Corrigé de la première épreuve
Agrégation interne 2008

Michel Coste
Université de Rennes 1*

Ce document provient de la préparation à l'agrégation de mathématiques de l'Université de Rennes 1:

`http://agreg-maths.univ-rennes1.fr`

Notations

On désigne par $\mathbb{C}$ le corps des nombres complexes.

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. On désigne par E^* l'espace vectoriel dual de E. On désigne par $\mathrm{End}(E)$ *l'algèbre des endomorphismes de E et par* $\mathrm{GL}(E)$ *le groupe des endomorphismes inversibles de E. On note $\mathbf{1}_E$ l'application identique de E.*

Si u est un endomorphisme de E, on note ${}^t u$ l'endomorphisme de E^* transposé de u ; si X est une partie de $\mathrm{End}(E)$*, on note ${}^t X$ l'ensemble des transposés des éléments de X.*

Soit u une application linéaire d'un espace vectoriel E dans un espace vectoriel F et soit x un vecteur de E. Pour alléger les notations, il nous arrivera d'écrire ux pour désigner l'image $u(x)$ du vecteur x par l'application u.

Soit n un entier ≥ 1 ; on désigne par $\mathrm{M}_n(\mathbb{C})$ *l'algèbre des matrices carrées complexes à n lignes et n colonnes. On note $E_{i,j}$ la matrice de* $\mathrm{M}_n(\mathbb{C})$ *dont tous les coefficients sont nuls excepté celui de la i-ème ligne et j-ème colonne qui est égal à 1. Oit note* $\mathrm{GL}(n.\mathbb{C})$ *le groupe des matrices inversibles et $\mathbf{1}_n$ la matrice unité de* $\mathrm{M}_n(\mathbb{C})$*.*

Soient $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{C}$-algèbres possédant chacune, un élément unité ; un morphisme unitaire d'algèbres de $\mathcal{A}$ dans $\mathcal{B}$ est une application $\mathbb{C}$-linéaire qui préserve les produits et les éléments unités.

Les deux premières parties sont indépendantes. La sixième partie est indépendante des précédentes.

Partie I

1) *Soit W un $\mathbb{C}$-espace vectoriel de dimension finie. Soient $p_1, \ldots, p_n$ des endomorphismes de W. Pour $i = 1, \ldots, n$, on note W_i l'image de p_i.*

Démontrer que les conditions suivantes sont équivalentes :

(i) L'espace vectoriel W est somme directe des sous-espaces W_i et, pour $i = 1, \ldots, n$, p_i est le projecteur d'image W_i parallèlement à la somme directe des W_j, $j \neq i$.

(ii) Pour $i = 1, \ldots, n,$, on a ${p_i}^2 = p_i$; pour $j \neq i$,on a $p_i\, p_j = 0$; et on a $p_1 + \cdots + p_n = 1_W$.

*remarques et questions bienvenues à `michel.coste@univ-rennes1.fr`

Supposons (i). Puisque p_i est un projecteur on a ${p_i}^2 = p_i$. Si $j \neq i$, l'image de p_j est contenue dans le noyau de p_i et donc $p_i\, p_j = 0$. Enfin tout vecteur $x \in W$ se décompose de manière unique en $x = y_1 + \cdots + y_n$ avec $y_i \in W_i$, et on a $y_i = p_i\, x$; ceci montre que $\mathbf{1}_w = p_1 + \cdots + p_n$.

Supposons (ii). L'égalité ${p_i}^2 = p_i$ veut dire que p_i est un projecteur d'image W_i, et l'égalité $p_i\, p_j = 0$ veut dire que W_j est contenu dans le noyau de p_i pour $j \neq i$. Puisque pour tout $x \in W$ on a $x = p_1\, x + \cdots + p_n\, x$, W est la somme $W_1 + \cdots + W_n$. Cette somme est directe puisque si $0 = y_1 + \cdots + y_n$ avec $y_i \in W_i$, alors pour tout i on a $y_i = p_i(y_1 + \cdots + y_n) = 0$. Enfin la somme directe des W_j pour $j \neq i$ est contenue dans le noyau de p_i, et elle est égale à ce noyau puisque sa dimension est égale à la dimension $\dim w - \dim W_i$ du noyau.

2) *Soit toujours W un $\mathbb{C}$-espace vectoriel de dimension finie, soit n un entier ≥ 1 et suit $\rho : \mathrm{M}_n(\mathbb{C}) \to \mathrm{End}(W)$ un morphisme unitaire d'algèbres.*

a) *Pour $i = 1, \ldots, n$, on note p_i l'endomorphisme $\rho(E_{i,i})$. Démontrer que les endomorphismes p_i satisfont à la condition (ii) de la question (I.1).*

On a clairement $E_{i,i}^2 = E_{i,i}$, $E_{i,i}E_{j,j} = \mathbf{0}_n$ si $j \neq i$ et $E_{1,1} + \cdots + E_{n,n} = \mathbf{1}_n$. En appliquant le morphisme unitaire ρ, on obtient que les p_i vérifient les égalités de la condition (ii).

b) *Pour $i = 1, \ldots, n$. on note W_i l'image de p_i. Démontrer que la restriction de $\rho(E_{i,j})$ à W_j induit un isomorphisme de W_j sur W_i.*

On a $\rho(E_{i,j})\, \rho(E_{k,\ell}) = \delta_{j,k}\rho(E_{i,\ell})$ car $E_{i,j}\, E_{k,\ell} = \delta_{j,k}E_{i,\ell}$. En particulier, $p_i\, \rho(E_{i,j}) = \rho(E_{i,j})$. Donc l'image de $\rho(E_{i,j})$ est contenue dans W_i, et la restriction de $\rho(E_{i,j})$ à W_j induit une application linéaire de W_j dans W_i. Comme $\rho(E_{i,j})\, \rho(E_{j,i}) = p_i$ et $\rho(E_{j,i})\, \rho(E_{i,j}) = p_j$ et que p_i (resp. p_j) induit l'identité sur W_i (resp. W_j), $\rho(E_{i,j})$ induit un isomorphisme linéaire de W_j sur W_i, dont l'iinverse est induit par $\rho(E_{j,i})$.

c) *Dans la suite de cette question, on fixe une base $(w_1, \ldots, w_r)$ de l'espace vectoriel W_1, On pose*

$$v_1 = w_1, \quad v_2 = \rho(E_{2,1})w_1, \quad \ldots, \quad v_n = \rho(E_{n,1})w_1 \ .$$

Démontrer que la famille $(v_1, \ldots, v_n)$ est libre et que, pour tous entiers s, t et k compris entre 1 et n, on a

$$\rho(E_{s,t})v_k = \delta_{t,k}v_s \ ,$$

où le symbole de Kronecker $\delta_{t,k}$ vaut 1 lorsque $t = k$. et vaut 0 sinon.

Supposons que $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$. Comme les W_i sont en somme directe et que $\lambda_i v_i \in W_i$, on doit avoir $\lambda_i v_i = 0$, d'où $\lambda_i = 0$ pour $i = 1, \ldots, n$ puisque v_i est un vecteur non nul. Donc $(v_1, \ldots, v_n)$ est une famille libre. L'égalité $\rho(E_{s,t})v_k = \delta_{t,k}v_s$ vient de $\rho(E_{s,t})\, \rho(E_{k,1}) = \delta_{t,k}\rho(E_{s,1})$.

d) *Plus généralement, pour $1 \leq j \leq r$, on note V_j le sous-espace vectoriel de W engendré par les vecteurs $\rho(E_{k,1})w_j$, pour $k = 1, \ldots, n$, Démontrer que W est somme directe des sous-espaces V_j, $1 \leq j \leq r$.*

Les vecteurs $\rho(E_{k,1})w_j$ pour $j = 1, \ldots, r$ forment une base de W_k. Comme W est la somme directe des W_k, la famille $(\rho(E_{k,1})w_j)_{k=1,\ldots,n;\ j=1,\ldots,r}$ est une base de W. Donc W est la somme directe des V_j.

e) *Démontrer qu'il existe une base de l'espace vectoriel W dans laquelle, pour toute matrice $M \in \mathrm{M}_n(\mathbb{C})$, la matrice de l'endomorphisme $\rho(M)$ est la matrice diagonale par blocs*

$$\mathrm{diag}(M, \ldots, M) = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix} .$$

Comme $\mathrm{M}_n(\mathbb{C})$ est engendré en tant qu'espace vectoriel par les $E_{i,j}$, il suffit de montrer le résultat pour les $E_{i,j}$. Plaçons nous dans la base

$$(v_1, \ldots, v_n, w_2, \rho(E_{2,1})w_2, \ldots, \rho(E_{n,1})w_2, w_3, \ldots, \rho(E_{n,1})w_r) \ .$$

Comme $\rho(E_{i,j})\rho(E_{k,1})w_\ell = \delta_{j,k}\,\rho(E_{i,1})w_\ell$, la matrice de $\rho(E_{i,j})$ dans cette base est $\mathrm{diag}(E_{i,j},\ldots,E_{i,j})$.

Partie II

Dans cette partie, on désigne par E un $\mathbb{C}$-espace vectoriel de dimension finie. On dit qu'une partie X de $\mathrm{End}(E)$ est irréductible si les seuls sous-espaces vectoriels de E stables par tous les éléments de X sont $\{0\}$ et E. On désigne par $\mathcal{A}$ une sous-algèbre irréductible de $\mathrm{End}(E)$ qui contient $\mathbf{1}_E$, et on se propose de démontrer qu'elle est égale à $\mathrm{End}(E)$.

1) *Soient u et v des éléments de $\mathrm{End}(E)$ qui commutent entre eux. Démontrer que tout sous-espace propre de l'un est stable par l'autre.*

Soit E_λ le sous-espace propre pour u associé à la valeur propre λ, et soit $x \in E_\lambda$. Alors $u(v(x)) = v(u(x)) = v(\lambda x) = \lambda v(x)$, donc $v(x) \in E_\lambda$. Ainsi E_λ est stable par v.

2) *Soit X une partie irréductible de $\mathrm{End}(E)$. Démontrer que l'ensemble des endomorphismes de E qui commutent avec tous les éléments de X est l'ensemble des endomorphismes scalaires.*

Soit u un endomorphisme qui commute avec tous les éléments de X et soit λ une valeur propre de u (il en existe puisqu'on est sur $\mathbb{C}$). D'après la question précédente, l'espace propre E_λ pour u est stable par tous les éléments de X. Puisqu'il n'est pas réduit à $\{0\}$, c'est E tout entier et donc $u = \lambda \mathbf{1}_E$. Réciproquement, une homothétie commute avec n'importe quel endomorphisme, et en particulier avec ceux de X.

3) *Rappelons que $\mathcal{A}$ est une sous-algèbre irréductible de $\mathrm{End}(E)$ contenant $\mathbf{1}_E$. Démontrer que ${}^t\!\mathcal{A}$ est une sous-algèbre irréductible de $\mathrm{End}(E^*)$.*

${}^t\!\mathcal{A}$ est une sous-algèbre de $\mathrm{End}(E^*)$. C'est un sous-espace vectoriel car ${}^t(u+\lambda v) = {}^tu + \lambda\,{}^tv$, et on a ${}^t(uv) = {}^tv\,{}^tu$. L'algèbre ${}^t\!\mathcal{A}$ est unitaire car ${}^t\mathbf{1}_E = \mathbf{1}_{E^*}$.

On sait qu'un sous-espace F de E est stable par $v \in \mathrm{End}(E)$ si et seulement si son orthogonal $E^\perp = \{\ell \in E^*;\ \forall x \in F\ \ell(x) = 0\}$ est stable par ${}^tv$ (rappelons que ${}^tv(\ell)\,x = \ell(v\,x)$). Donc les seuls sous-espaces de E^* stables par tous les éléments de ${}^t\!\mathcal{A}$ sont $\{0\}^\perp = E^*$ et $E^\perp = \{0\}$, ce qui montre que ${}^t\!\mathcal{A}$ est irréductible.

4) *Soit x un vecteur non nul de E. Préciser à quoi est égal le sous-espace vectoriel $\mathcal{A}\,x$ de E.*

Remarquons que $\mathcal{A}\,x$ est bien un sous-espace vectoriel de E car $\mathcal{A}$ est un sous-espace vectoriel de $\mathrm{End}(E)$. Il est stable par tous les éléments de $\mathcal{A}$ et non nul, donc c'est E.

5) *Soit $u \in \mathrm{End}(E)$ un endomorphisme de rang 1. Démontrer qu'il existe un vecteur y de E et une forme linéaire $\ell \in E^*$ tels que l'on ait $u(x) = \ell[x]\,y$ pour tout $x \in E$.*

Soit y un vecteur qui engendre l'image de u. Alors pour tout $x \in E$ il existe un unique scalaire $\ell(x)$ tel que $u(x) = \ell(x)\,y$, et la linéarité de u entraîne que ℓ est une forme linéaire.

6) *Démontrer que, si l'algèbre $\mathcal{A}$ contient un endomorphisme de rang 1, alors elle les contient tous. En déduire que l'on a alors $\mathcal{A} = \mathrm{End}(E)$,*

Soit u un endomorphisme de rang 1 dans $\mathcal{A}$, et soit v un endomorphisme de rang 1 dans $\mathrm{End}(E)$. D'après la question précédente, il existe des vecteurs non nuls y et z de E et des formes linéaires non nulles ℓ et m de E^* tels que $u(x) = \ell(x)y$ et $v(x) = m(x)\,z$ pour tout $x \in E$. D'après la question II.4, il existe a dans $\mathcal{A}$ tel que $a\,y = z$. En appliquant II.4 à la sous-algèbre irréductible ${}^tA$ de $\mathrm{End}(E^*)$ (II.3), on voit qu'il existe b dans $\mathcal{A}$ tel que ${}^tb\,\ell = m$, c'est-à-dire $m = \ell\,b$. Alors $v = a\,u\,b$, car

$$(a\,u\,b)x = a(\ell(b\,x)\,y) = a(m(x)\,y) = m(x)\,a(y) = m(x)\,z = v(x)\ .$$

On en déduit que v appartient à $\mathcal{A}$. Donc $\mathcal{A}$ contient tous les endomorphismes de rang 1. Or n'importe quel endomorphisme de E est somme d'endomorphismes de rang 1 : si $(e_1,\ldots,e_n)$ est une base de E, alors pour tout endomorphisme u de E il existe des formes linéaires $u_1, \ldots, u_n$ telles que, pour tout $x \in E$, on ait $u(x) = u_1(x)e_1 + \cdots + u_n(x)e_n$. Par conséquent, $\mathcal{A} = \mathrm{End}(E)$.

7) *Dans cette question, on suppose que $\mathcal{A}$ contient un endomorphisme u dont le rang r est ≥ 2, et on se propose de démontrer qu'il existe un endomorphisme $u' \in \mathcal{A}$, non nul, dont le rang est strictement plus petit que r.*

a) *Démontrer qu'il existe x et y dans E et v dans $\mathcal{A}$ tels que le couple de vecteurs $(u(x), u(y))$ soit libre et que l'on ait $vu(x) = y$.*

Puisque u est de rang ≥ 2, on peut trouver deux vecteurs x et y de E tels que $u(x)$ et $u(y)$ soient linéairement indépendants. En particulier, $u(x)$ est non nul. Donc, d'après la question II.4, il existe $v \in \mathcal{A}$ tel que $vu(x) = y$.

b) *Démontrer qu'il existe alors $\lambda \in \mathbb{C}$ tel que la restriction de l'endomorphisme $uv - \lambda \mathbf{1}_E$ à l'image $u(E)$ de u ne soit ni injective ni nulle.*

Remarquons que $u(E)$ est stable par uv. Soit λ une valeur propre de la restriction de uv à $u(E)$. Alors la restriction de $uv - \lambda \mathbf{1}_E$ à $u(E)$ n'est pas injective. Cette restriction n'est pas nulle non plus car $(uv - \lambda \mathbf{1}_E)(u(x)) = u(y) - \lambda u(x) \neq 0$, car $u(x)$ et $u(y)$ sont linéairement indépendants.

c) *Vérifier que l'endomorphisme $u' = uvu - \lambda u$ convient.*

D'après le b), la dimension de $u'(E) = (uv - \lambda \mathbf{1}_E)(u(E))$ est strictement inférieure à celle de $u(E)$, ce qui veut dire que le rang de u' est strictement plus petit que r; par ailleurs $u' \neq 0$ car on a vu que $u'\,x \neq 0$.

8) *Démontrer finalement que l'on a $\mathcal{A} = \mathrm{End}(E)$.*

$\mathcal{A}$ ne peut pas être réduit à l'endomorphisme nul, pour lequel tout sous-espace est stable. D'après la question 7), le minimum des rangs des endomorphismes non nuls de $\mathcal{A}$ est 1. Ainsi $\mathcal{A}$ contient un endomorphisme de rang 1, et d'après la question 6 on a $\mathcal{A} = \mathrm{End}(E)$.

Partie III

Soit n un entier ≥ 1. On appelle dérivation de $\mathrm{M}_n(\mathbb{C})$ toute application linéaire d de $\mathrm{M}_n(\mathbb{C})$ dans $\mathrm{M}_n(\mathbb{C})$ telle que, pour tous X et $Y \in \mathrm{M}_n(\mathbb{C})$, on ait

$$d(XY) = d(X)Y + Xd(Y) .$$

1] *Soit $A \in \mathrm{M}_n(\mathbb{C})$; démontrer que l'application d_A de $\mathrm{M}_n(\mathbb{C})$ dans $\mathrm{M}_n(\mathbb{C})$ définie par*

$$d_A(X) = AX - XA ,$$

est une dérivation.

L'application d_A est clairement linéaire, et

$$d_A(XY) = AXY - XYA = (AX - XA)Y + X(AY - YA) = d_A(X)Y + Xd_A(Y) .$$

2) *Dans cette question, on se propose de démontrer que toute dérivation de $\mathrm{M}_n(\mathbb{C})$ est de la forme ci-dessus.*

a) *Soit $d : \mathrm{M}_n(\mathbb{C}) \to \mathrm{M}_n(\mathbb{C})$ une dérivation. Démontrer que l'application ρ de $\mathrm{M}_n(\mathbb{C})$ dans $\mathrm{M}_{2n}(\mathbb{C})$ définie par*

$$\rho(X) = \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix}$$

est un morphisme unitaire d'algèbres.

L'application ρ est linéaire car d est linéaire. En appliquant la formule de dérivation au produit $\mathbf{1}_n\,\mathbf{1}_n$, on trouve $d(\mathbf{1}_n) = 2d(\mathbf{1}_n)$, d'où $d(\mathbf{1}_n) = 0$ et $\rho(\mathbf{1}_n) = \mathbf{1}_{2n}$. Enfin

$$\begin{aligned}\rho(XY) &= \begin{pmatrix} XY & d(XY) \\ 0 & XY \end{pmatrix} = \begin{pmatrix} XY & Xd(Y) + d(X)Y \\ 0 & XY \end{pmatrix} \\ &= \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix} \begin{pmatrix} Y & d(Y) \\ 0 & Y \end{pmatrix} = \rho(X)\,\rho(Y)\,.\end{aligned}$$

b) *Démontrer qu'il existe une matrice inversible* $P = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *où* A*,* B*,* C*,* D *appartiennent à* $\mathrm{M}_n(\mathbb{C})$*, telle que l'on ait, pour tout* $X \in \mathrm{M}_n(\mathbb{C})$*,*

$$P\,\rho(X) = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} P\,.$$

D'après la question I.2.e, on peut trouver une base de $\mathbb{C}^{2n}$ dans laquelle, pour tout $X \in \mathrm{M}_n(\mathbb{C})$, la matrice de $\rho(X)$ est $\operatorname{diag}(X, X)$. Si $P = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ est l'inverse de la matrice de changement de base, on a donc $P\,\rho(X)\,P^{-1} = \operatorname{diag}(X, X)$, soit encore $P\,\rho(X) = \operatorname{diag}(X, X)\,P$

c) *Conclure.*

En comparant les blocs, il vient pour tout X de $\mathrm{M}_n(\mathbb{C})$: $AX = XA$, $CX = XC$, $A\,d(X) + BX = XB$ et $C\,d(X) + DX = XD$. On en déduit que A est une matrice scalaire $a\mathbf{1}_n$, et que $d(X) = -a^{-1}BX - X(-a^{-1}B)$. En conclusion, $d = d_{-a^{-1}B}$.

Partie IV

Soit n *un entier* ≥ 1*, Pour toute matrice* $M \in \mathrm{M}_n(\mathbb{C})$*, on note* $\mathrm{Tr}(M)$ *la trace de* M*, somme des coefficients diagonaux de* M*.*

1) a) *Démontrer que l'application de* $\mathrm{M}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C})$ *dans* $\mathbb{C}$ *définie par*

$$\psi(X, Y) = \mathrm{Tr}(XY)\,,$$

est une forme bilinéaire symétrique non dégénérée.

Il est clair que ψ est bilinéaire, symétrique car $\mathrm{Tr}(XY) = \mathrm{Tr}(YX)$. Montrons que le noyau de ψ est réduit à $\{0\}$. Soit $X = (x_{i,j}) \in \mathrm{M}_n(\mathbb{C})$ tel que $\mathrm{Tr}(XY) = 0$ pour tout $Y \in \mathrm{M}_n(\mathbb{C})$. En particulier, pour $Y = E_{j,i}$ on a $x_{i,j} = \mathrm{Tr}(XE_{j,i}) = 0$ et donc $X = 0$. On conclut que ψ est bien une forme bilinéaire symétrique non dégénérée.

b) *Démontrer que, si* $(X_1, \ldots, X_{n^2})$ *est une base de l'espace vectoriel* $\mathrm{M}_n(\mathbb{C})$*. il existe une autre base* $(X'_1, \ldots, X'_{n^2})$ *de* $\mathrm{M}_n(\mathbb{C})$ *telle que, pour tous entiers* i *et* j *compris entre* 1 *et* n^2*, on ait*

$$\psi(X_i, X_j) = \delta_{i,j} \qquad \textit{(symbole de Kronecker).}$$

Puisque ψ est non dégénérée, l'application linéaire $X \mapsto (Y \mapsto \psi(X, Y))$ est un isomorphisme de $\mathrm{M}_n(\mathbb{C})$ sur son dual. Soit $(X'_1, \ldots, X'_{n^2})$ l'image réciproque par cet isomorphisme de la base duale de $(X_1, \ldots, X_{n^2})$. Alors on a bien $\psi(X_i, X'_j) = \delta_{i,j}$.

2) *Démontrer que, pour toute matrice* $A \in \mathrm{M}_n(\mathbb{C})$*, on a*

$$\sum_{1 \leq i \leq n^2} X_i\, A X_i' = \mathrm{Tr}(A)\, \mathbf{1}_n \ .$$

Soit $P = (p_{i,j})$ la matrice de passage de la base $\mathcal{B} = (X_1, \ldots, X_{n^2})$ à la base $\mathcal{C} = (Y_1, \ldots, Y_{n^2})$ de $\mathrm{M}_n(\mathbb{C})$, de sorte que $Y_j = \sum_{i=1}^{n^2} p_{i,j} X_i$. Soit P' la matrice de passage de la base $\mathcal{B}' = (X_1', \ldots, X_{n^2}')$ à la base $\mathcal{C}' = (Y_1', \ldots, Y_{n^2}')$ (toutes deux données par la question 1b). Pour toutes matrices A et B de $\mathrm{M}_n(\mathbb{C})$, on doit avoir

$${}^t\!\gamma\, \delta' = \psi(A, B) = {}^t\!\alpha\, \beta' = {}^t\!(P\gamma)\, P'\delta' = {}^t\!\gamma\, {}^t\!P\, P'\, \delta' \ ,$$

où α et β' (resp. γ et δ') sont les vecteurs colonnes des coordonnées de A et B dans les bases $\mathcal{B}$ et $\mathcal{B}'$ (resp. $\mathcal{C}$ et $\mathcal{C}'$). Donc $P' = {}^t\!P^{-1}$. Si $P^{-1} = (q_{i,j})$, on a ainsi $Y_j' = \sum_{i=1}^{n^2} q_{j,i} X_i'$.

Calculons maintenant

$$\begin{aligned}
\sum_{j=1}^{n^2} Y_j\, A Y_j' &= \sum_{j=1}^{n^2} \left((\sum_{i=1}^{n^2} p_{i,j} X_i) A (\sum_{k=1}^{n^2} q_{j,k} X_k') \right) \\
&= \sum_{i=1}^{n^2} \sum_{k=1}^{n^2} (\sum_{j=1}^{n^2} p_{i,j} q_{j,k})\, X_i A X_k' = \sum_{i=1}^{n^2} \sum_{k=1}^{n^2} \delta_{i,k}\, X_i A X_k' \\
&= \sum_{i=1}^{n^2} X_i A X_i' \ .
\end{aligned}$$

Ce calcul montre que la matrice $\sum_{i=1}^{n^2} X_i A X_i'$ ne dépend pas du choix de la base $\mathcal{B}$ de $\mathrm{M}_n(\mathbb{C})$. On peut donc la calculer pour la base formée par les $E_{i,j}$, en remarquant que $\psi(E_{i,j}, E_{k,\ell}) = \delta_{j,k}\, \delta_{i,\ell}$. On obtient donc, si $A = (a_{i,j})$:

$$\sum_{i=1}^{n^2} X_i\, A X_i' = \sum_{i=1}^{n} \sum_{j=1}^{n} E_{i,j} A E_{j,i} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{j,j} E_{i,i} = \mathrm{Tr}(A)\, \mathbf{1}_n \ .$$

[Je ne suis pas satisfait de cette réponse calculatoire.]

Partie V

On considère dans cette partie un sous-groupe G *de* $\mathrm{GL}(n, \mathbb{C})$ *ayant la propriété suivante :*
(P) Il existe un entier $m \geq 1$ *tel que l'on ait* $g^m = \mathbf{1}_n$ *pour tout* $g \in G$*.*
On fixe l'entier m*.*

1) *Démontrer que chaque élément* g *de* G *est diagonalisable. Que peut-on dire de ses valeurs propres ?*

Chaque élément g de G admet comme polynôme annulateur $X^m - 1$ qui est scindé sur $\mathbb{C}$ à racines simples. Donc g est diagonalisable. Sers valeurs propres figurent parmi les racines m-èmes de l'unité.

2) *Démontrer que l'ensemble* $\{\mathrm{Tr}(g),\ g \in G\}$ *est fini,*

Si g est dans G, sa trace est une somme de n racines m-èmes de l'unité. Or de telles sommes sont en nombre fini, certainement majoré par m^n.

3) *On suppose, dans cette question, que l'ensemble G, considéré comme ensemble d'endomorphismes de $\mathbb{C}^n$ (en identifiant $\mathrm{M}_n(\mathbb{C})$ et $\mathrm{End}(\mathbb{C}^n)$), est irréductible.*

a) *Démontrer que l'ensemble G contient une base de l'espace vectoriel $\mathrm{M}_n(\mathbb{C})$.*

Le sous-espace vectoriel de $\mathrm{M}_n(\mathbb{C})$ engendré par G est une sous-algèbre unitaire de $\mathrm{M}_n(\mathbb{C})$, car G contient $\mathbf{1}_n$ et est stable par produit. Notons $\mathbb{C}[G]$ cette algèbre. Si G est irréductible, alors l'algèbre $\mathbb{C}[G]$ l'est aussi, et d'après II.8 on a donc $\mathbb{C}[G] = \mathrm{M}_n(\mathbb{C})$. par conséquent, G engendre $\mathrm{M}_n(\mathbb{C})$ et en contient une base.

b) *Démontrer que l'ensemble G est fini (on pourra utiliser les questions (IV.l) et (V,2)).*

Soit $(X_1, \ldots, X_{n^2})$ une base de $\mathrm{M}_n(\mathbb{C})$ contenue dans G, et $(X'_1, \ldots, X'_{n^2})$ la base obtenue comme en IV.1.b. Soit $g = \sum_{i=1}^{n^2} \lambda_i X'_i$ un élément de G. Alors chaque $\lambda_i = \mathrm{Tr}(X_i g)$ appartient à l'ensemble fini des traces d'éléments de G. Donc G est fini.

4) *Dans cette question, on ne suppose plus que l'ensemble G soit irréductible.*

a) *Démontrer qu'il existe des entiers p et q, avec $p + q = n$, et une base de l'espace vectoriel $\mathbb{C}^n$ dans laquelle chaque élément g de G s'écrit par blocs*

$$\begin{pmatrix} T(g) & U(g) \\ 0 & V(g) \end{pmatrix},$$

où $T(g) \in \mathrm{M}_p(\mathbb{C})$ et $V(g) \in \mathrm{M}_q(\mathbb{C})$.

Visiblement, la question devrait être posée avec $0 < p < n$ (sinon on pourrait toujours prendre $p = 0$ ou $q = 0$), et on doit supposer G non irréductible. Puisque G n'est pas irréductible, il existe un sous-espace E de $\mathbb{C}^n$, différent de $\{0\}$ et de $\mathbb{C}^n$, et stable par tous les éléments de G. Fabriquons alors une base de $\mathbb{C}^n$ en complétant une base de E. Dans cette base, la matrice de n'importe quel élément g de G s'écrit par blocs

$$\begin{pmatrix} T(g) & U(g) \\ 0 & V(g) \end{pmatrix},$$

où $T(g)$ est une matrice carrée de taille la dimension p de E, et $V(g)$ de taille $q = n - p$.

b) *Posons $G_1 = \{g \in G,\ T(g) = \mathbf{1}_p\}$ et $G_2 = \{g \in G,\ V(g) = \mathbf{1}_q\}$. Démontrer que G_1 et G_2 sont des sous-groupes distingués de G.*

Déterminer $G_1 \cap G_2$.

D'après les propriétés de la multiplication par blocs, les applications $g \mapsto T(g)$ et $g \mapsto V(g)$ sont des morphismes de groupes de G dans $\mathrm{GL}(p, \mathbb{C})$ et $\mathrm{GL}(q, \mathbb{C})$. Leurs noyaux G_1 et G_2 sont donc des sous-groupes distingués de G.

Si g appartient à $G_1 \cap G_2$, sa matrice dans la base choisie au a) est

$$\begin{pmatrix} \mathbf{1}_p & U(g) \\ 0 & \mathbf{1}_q \end{pmatrix},$$

et la matrice de $g^m = \mathbf{1}_n$ est

$$\begin{pmatrix} \mathbf{1}_p & m\,U(g) \\ 0 & \mathbf{1}_q \end{pmatrix}.$$

On en déduit $U(g) = 0$ et $g = \mathbf{1}_n$. Donc $G_1 \cap G_2 = \{\mathbf{1}_n\}$.

c) *Soient K un groupe et H un sous-groupe de K. L'indice de H dans K est le cardinal de l'ensemble quotient K/H. Établir le résultat général suivant :*

Soient K un groupe, K_1 et K_2 des sous-groupes distingues de K, tous deux d'indice fini dans K ; alors l'indice de $K_1 \cap K_2$ dans K est fini,

L'inclusion de K_1 dans K induit un morphisme injectif $K_1/(K_1 \cap K_2) \to K/K_2$. Comme K/K_2 est fini, $K_1/(K_1 \cap K_2)$ aussi. L'application identique de K induit un morphisme sujectif $K/(K_1 \cap K_2) \to K/K_1$

dont l'image et le noyau $K_1/(K_1 \cap K_2)$ sont finis. Donc $K/(K_1 \cap K_2)$ est fini. On peut même voir que l'indice de $K_1 \cap K_2$ dans K est un diviseur du produit des indices de K_1 et de K_2.

d) *Conclure.*

On montre par récurrence sur n que G est fini. L'hypothèse de récurrence est que pour tout entier strictement positif $p < n$, tout sous-groupe de $\mathrm{GL}(p, \mathbb{C})$ vérifiant la propriété (P) est fini. Soit G comme dans le préambule de cette partie. Ou bien G est irréductible et donc fini d'après 3b. Ou bien G n'est pas irréductible, et alors d'après b) on a deux sous-groupes distingués G_1 et G_2 de G, d'intersection $\{1\}$. De plus G/G_1 est isomorphe à l'image de G par T dans $\mathrm{GL}(p, \mathbb{C})$, et est donc fini d'après l'hypothèse de récurrence. Il en est de même pour G/G_2. On en déduit que l'intersection $\{1\}$ de G_1 et G_2 est d'indice fini dans G, ce qui veut dire que G est fini.

Partie VI

Soient n et m des entiers ≥ 1. Soient $A \in \mathrm{M}_n(\mathbb{C})$ et $B \in \mathrm{M}_m(\mathbb{C})$; on définit la matrice $A * B \in \mathrm{M}_{nm}(\mathbb{C})$ par

$$A * B = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ \vdots & \vdots & \ldots & \vdots \\ a_{n,1}B & a_{n,2}B & \cdots & a_{n,n}B \end{pmatrix}$$

1) *Démontrer que l'application ϕ de $\mathrm{M}_n(\mathbb{C}) \times \mathrm{M}_n(\mathbb{C})$ dans $\mathrm{M}_{nm}(\mathbb{C})$ définie par $\phi((A, B) = A * B$ est bilinéaire et satisfait à*

$$(A * B)(A' * B') = AA' * BB'$$

pour toutes matrices A, $A' \in \mathrm{M}_n(\mathbb{C})$, B, $B' \in \mathrm{M}_m(\mathbb{C})$.

L'application ϕ est bilinéaire car $A \mapsto a_{i,j}$ est linéaire de $\mathrm{M}_n(\mathbb{C})$ dans $\mathbb{C}$ et l'application $(a, B) \mapsto aB$ bilinéaire de $\mathbb{C} \times \mathrm{M}_m(\mathbb{C})$ dans $\mathrm{M}_m(\mathbb{C})$. On vérifie

$$\begin{aligned} (A * B)(A' * B') &= \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ldots & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix} \begin{pmatrix} a'_{1,1}B' & \cdots & a'_{1,n}B' \\ \vdots & \ldots & \vdots \\ a'_{n,1}B' & \cdots & a'_{n,n}B' \end{pmatrix} \\ &= \begin{pmatrix} (\sum_{j=1}^n a_{1,j}a'_{j,1})BB' & \cdots & (\sum_{j=1}^n a_{1,j}a'_{j,n})BB' \\ \vdots & \ldots & \vdots \\ (\sum_{j=1}^n a_{n,j}a'_{j,1})BB' & \cdots & (\sum_{j=1}^n a_{n,j}a'_{j,n})BB' \end{pmatrix} \\ &= AA' * BB' \end{aligned}$$

2) *Démontrer que l'image de l'application ϕ engendre l'espace vectoriel $\mathrm{M}_{nm}(\mathbb{C})$.*

Pour s'y retrouver, on note $(E_{i,j})$ la base standard de $\mathrm{M}_n(\mathbb{C})$, $(F_{i,j})$ celle de $\mathrm{M}_m(\mathbb{C})$ et $(G_{i,j})$ celle de $\mathrm{M}_{nm}(\mathbb{C})$. On remarque que

$$E_{i,j} * F_{k,\ell} = G_{m(i-1)+k, m(j-1)+\ell}$$

et que $m(i-1)+k$ (resp. $m(j-1)+\ell$) prend toutes les valeurs entières de 1 à nm quand i (resp. k) parcourt l'ensemble $\{1, \ldots, n\}$ et j (resp. ℓ) l'ensemble $\{1, \ldots, m\}$. L'image de ϕ contient une base de $\mathrm{M}_{nm}(\mathbb{C})$ et engendre donc cet espace.

On suppose désormais $n = m$.

3) *Posons*

$$P = \sum_{1\leq i,j\leq n} E_{i,j} * E_{j,i} \ .$$

a) *Démontrer que l'on a* $P^2 = \mathbf{1}_{n^2}$. [coquille de l'énoncé]
Calculons, en utilisant 1,

$$\begin{aligned} P^2 &= (\sum_{i,j} E_{i,j} * E_{j,i})(\sum_{k,\ell} E_{k,\ell} * E_{\ell,k}) = \sum_{i,j,k,\ell} (E_{i,j}E_{k,\ell} * E_{j,i}E_{\ell,k}) \\ &= \sum_{i,j,k,\ell} (\delta_{j,k}E_{i,\ell} * \delta_{i,\ell}E_{j,k}) = \sum_{i,j} E_{i,i} * E_{j,j} = \sum_{\nu=1}^{n^2} G_{\nu,\nu} = \mathbf{1}_{n^2} \end{aligned}$$

b) Démontrer que, pour toutes matrices A. $B \in \mathrm{M}_n(\mathbb{C})$ on a

$$P(A * B)P = B * A \ .$$

Par bilinéarité, il suffit de démontrer l'égalité pour $A = E_{\alpha,\beta}$ et $B = E_{\gamma,\delta}$. Calculons donc

$$P(A * B)P = (E_{\gamma,\beta} * E_{\alpha,\delta})P = E_{\gamma,\delta} * E_{\alpha,\beta} = B * A \ .$$

4) *Soient* A *et* $B \in \mathrm{M}_n(\mathbb{C})$.
a) *Calculer la trace et le déterminant de la matrice* $A * B$.
On peut trigonaliser les matrices A et B : $A = U^{-1}SU$ et $B = V^{-1}TV$, avec S et T triangulaires supérieures de diagonales respectivement $(\lambda_1, \ldots, \lambda_n)$ et $(\mu_1, \ldots, \mu_n)$. On remarque que $S * T$ est triangulaire supérieure de diagonale $(\lambda_i\mu_j)_{i=1,\ldots,n;\ j=1,\ldots,n}$. Par ailleurs $A * B$ est semblable à $S * T$ car, d'après 1, on a

$$A * B = (U^{-1}SU) * (V^{-1}TV) = (U^{-1} * V^{-1})(S * T)(U * V) = (U * V)^{-1}(S * T)(U * V) \ .$$

On en déduit que

$$\mathrm{tr}(A * B) = \sum_{i,j} \lambda_i\mu_j = (\sum_i \lambda_i)(\sum_j \mu_j) = \mathrm{Tr}(A) \times \mathrm{Tr}(B) \ ,$$

et que

$$\det(A * B) = \prod_{i=1}^{n}\prod_{j=1}^{n} \lambda_i\mu_j = (\prod_{i=1}^{n} \lambda_i)^n(\prod_{j=1}^{n} \mu_j)^n = \det(A)^n \ \det(B)^n \ .$$

b) *Déterminer les valeurs propres de* $A * B$ *en fonction de colles de* A *et de* B.
Avec les notations du a, les valeurs propres de A sont les λ_i, celle de B les μ_j et on a vu que les valeurs propres de $A * B$ sont les $\lambda_i\mu_j$ pour $i = 1, \ldots, n$ et $j = 1, \ldots, n$.