coordonnées strictement positives, et c'est aussi le cas pour z.

(f) De $\alpha y_i = \sum_{j=1}^n a_{i,j} y_j$ on déduit $|\alpha|\,|y_i| \leq \sum_{j=1}^n a_{i,j}\,|y_j|$, et donc $|\alpha|\,y_+ \leq Ay_+$. On a donc $|\alpha| \leq r(y_+) \leq r$.

(g) Soit y un vecteur propre de A de valeur propre r. Alors d'après ce que nous venons de voir $r \leq r(y_+) \leq r$, donc d'après (d) y_+ est vecteur propre de A de valeur propre r. D'après (e) y_+ a toutes ses coordonnées strictement positives, et y n'a aucune coordonnée nulle.

Soit maintenant z un autre vecteur propre de A de valeur propre r, et supposons qu'il est linéairement indépendant de y. Alors z aussi n'a aucune coordonnée nulle. On peut supposer $y_1 = z_1$, quitte à multiplier z par une constante non nulle. Alors $y - z$ est vecteur propre non nul de A de valeur propre r, et sa première coordonnée est nulle : contradiction.

Comme on sait déjà que r est valeur propre de A, la dimension du sous-espace propre associé est 1.

3. Soit z le vecteur propre de A de valeur propre r qui appartient à E (il est unique par 2(g)); toutes ses coordonnées sont strictement positives.

Supposons qu'il existe un vecteur propre $y \geq 0$, linéairement indépendant de z. Soit α la valeur propre associée à y. Puisque $\alpha y = Ay \geq 0$, α est forcément un réel positif ou nul, et on a $\alpha < r$ par 2(f) et (g)

On montre maintenant que toutes les coordonnées de y sont strictement positives. Sinon, quitte à permuter les coordonnées on a $y_1 = \ldots = y_p = 0$ et $y_{p+1} > 0, \ldots, y_n > 0$ avec $0 < p < n$. On doit avoir $(Ay)_1 = \ldots = (Ay)_p = 0$, d'où $a_{i,j} = 0$ pour $1 \leq i \leq p$ et $p+1 \leq j \leq n$, ce qui est contradictoire avec l'hypothèse que A est irréductible. (Remarquer que ce raisonnement fournit une variante pour 2(e).)

Quitte à multiplier y par une constante strictement positive et à permuter les coordonnées, on peut supposer que $z \leq y$ et que $z_1 = y_1$. Alors

$$\alpha y_1 = (Ay)_1 \geq (Az)_1 = rz_1 = ry_1,$$

d'où $\alpha \geq r$, ce qui est une contradiction.

4.

(a) Soit y un vecteur propre de B de valeur propre γ. De $\gamma y = By$ on obtient $|\gamma|\,y_+ \leq Ay_+$ (avec la notation de 2(f)), et donc $|\gamma| \leq r$.

(b) Si $|\gamma| = r$, alors, comme ci-dessus, $ry_+ \leq Ay_+$ d'où $r(y_+) = r$. D'après 2(d) et (e), y_+ est vecteur propre de A de valeur propre r, et il est strictement positif. Si B est positive, on a aussi $ry_+ \leq By_+$, et donc $Ay_+ \leq By_+$; vu que y_+ est strictement positif, ceci n'est possible que si $B = A$.

5. On sait déjà d'après 2(f) que $|\alpha| \leq r$. Supposons $|\alpha| = r$, et soit y un vecteur propre de A de valeur propre α. Alors, comme en 4(b), y_+ est un vecteur propre de A de valeur propre r, et on a

$$Ay_+ = ry_+ = (\alpha y)_+ = (Ay)_+.$$

On a donc

$$\sum_{j=1}^{n} a_{1,j}\,|y_j| = \left|\sum_{j=1}^{n} a_{1,j} y_j\right|.$$

Vu que tous les $a_{1,j}$ sont strictement positifs, ceci n'est possible que si tous les y_j ont même argument (modulo 2π), c.-à-d. s'écrivent $y_j = \rho_j e^{i\theta}$ avec $\rho_j > 0$. Alors $y = e^{i\theta} y_+$ et donc $\alpha = r$.

6.

(a) Si A est réductible, alors quitte à permuter les coordonnées on a

$$A = \begin{pmatrix} B & O \\ C & D \end{pmatrix}$$

où B et D sont carrées, et on vérifie facilement par récurrence que

$$A^p = \begin{pmatrix} B^p & O \\ C_p & D^p \end{pmatrix}$$

où C_p est une matrice de taille convenable; donc A^p est réductible. Si A^p est strictement positive, A^p est irréductible, et A aussi.

(b) Supposons $|\alpha| = r$. On sait que α^p est valeur propre de A^p, et que r^p est la valeur propre positive de module maximal de A^p. D'après 5 on en déduit $\alpha^p = r^p$. Si $\alpha \neq r$, le sous-espace propre pour A^p associé à la valeur propre r^p contient la somme directe des sous-espaces propres pour A associés aux valeurs propres α et r, et donc est de dimension strictement supérieure à 1, ce qui est contradictoire avec 2(g). Donc $\alpha = r$.

7.

(a) On commence par caractériser le fait que la matrice B est redondante ou décomposable d'une manière un peu plus maniable. On introduit les listes Λ et Γ d'indices de lignes et de colonnes respectivement. Alors B est redondante ou décomposable si et seulement s'il existe une permutation de Λ en $\Lambda' \cup \Lambda''$, et une permutation de Γ en $\Gamma' \cup \Gamma''$ (ici $\cup$ note la concaténation des listes) telles que ces permutations transforment la matrice B en

$$\begin{array}{c|c|c|} & \Gamma' & \Gamma'' \\ \hline \Lambda' & B' & O \\ \hline \Lambda'' & O & B'' \\ \hline \end{array} \quad ,$$

que Λ' et Γ' ne soient pas simultanément vides, de même que Λ'' et Γ''. (Remarquer que B est redondante quand une de ces quatre listes est vide).

On va maintenant exprimer, sur le même modèle, le fait que la matrice C est réductible. Comme C est symétrique, toute matrice obtenue par permutation des coordonnées à partir de C sera encore symétrique. Dire que C est réductible équivaut à dire qu'il existe une permutation de Λ en $\Lambda' \cup \Lambda''$, et une permutation de Γ en $\Gamma' \cup \Gamma''$ qui transforme

$$C = \begin{array}{c|c|c|} & \Lambda & \Gamma \\ \hline \Lambda & O & B \\ \hline \Gamma & {}^tB & O \\ \hline \end{array} \quad \text{en} \quad \begin{array}{c|c|c|c|c|} & \Lambda' & \Gamma' & \Lambda'' & \Gamma'' \\ \hline \Lambda' & O & B' & O & O \\ \hline \Gamma' & {}^tB' & O & O & O \\ \hline \Lambda'' & O & O & O & B'' \\ \hline \Gamma'' & O & O & {}^tB'' & O \\ \hline \end{array} \ ,$$

avec Λ' et Γ' non simultanément vides, de même que Λ'' et Γ''.

Il est clair maintenant que B est redondante ou décomposable si et seulement si C est réductible.

(b) Si $B\,{}^tB$ est réductible, on a une permutation de Λ en $\Lambda_1 \cup \Lambda_2$ avec Λ_1 et Λ_2 tous deux non vides, qui met $B\,{}^tB$ sous la forme

$$\begin{array}{c|c|c|} & \Lambda_1 & \Lambda_2 \\ \hline \Lambda_1 & A_1 & O \\ \hline \Lambda_2 & O & A_2 \\ \hline \end{array} \ .$$

Ceci nous dit que le produit scalaire de n'importe quelle ligne de B dans Λ_1 avec n'importe quelle ligne de B dans Λ_2 est nul. Comme les coefficients de B sont des réels positifs ou nuls, on en déduit une permutation de la liste des indices de colonnes Γ en $\Gamma_1 \cup \Gamma_2$ de telle sorte que les lignes de Λ_1 (resp. Λ_2) n'aient des coefficients non nuls que dans les colonnes de Γ_1 (resp. Γ_2). Si Γ_1 ou Γ_2 est vide, B est redondante, sinon elle est décomposable. Donc si B est indécomposable, $B\,{}^tB$ est irréductible; comme ${}^tB$ est également indécomposable, ${}^tB\,B$ est irréductible.

Posons $A = B\,{}^tB$. Puisque A est symétrique, toutes ses valeurs propres sont réelles, et A est diagonalisable sur $\mathbf{R}$. Toutes les valeurs propres de A sont positives ou nulles. En effet, si $x \in \mathbf{R}^n$ est un vecteur propre de A, de valeur propre α, alors

$$\alpha\,\|x\|^2 = {}^txAx = \|{}^tBx\|^2 \geq 0 \ .$$

Soit r la valeur propre maximale de A. Comme A est irréductible, on obtient d'après 2(f) que toutes les autres valeurs propres α vérifient $0 \leq \alpha < r$. On peut raisonner de la même façon pour ${}^tBB$.

Deuxième partie : Algèbres de matrices.

1.

(a) Un idéal bilatère J de M est un sous-groupe additif de M tel que pour tout x de J et tous y, z de M, on a $yxz \in J$. Si J est non nul, on peut choisir $x \neq 0$ dans J, avec un coefficient $x_{i,j} \neq 0$. Alors $x_{i,j}^{-1} E_{l,i} x Ej, l = E_{l,l}$ est dans J, et aussi la matrice identité qui est la somme des $E_{l,l}$. De là on obtient $J = M$.

(b) Si x est dans le centre de M, on a $E_{i,j}x = xE_{i,j}$, ce qui entraîne que $x_{i,j} = 0$ si $i \neq j$, et que $x_{i,i} = x_{j,j}$. Donc x est une matrice scalaire, et par ailleurs il est clair que toute matrice scalaire est dans le centre de M.

2.

(a) On a $\sum_{i=1}^n E_{i,i} = 1$, $E_{i,i}^2 = E_{i,i}$ et $E_{i,i}E_{j,j} = 0$ si $i \neq j$. Ces relations se transportent par ρ : chaque $\rho(E_{i,i})$ est un projecteur de V, d'image V_i, la somme des $\rho(E_{i,i})$ est l'identité, et si $j \neq i$, V_j est contenu dans le noyau de $\rho(E_{i,i})$. Tout vecteur $v \in V$ s'écrit $v = \sum_{i=1}^n \rho(E_{i,i})v$; par ailleurs si $v = \sum_{i=1}^n w_i$ avec $w_i \in V_i$, on trouve $\rho(E_{i,i})v = \rho(E_{i,i})w_i = w_i$. Ainsi tout vecteur de V s'écrit de manière unique comme somme de vecteurs de V_i, et $V = \bigoplus_{i=1}^n V_i$.

(b) Si $k \neq j$, on a $\rho(E_{i,j})\,\rho(E_{k,k}) = 0$ parce que $E_{i,j}E_{k,k} = 0$, et donc $\rho(E_{i,j})$ est nul sur V_k.

Comme $E_{i,j} = E_{i,i}E_{i,j}$, l'image de $\rho(E_{i,j})$ est contenue dans V_i. La restriction $\rho(E_{i,j})|_{V_j}$ est un isomorphisme de V_j sur V_i, d'inverse $\rho(E_{j,i})|_{V_i}$, parce que $E_{i,j}E_{j,i} = E_{i,i}$ et que $E_{j,i}E_{i,j} = E_{j,j}$.

(c)(i) Le vecteur $\rho(E_{i,1})e_k$ est un vecteur non nul de V_i. Comme les V_i sont en somme directe, la famille de ces vecteurs pour i variant de 1 à n est libre, et elle forme une base de l'espace W_k qu'elle engendre; celui-ci est donc de dimension n.

(c)(ii) Par définition, W_k est l'ensemble des vecteurs de la forme $\rho(y)e_k$ où y est une matrice de M dont toutes les colonnes sauf la première sont nulles. Pour n'importe quelle autre matrice x de M, le produit xy a encore la même propriété, et donc $\rho(x)$ envoie W_k dans W_k.

(c)(iii) On a $xE_{j,1} = \sum_{i=1}^n x_{i,j}E_{i,1}$ et donc

$$\rho_k(x)(\rho(E_{j,1})e_k) = \sum_{i=1}^n x_{i,j}\rho(E_{i,1})e_k.$$

Ceci montre que la matrice de $\rho_k(x)$ dans la base de (c)(i) est x.

(c)(iv) En mettant ensemble les bases des W_k décrites au (c)(i), on obtient la réunion des bases des V_i, puisque les $\rho(E_{i,1})$ induisent des isomorphismes de V_1 sur V_i. Comme ceci fait une base de V, c'est que V est la somme directe des W_k.

(c)(v) La matrice de $\rho(x)$ dans la base que l'on vient de former est la matrice diagonale par blocs :

$$\begin{pmatrix} x & 0 & \dots & 0 \\ 0 & x & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & x \end{pmatrix}.$$

Les blocs hors de la diagonale sont 0 par (c)(ii) et ceux sur la diagonale sont x par (c)(iii).

(d) On applique la question 2 avec $V = \mathbf{C}^m$, et $End(V)$ canoniquement isomorphe à $M_m(\mathbf{C})$. Le résultat 2(c)(v) montre que $\rho(x) = 0$ entraîne $x = 0$, et donc que ρ est injectif. Le résultat 2(c)(iv) montre que $m = nd$, un multiple de n.

3.

(a) L'écriture matricielle par blocs de l'égalité $\rho(x)A = A\rho(x)$ nous donne que $xA_{i,j} = A_{i,j}x$ pour tout (i,j). Donc A commute avec $\rho(M)$ si et seulement si les $A_{i,j}$ sont dans le centre de M, c.-à-d. d'après 1(b) si et seulement si les $A_{i,j}$ sont des matrices scalaires.

(b) Dans la situation ci-dessus, on pose $A_{i,j} = a_{i,j}I_n$. L'application qui à une matrice A commutant avec $\rho(M)$ associe la matrice de coefficients $a_{i,j}$ est, d'après les règles de calcul par blocs sur les matrices, clairement un isomorphisme d'algèbres avec unité de $\rho(M)'$ sur $M_c(\mathbf{C})$.

Appelons $\sigma : M_d(\mathbf{C}) \to End(V)$ le composé de l'isomorphisme inverse avec l'inclusion dans $End(V)$. On peut appliquer à σ tous les résultats obtenus pour ρ, en inversant bien sûr les rôles de n et d. En particulier, on sait que l'ensemble $\rho(M)''$ des endomorphismes de V qui commutent avec $\rho(M)'$ (l'image de σ) est isomorphe à l'algèbre de matrices $M_n(\mathbf{C})$, et donc de dimension n^2 comme espace vectoriel sur $\mathbf{C}$. Comme il est clair que $\rho(M)''$ contient $\rho(M)$, il doit être égal à $\rho(M)$.

4. Contrairement à ce que laisse penser l'énoncé, les i_j ne sont pas des morphismes d'algèbres avec unité car $i_j(1) = p_j \neq 1$. Les π_j, eux, sont bien des morphismes d'algèbres avec unité.

(a) Evident.

(b) L'élément $(a_1, \ldots, a_m)$ est dans le centre de N si et seulement si chacun des a_i est dans le centre de A_i, c.-à-d. si et seulement si chaque a_i est une matrice scalaire. Le centre de N est donc isomorphe à $\mathbf{C}^m$ comme algèbre avec unité.

(c) Les seuls scalaires idempotents sont 0 et 1. Donc les idempotents centraux de N sont les éléments dont les composantes sont soit 0 soit I_j. Ce sont les sommes finies de p_j (y compris 0). On a une bijection de l'ensemble des idempotents centraux de N sur l'ensemble des parties de $\{1, \ldots, m\}$ qui consiste à associer à un idempotent central p l'ensemble des j tels que la $\pi_j(p) = I_j$. Si on définit, pour des idempotents centraux p et q,

$$p \cap q = pq \qquad \text{et} \qquad p \cup q = p + q - pq,$$

alors cette bijection devient un isomorphisme d'algèbres de Boole.

(d) Il faut préciser par rapport à l'énoncé qu'un idempotent central minimal doit être *non nul*. Par la bijection entre idempotents centraux et parties de $\{1, \ldots, m\}$, il est clair qu'un idempotent central minimal correspond à une partie non vide minimale, c.-à-d. à un singleton. Les idempotents centraux minimaux sont donc les p_j pour $j = 1, \ldots, m$.

5.

(a) Le raisonnement pour les p_j, en utilisant 4(a), est le même que celui pour les $E_{i,i}$ au 2(a).

(b) Si $k \neq j$, $yp_k = 0$ et donc y agit par 0 sur W_k. Comme $p_j y = y$, y envoie W dans W_j, et donc W_j dans lui-même.

(c) L'application $\rho : A_j \to End(W_j)$ est un morphisme d'algèbres avec unité. La seule chose à vérifier est que ρ envoie unité sur unité, et ceci est vrai parce que p_j agit comme l'identité sur W_j. On peut donc appliquer tous les résultats de 2, en particulier 2(c)(v).

(d) Puisque les p_j sont dans le centre de N, on a $\rho(p_j)C(N)\rho(p_j) \subset C(N)$. Soit $u \in C(N)$. Puisque u commute avec les $\rho(p_j)$ on a

$$\sum_{j=1}^{m} \rho(p_j)u\rho(p_j) = u\sum_{j=1}^{m} \rho(p_j)^2 = u.$$

Si on a une autre décomposition $u = \sum_{j=1}^{m} \rho(p_j)u_j\rho(p_j)$ avec $u_j \in C(N)$, en multipliant à droite et à gauche par $\rho(p_j)$ on trouve $\rho(p_j)u\rho(p_j) = \rho(p_j)u_j\rho(p_j)$. Au total $C(N)$ est la somme directe des $\rho(p_j)C(N)\rho(p_j)$.

(e) $\rho(p_j)\, End(W)\rho(p_j)$ s'identifie à $End(W_j)$ puisque $\rho(p_j)$ est un projecteur sur W_j, et cette identification envoie $\rho(p_j)C(N)\rho(p_j)$ sur $\rho(A_j)'$. Ceci montre d'après (d) que $C(N)$ est $\bigoplus_{j=1}^{m} \rho(A_j)'$. On conclut grâce à 3(b) que $C(N)$ est isomorphe à $\bigoplus_{j=1}^{m} M_{d_j}(\mathbf{C})$.

(f) Puisque $C(N)$ contient les $\rho(p_j)$, tout élément u de $C(N)'$ commute avec les projecteurs $\rho(p_j)$ et se décompose donc de manière unique comme $u = \sum_{j=1}^{m} u_j p_j$ (avec un petit abus de notation), où u_j est un endomorphisme de W_j qui commute avec $\rho(A_j)'$, et ceci montre que $C(N)'$ est $\bigoplus_{j=1}^{m} \rho(A_j)''$. En utilisant la deuxième partie de 3(b) on voit que $C(N)'$ est $\bigoplus_{j=1}^{m} \rho(A_j) = \rho(N)$.

6.

(a)(i) q est la matrice d'un projecteur sur un sous-espace vectoriel V de $\mathbf{C}^n$, et qAq est isomorphe à $End(V)$ et donc à $M_p(\mathbf{C})$ où p est la dimension de V. Le même argument vaut pour qBq; en utilisant la description de 2(c)(v) on voit que le rang de $\rho(q)$ est dp où $d = m/n$, et qBq est isomorphe à $M_{dp}(\mathbf{C})$.

(a)(ii) Il est clair que $qC(A)q$ commute à qAq. Le commutant de qAq dans qBq est isomorphe à $M_d(\mathbf{C})$ d'après 3(b). En se plaçant dans la situation de 3 on voit que $qC(A)q$ est de dimension d^2 sur $\mathbf{C}$, et donc $qC(A)q$ est le commutant de qAq dans qBq. Il ressort aussi de cet argument que l'homomorphisme $x \mapsto qxq$ de $C(A)$ sur $qC(A)q$ est un isomorphisme.

(b)(i) On peut échanger les rôles de A et de $C(A)$ d'après 3(b), et donc la remarque que l'on vient de faire montre que si q est un idempotent de $C(A)$ alors $x \mapsto qxq$ donne un isomorphisme d'algèbres avec unité de A sur qAq.

(b)(ii) qAq, qBq et $qC(A)q$ sont respectivement isomorphes à des algèbres de matrices $n \times n$, $pn \times pn$ et $p \times p$ respectivement. Le commutant de qAq dans qBq est donc isomorphe à une algèbre de matrices $p \times p$ d'après 3, et comme il contient visiblement $qC(A)q$, c'est $qC(A)q$ pour des raisons de dimension.

Troisième partie : Normes des matrices à coefficients entiers.

1.

(a) Soient $\mu_1, \ldots, \mu_l$ les racines de P. On a $a_k = \sigma_k(\mu_1, \ldots, \mu_l)$, et donc a_k est somme de $\binom{l}{k}$ termes tous de module inférieur ou égal à 1. Donc $|a_k| \leq \binom{l}{k}$.

(b) Puisque les coefficients ne peuvent prendre qu'un nombre fini de valeurs d'après (a), l'ensemble des polynômes de U de degré l dont toutes les racines sont de module inférieur ou égal à 1 est fini.

(c)(i) Les coefficients de P_k sont des polynômes symétriques à coefficients entiers en les racines μ_i de P, et donc ce sont des polynômes à coefficients entiers en les coefficients a_k. Ils sont entiers.

(c)(ii) Les racines μ_i^k de P_k sont de module inférieur ou égal à 1. D'après (b), les P_k apartiennent à un ensemble fini. Il existe donc deux entiers strictement positifs $j < k$ tels que $P_j = P_k$.

(c)(iii) Soient j et k comme ci-dessus. On a donc une permutation τ des indices $i \in \{1, \ldots, l\}$ telle que $\mu_i^j = \mu_{\tau(i)}^k$. Si l'orbite de i sous τ a λ éléments, on en déduit que $\mu_i^{j^\lambda} = \mu_i^{k^\lambda}$. Il y a deux possibilités : ou bien $\mu_i = 0$, ou bien $\mu_i^{k^\lambda - j^\lambda} = 1$, et donc μ est une racine de l'unité (l'énoncé oublie la possibilité de racines nulles).

(d) Si on pose $Q(X) = X^l P(X + \frac{1}{X})$, alors Q est un polynôme à coefficients entiers de degré $2l$. Les racines de Q sont des nombres complexes de module 1. En effet de $y = x + \frac{1}{x}$ on tire $x^2 - xy + 1 = 0$. Quand y est réel et dans $[-2, 2]$, le discriminant $y^2 - 4$ est négatif ou nul, et les deux solutions en x sont confondues ou complexes conjuguées, de produit 1. Comme Q n'a pas de racine nulle, on peut déduire de (c) que les racines de Q sont des racines de l'unité, de la forme $e^{2i\pi r}$, où r est rationnel. Alors les racines de P sont de la forme $e^{2i\pi r} + e^{-2i\pi r} = 2\cos(2\pi r)$.

(e)(i) ω et ρ ont même polynôme minimal sur $\mathbf{Q}$, à savoir le polynôme cyclotomique d'ordre n (le polynôme unitaire à coefficients entiers qui a pour racines les racines primitives n-èmes de l'unité, et qui est irréductible). Donc il existe un unique isomorphisme $\mathbf{Q}$-linéaire de $\mathbf{Q}(\omega)$ sur $\mathbf{Q}(\rho)$ qui envoie ω sur ρ. Enfin, comme ρ est une puissance de ω et vice-versa, on a $L = \mathbf{Q}(\omega) = \mathbf{Q}(\rho)$.

(e)(ii) Si P a la racine $2\cos(2\pi\frac{p}{q})$, alors (avec les notations de (d)), Q a la racine $e^{2i\pi\frac{p}{q}}$, qui est une racine primitive q-ème de l'unité. Donc Q est divisible par le polynôme cyclotomique d'ordre q, et il a aussi pour racine $e^{\frac{2i\pi}{q}}$. Ainsi P a pour racine $2\cos(\frac{2\pi}{q})$. En fait cet argument montre que P a pour racine tous les $2\cos(2\pi\frac{p'}{q})$ où p' est premier avec q.

(e)(iii) On sait déjà, d'après (d) et (e)(ii) et le fait que ni 2 ni -2 ne sont racines de P, qu'il existe un entier $q > 2$ tel que

$$\max\{|\lambda_j|,\ j = 1, \ldots, l\} = \max\{2\,|\cos(2\pi\frac{p}{q})|\ ,\ p \text{ premier avec } q\},$$

Si $q = 2q'$ est pair, le maximum est atteint pour $p = 1$, il vaut $2\cos(\pi/q')$ et on a nécessairement $q' \geq 3$ car ce maximum doit être non nul. Si $q = 2q' + 1$ est impair, le maximum est atteint pour $p = q'$, et il vaut $-2\cos(2\pi q'/(2q' + 1)) = 2\cos(\pi/q)$, avec $q \geq 3$.

2.

(a) La norme d'un vecteur vaut le maximum des produits scalaires de ce vecteur avec tous les vecteurs de norme 1, donc

$$\|B\| = \max\{{}^t yBx,\ \|y\| = \|x\| = 1\},$$

et ce maximum est bien atteint parce que x et y appartiennent à des compacts et que la fonction $(x, y) \mapsto {}^t yBx$ est continue. Comme ${}^t yBx = {}^t x\, {}^t By$, on voit immédiatement que $\|B\| = \|{}^t B\|$.

Comme

$$C \begin{pmatrix} y \\ x \end{pmatrix} = \begin{pmatrix} Bx \\ {}^t By \end{pmatrix},$$

on a, en posant $z = \begin{pmatrix} y \\ x \end{pmatrix}$

$$\|Cz\|^2 = \|Bx\|^2 + \|{}^t By\|^2 \leq \|B\|^2 \|x\|^2 + \|{}^t B\|^2 \|y\|^2 = \|B\|^2 \|z\|^2.$$

On en déduit $\|C\| \leq \|B\|$, et on obtient l'égalité en choisissant pour z un vecteur de norme 1 tel que $\|Bx\| = \|B\|\,\|x\|$ et que $\|{}^t By\| = \|{}^t B\|\,\|y\|$.

La norme de $B\,{}^t B$ est le maximum des ${}^t y' B\, {}^t By$ pour y et y' de norme 1. Si ce maximum est réalisé par ${}^t y' B\, {}^t By$, il l'est aussi par ${}^t yB\, {}^t By = \|{}^t By\|^2$ et par $\|{}^t By'\|^2$, puisque l'on a

$$\|{}^t By\|^2 + \|{}^t By'\|^2 - 2\,{}^t y' B\, {}^t By = \|{}^t B(y - y')\|^2 \geq 0.$$

Comme le maximum des $\|{}^t By\|^2$ pour y de norme 1 est $\|{}^t B\|^2$, on a bien $\|B\,{}^t B\| = \|{}^t B\|^2$, et de même $\|{}^t BB\| = \|B\|^2$.

(b) La matrice C est symétrique, elle se diagonalise dans une base orthonormale, et ceci rend clair le fait que $\|B\| = \|C\|$ est la plus grande valeur absolue de valeur propre de C. Si B est à coefficients entiers, C aussi et donc le polynôme caractéristique P de C est un polynôme à coefficients entiers. Le maximum des valeurs absolues de racines de P est $\|B\|$. Donc ou bien $\|B\| \geq 2$, ou bien $B = 0$ et $\|B\| = 2\cos(\frac{\pi}{2})$, ou bien d'après 1 on a $\|B\| = 2\cos(\frac{\pi}{q})$ où q est un entier supérieur ou égal à 3.

Quatrième partie : Indices d'inclusions.

1. Si $z \in C$ commute avec $\tau(B)$, il commute a fortiori avec $\tau(\rho(A))$. Donc $\tau(B)'$ est une sous-algèbre de $(\tau \circ \rho(A))'$.

D'après le 3 de la deuxième partie, $\tau(B)'$ (resp. $(\tau \circ \rho(A))'$) est isomorphe à une algèbre de matrices de taille f/m (resp. f/n), et donc

$$[(\tau \circ \rho(A))' : \tau(B)'] = \left(\frac{f/m}{f/n}\right)^2 = \left(\frac{n}{m}\right)^2 = [B : A].$$

2.

(a) Tout d'abord, $p_i q_j \in B_i$ car $B_i = p_i B$. Puisque p_i est dans le centre de B, on a $(p_i q_j)^2 = p_i^2 q_j^2 = p_i q_j$, donc $p_i q_j$ est bien un idempotent de B_i. Les $p_i q_j$ pour $j = 1, \ldots, s$ sont des idempotents deux à deux orthogonaux de somme l'unité de B_i.

(b) On a $S_{ij} = p_i q_j B_i p_i q_j$ et donc S_{ij} est isomorphe à une algèbre de matrices d'après le (a) et le 6 de la deuxième partie.

L'application $A_j \to S_{ij}$ qui envoie x sur $p_i x p_i = p_i q_j x p_i q_j$ est un homorphisme d'algèbres avec unité, et est donc injectif d'après le 2 de la deuxième partie. Il induit donc un isomorphisme de A_j sur son image, qui est R_{ij}.

(c) On peut décrire λ_{ij} d'une autre façon. On identifie A_j à $End(U_j)$ et B_i à $End(V_i)$. Alors $p_i q_j$ est un projecteur de V_i d'image V_{ij}, et on a $\dim(V_{ij}) = \lambda_{ij} \dim(U_j)$. Ceci est clair car V_{ij} est nul si $p_i q_j = 0$, et sinon S_{ij} s'identifie à $End(V_{ij})$. On a de plus $V_i = \bigoplus_{j=1}^r V_{ij}$.

Si la i-ème ligne de Λ_R^S est nulle, alors $p_i = \sum_{j=1}^r p_i q_j = 0$ et ceci n'est pas. De même la j-ème colonne de Λ_R^S n'est pas nulle car $q_i \neq 0$.

(d) On a $Z(R) = \bigoplus_{j=1}^r q_j \mathbf{C} q_j$ et $Z(S) = \bigoplus_{i=1}^s p_i \mathbf{C} p_i$ (voir le 4(b) de la deuxième partie). Un élément de $Z(R) \cap Z(S)$ s'écrit de manière unique $\sum_{j=1}^r q_j z_j$ où les z_j sont des nombres complexes, et aussi de manière unique $\sum_{i=1}^s p_i w_i$ où les w_i sont des nombres complexes. En multipliant par p_i on obtient $\sum_{j=1}^r p_i q_j z_j = p_i w_i$, et en lisant cette égalité dans B_i on obtient $z_j = w_i$ chaque fois que $\lambda_{ij} \neq 0$. Donc $Z(R) \cap Z(S)$ n'est pas réduit à $\mathbf{C}$ si et seulement si on peut trouver deux partitions $\{1, \ldots, r\} = C_1 \cup C_2$ et $\{1, \ldots, s\} = L_1 \cup L_2$, aucun des C_1, C_2, L_1, L_2 n'étant vide, tel que $\lambda_{i,j} = 0$ quand $i \in L_1$ et $j \in C_1$, ou quand $i \in L_2$ et $j \in C_2$, c.-à.-d. si et seulement si Λ_R^S est décomposable. Vu que Λ_R^S ne peut pas être redondante d'après (c), on voit que Λ_R^S est indécomposable si et seulement si $Z(R) \cap Z(S) = \mathbf{C}$.

(e) On reprend les notations introduites au début de la réponse au (c). On identifie T à $\bigoplus_{h=1}^t End(W_h)$, et on note r_h l'image de l'identité de $End(W_h)$ dans T. Les images des projecteurs $r_h q_j$, $r_h p_i$, $r_h p_i q_j$ de W_h sont notées respectivement W_{hj}, W'_{hi}, W_{hij}. On a $End(W_{hj}) = r_h q_j T r_h q_j = T_{hj}$ et $End(W'_{hi}) = r_h p_i T r_h p_i = T'_{hi}$. Les coefficients de Λ_S^T sont les λ'_{hi} tels que $\dim(W'_{hi}) = \lambda'_{hi} \dim(V_i)$. En appliquant le résultat du 6 de la deuxième partie au morphisme $B_i \to T'_{hi}$ et à l'idempotent $p_i q_j$ de B_i, et en remarquant que $p_i q_j T'_{hi} p_i q_j = End(W_{hij})$, on obtient que $\dim(W_{hij}) = \lambda'_{hi} \dim(V_{ij})$. Puisque $W_{hj} = \bigoplus_{i=1}^s W_{hij}$, on a

$$\dim(W_{hj}) = \sum_{i=1}^s \lambda'_{hi} \dim(V_{ij}) = \sum_{i=1}^s \lambda'_{hi} \lambda_{ij} \dim(U_j).$$

Ceci établit l'égalité $\Lambda_R^T = \Lambda_R^S \Lambda_S^T$.

(f) Puisque R est contenu dans S il est clair que $C(S)$ est une sous-algèbre de $C(R)$. Notons μ_{ji} les coefficients de la matrice d'indice pour l'inclusion de $C(S)$ dans $C(R)$. D'après le 5 de la deuxième partie, on a $C(R) = \bigoplus_{j=1}^r q_j C(R) q_j$ et $C(S) = \bigoplus_{i=1}^s p_i C(S) p_i$. Si $q_j p_i = 0$, alors $\mu_{ji} = 0 = \lambda_{ij}$. Si $q_j p_i \neq 0$, alors par définition dela matrice d'indice

$$\mu_{ji} = [q_j p_i C(R) q_j p_i : q_j p_i C(S) q_j p_i] \, .$$

Comme $q_j p_i$ est un idempotent non nul de $C(R)$, alors d'après le 6(b) de la deuxième partie $q_j p_i C(R) q_j p_i$ est le commutant de $R_{ij} = q_j p_i R q_j p_i$ dans $q_j p_i F q_j p_i$. Comme $q_j p_i$ est un idempotent non nul de S, alors d'après le 6(a) de la deuxième partie $q_j p_i C(S) q_j p_i$ est le commutant de $S_{ij} = q_j p_i S q_j p_i$ dans $q_j p_i F q_j p_i$. Donc d'après 1 on a $\mu_{ji} = [S_{ij} : R_{ij}] = \lambda_{ij}$. Au total, la matrice d'indice pour l'inclusion de $C(S)$ dans $C(R)$ est bien la transposée de Λ_R^S.

3.

(a) Tout est clair; l'injectivité de λ vient de $x = \lambda(x)1$. De même ρ est injectif.

(b) $End_R(S)$ est le commutant de la sous-algèbre $\rho(R)$ dans F. Comme $\rho(R)$ est antiisomorphe à l'algèbre R qui est une somme directe d'algèbre de matrices, $\rho(R)$ est isomorphe à une somme directe d'algèbre de matrices. En effet, il suffit de composer avec l'antiisomorphisme de R sur elle-même qui est induit par la transposition sur chacune des algèbres de matrices facteurs de R. D'après le 5(e) de la deuxième partie, $End_R(S)$ est isomorphe à une somme directe d'algèbres de matrices. Il est clair que $End_R(S)$ contient $\lambda(S)$.

(c) Le commutant $C(\rho(S))$ de $\rho(S)$ dans F est $\lambda(S)$. L'inclusion $\lambda(S) \subset \rho(S)$ est claire. Si $f \in F$ commute à $\rho(S)$, alors

$$\forall x \in S \quad f(x) = f(\rho(x)1) = \rho(x)f(1) = f(1)x = \lambda(f(1))x \ ,$$

et donc $f = \lambda(f(1)) \in \lambda(S)$. D'après 2(f), la matrice d'indice pour l'inclusion de $\lambda(S)$ dans $End_R(S)$ est la transposée de la matrice d'indice pour l'inclusion de $\rho(R)$ dans $\rho(S)$. Comme ρ est un antihomomorphisme injectif, cette dernière matrice d'indice est la même que Λ_R^S.

4.

(a) D'après 3(c) la matrice d'indice pour l'inclusion de S_{2k} dans S_{2k+1} (resp. S_{2k+1} dans S_{2k+2}) est Λ (resp ${}^t\Lambda$). Donc d'après 2(e) la matrice d'indice pour l'inclusion de S_0 dans S_{2k} (resp. S_{2k+1}) est $({}^t\Lambda\Lambda)^k$ (resp. $\Lambda\,({}^t\Lambda\Lambda)^k$).

(b) L'hypothèse que $Z(R) \cap Z(S) = \mathbf{C}$ entraîne d'après 2(d) que Λ est indécomposable. D'après le 7(b) de la première partie, si $A = \Lambda\,{}^t\Lambda$ ou ${}^t\Lambda\,\Lambda$, alors A est une matrice irréductible symétrique à valeurs propres positives ou nulles, et telle que l'espace propre associé à la plus grande valeur propre r soit de dimension 1.

(c) On sait d'après la première partie que l'espace propre associé à la valeur propre maximale r de A est engendré par un vecteur strictement positif z, que l'on peut prendre de norme 1. Alors $P_0(y) = (y \cdot z)z$ est un vecteur strictement positif car $y \cdot z > 0$. L'espace propre $\mathbf{R}z$ et son orthogonal $z^\perp$ sont stables par A, on a $r = \|A\|$, et il existe un réel positif ou nul $s < r$ tel que pour tout $w \in z^\perp$ on a $\|Aw\| \leq s\|w\|$; on peut prendre pour s la plus grande valeur propre de A après r. On obtient ainsi

$$\left\| \frac{A^k}{\|A\|^k}\, y - P_0(y) \right\| = \left\| \frac{A^k}{\|A\|^k}\, (y - P_0(y)) \right\| \leq \left(\frac{s}{r}\right)^k \|y - P_0(y)\| \ ,$$

ce qui montre que $\frac{A^k}{\|A\|^k}\, y$ converge vers $P_0(y)$.

(d) D'après ce qui précède, comme $P_0 y$ est non nul, on sait que $\ln\|A^k y\| - k \ln\|A\|$ converge vers $\ln\|P_0 y\|$, donc $\frac{1}{k}\ln\|A^k y\|$ converge vers $\ln\|A\|$, et donc

$$\lim_{k\to+\infty} \|Ay\|^{\frac{1}{k}} = \|A\| = \|\Lambda\|^2 \ ,$$

la dernière égalité venant du 2(a) de la troisième partie.

(e) Considérons, comme dans 2, $R = \bigoplus_{j=1}^{r} End(U_j)$ et $S = \bigoplus_{i=1}^{s} End(V_i)$. Soit q_j l'image de l'identité de U_j dans R, p_i l'image de l'identité de V_i dans S. La dimension de S est la somme des carrés des dimensions des V_i. On avait vu au 2 que $\dim(V_i) = \sum_{j=1}^{r} \lambda_{ij} \dim(U_i)$ où les λ_{ij} sont les coefficients de la matrice d'indice Λ pour l'inclusion de R dans S. Soit y le vecteur (strictement positif) des $\dim(U_i)$. On a donc $\dim(S) = \|\Lambda y\|^2$. On a de même

$$\dim(S_{2k}) = \|({}^t\Lambda\Lambda)^k y\|^2$$
$$\dim(S_{2k+1} = \|(\Lambda\,{}^t\Lambda)^k \Lambda y\|^2 \ .$$

Ces deux égalités et le (d) montrent que

$$\lim_{k\to+\infty} (\dim(S_k))^{\frac{1}{k}} = \|\Lambda\|^2.$$

D'après le 2 de la troisième partie, et le fait que Λ n'est pas nulle, cette limite est soit de la forme $4\cos^2(\pi/q)$ou q est un entier supérieur ou égal à 3, soit supérieure ou égale à 4.