Centrale 2022 PSI

Pour les notations, je vous renvoie à l'énoncé.

I Partie I

I.A – Quelques résultats préliminaires

Q 1. Soit $A \in \mathcal{M}_n(\mathbb{R})$, en notant $A = (a_{i,j})$, on a par définition $\text{tr}(A) = \sum_{i=1}^{n} a_{i,i} \in \mathbb{R}$.

Soit $B \in \mathcal{M}_n(\mathbb{R})$, en notant $B = (b_{i,j})$ on a :

$$\forall \lambda \in \mathbb{R} \quad \text{tr}(\lambda A + B) = \sum_{i=1}^{n} (\lambda a_{i,i} + b_{i,i} = \lambda \sum_{i=1}^{n} a_{i,i} + \sum_{i=1}^{n} b_{i,i} = \lambda \,\text{tr}(A) + \text{tr}(B))$$

donc l'application

$$\left| \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \to & \mathbb{R} \\ M & \mapsto & \text{tr}(M) \end{array} \right.$$

est une forme linéaire.

De plus en notant $AB = (c_{i,j})$ et $BA = (d_{i,j})$ on a :

$$\text{tr}(AB) = \sum_{i=1}^{n} c_{i,i} = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{i,k} b_{k,i} = \sum_{k=1}^{n} \sum_{i=1}^{n} b_{k,i} a_{i,k} = \sum_{k=1}^{n} d_{k,k} = \text{tr}(BA)$$

Q 2. tr est une forme linéaire sur $\mathcal{M}_n(\mathbb{R})$, donc l'application

$$\varphi : \left| \begin{array}{ccc} \left(\mathcal{M}_n(\mathbb{R})\right)^2 & \to & \mathbb{R} \\ (A, B) & \mapsto & \text{tr}\left(A^{\intercal} B\right) \end{array} \right.$$

est bien définie et à valeurs dans $\mathbb{R}$.

Pour $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_n(\mathbb{R})$, on note $A = (a_{i,j})$ et $B = (b_{i,j})$ alors

$$\text{tr}(A^T.B) = \sum_{i=1}^{n} \left(\sum_{k=1}^{n} a_{k,i} b_{k,i} \right) = \sum_{i=1}^{n} \left(\sum_{i=1}^{n} b_{k,i} a_{k,i} \right) = \text{tr}(B^T.A)$$

• On a donc $\varphi(A, B) = \varphi(B, A)$, φ est symétrique.

• Par linéarité de la trace, on a immédiatement

$$\varphi(A, \lambda B + C) = \text{tr}(A^T.(\lambda B + C)) = \text{tr}(\lambda A^T B + A^T C) = \lambda \,\text{tr}(A^T B) + \text{tr}(A^T C) = \lambda \varphi(A, B) + \varphi(A, C)$$

donc φ est linéaire à droite et par symétrie, φ est bilinéaire.

• Soit $A \neq 0_n$, il existe $(i_0, k_0) \in [\![1, n]\!]^2$, $\quad a_{k_0,i_0} \neq 0$, alors $a_{k_0,i_0}^2 > 0$ et par somme de réels positifs dont un est strictement positif, $\text{tr}(A^T A) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{k,i}^2 > 0$. On a donc $A \neq 0 \Longrightarrow \varphi(A, A) > 0$.

φ est une forme bilinéaire symétrique définie-positive sur $\mathcal{M}_n(\mathbb{R})$, c'est donc un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.

Q 3. Si A est une matrice de $\mathcal{M}_n(\mathbb{R})$ vérifiant $A^\mathsf{T}A = 0_n$ alors $\mathrm{tr}\left(A^\mathsf{T}A\right) = 0$ et par le caractère défini-positif du produit scalaire de la question précédente, on a immédiatement : $\boxed{A = 0_n.}$

I.B – Quelques propriétés de $\mathcal{N}_n$

Q 4. Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice nilpotente, il existe $p \in \mathbb{N}^*$ tel que $A^p = 0_n$.

• Pour montrer que 0 est valeur propre de A sans passer par le déterminant qui est demandé en question suivante, on raisonne par l'absurde :
Supposons que 0 ne soit pas valeur propre de A, alors A est inversible et par produit de matrices inversibles, A^p est inversible, ce qui est absurde puisque $A^p = 0_n$.
On en déduit que 0 est valeur propre de A.

• On a $A^p = 0_n$ donc $P = X^p$ est un polynôme annulateur de A, on sait alors que toute valeur propre de A est racine de P. Donc toute valeur propre complexe de A est nécessairement nulle.

Finalement 0 est une valeur propre complexe de A et c'est la seule.

Q 5. Soit A une matrice nilpotente de $\mathcal{M}_n(\mathbb{R})$, dans $\mathbf{C}$ le polynôme caractéristique de A est scindé, donc on sait que la trace et le déterminant de A sont respectivement égaux à la somme et au produit des valeurs propres complexes de A comptées avec leur multiplicté. Comme 0 est la seule valeur propre complexe de A, on a $\boxed{\mathrm{tr}(A) = 0 \text{ et } det(A) = 0.}$

Q 6. Si $M \in \mathcal{M}_n(\mathbb{R})$ est nilpotente, alors il existe $p \in \mathbb{N}^*$ tel que $M^p = 0_n$, alors $(M^2)^p = M^{2p} = (M^p)^2 = 0_n$ et donc $\boxed{M^2 \text{ est nilpotente.}}$

Q 7. On suppose que M et N sont deux matrices nilpotentes qui commutent. Il existe donc $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que $M^p = 0_n$ et $N^q = 0_n$.

• Puisque M et N commutent on a : $(M.N)^p = M^p.N^p = 0_n.N^p = 0_n$, donc $\boxed{M\,N \text{ est nilpotente.}}$

• Puisque M et N commutent, on peut appliquer la formule du binôme de Newton qui donne : $(M+N)^{p+q} = \sum_{k=0}^{p+q} \binom{p+q}{k} M^k N^{p+q-k}$.
Pour $k \in [\![p+1, p+q]\!]$ $M^k = 0$ et pour $k \in [\![0, p]\!]$ $(p+q-k) \geqslant q$ alors $N^{p+q-k} = 0$, finalement $\forall k \in [\![0, p+q]\!]$ $M^k N^{p+q-k} = 0$ donc $(M+N)^{p+q} = 0$, avec $p+q \in \mathbb{N}^*$, donc $\boxed{M+N \text{ est nilpotente.}}$

Q 8. On suppose que M, N et $M+N$ sont nilpotentes.

$$\begin{aligned}(M+N)^2 - M^2 - N^2 &= (M+N).(M+N) - M^2 - N^2 \\ &= M^2 + NM + MN + N^2 - M^2 - N^2 \\ &= MN + NM\end{aligned}$$

Avec les propriétés vues en question 1, on obtient : $\text{tr}(M\,N) = \frac{1}{2}\left(\text{tr}((M+N)^2) - \text{tr}(M^2) - \text{tr}(N^2)\right)$.
Par hypothèse M est nilpotente donc par les questions 5 et 6 on a : M^2 est nilpotente et $\text{tr}(M^2) = 0$.
De même $\text{tr}(N^2) = 0 = \text{tr}((M+N)^2)$. Finalement $\text{tr}(M\,N) = 0$.

Q 9. On a déjà vu que si M dans $\mathcal{M}_2(\mathbb{R})$ est nilpotente alors $\det(M) = \text{tr}(M) = 0$.
On suppose que $M \in \mathcal{M}_2(\mathbb{R})$ vérifie $det(M) = \text{tr}(M) = 0$. On sait que le polynôme caractéristique de M est $X^2 - \text{tr}(M)X + det(M)$ donc ici ce polynôme caractéristique est X^2 et par le théorème de Cayley-Hamilton on sait qu'il est annulateur de M donc $M^2 = 0$ et M est nilpotente.

Par double implication on a montré que $M \in \mathcal{M}_2(\mathbb{R})$ est nilpotente si, et seulement si $det(M) = \text{tr}(M) = 0$.

Q 10. Si M est une matrice réelle nilpotente et symétrique, alors par le théorème spectral on sait que M est diagonalisable. Sa seule valeur propre étant le réel 0, la matrice M est semblable à la matrice nulle donc M est la matrice nulle.
De plus la matrice nulle est nilpotente et symétrique réelle donc

la seule matrice matrice réelle nilpotente et symétrique est la matrice nulle.

On pouvait aussi utiliser : Si M est nilpotente et symétrique alors $M^TM = M^2$ et par les questions 6 et 5 on a $\text{tr}(M^TM) = \text{tr}(M^2) = 0$, alors par la question 3 on a $M = 0_n$. Et réciproquement la matrice nulle est nilpotente et symétrique.

Q 11. Soit A une matrice antisymétrique réelle et nilpotente. Il existe $p \in \mathbb{N}^*$ tel que $A^p = 0_n$.
Puisque $A^T = -A$, $A^TA = -A^2$ est aussi nilpotente (question 6).
$\left(A^\intercal\,A\right)^T = A^\intercal\left(A^\intercal\right)^\intercal = A^\intercal\,A$ donc $A^\intercal\,A$ est une matrice symétrique réelle qui est nilpotente, alors

par le résultat de la question 10 $A^\intercal\,A = 0_n$ puis par le résultat de la question 3 on a aussi $A = 0_n$.

Q 12. Pour $M = \begin{pmatrix} 0_{n-2} & & \\ & 1 & 0 \\ & 0 & -1 \end{pmatrix}$, on a $\text{tr}(M) = 0 = det(M)$ et $\forall p \in \mathbb{N}^* \quad M^p = \begin{pmatrix} 0_{n-2} & & \\ & 1 & 0 \\ & 0 & (-1)^p \end{pmatrix} \neq 0_n$
M n'est pas nilpotente.

II Matrices aléatoires à coefficients dans $\{-1, 1\}$

II.A – Quelques résultats algébriques

Soit $(E_1, \ldots, E_n)$ la base canonique de $\mathcal{M}_{n,1}(\mathbb{R})$. On note $V = \sum_{k=1}^{n} E_k$.

Q 13. Par définition $\mathcal{V}_{n,1}$ est l'ensemble des matrices-colonnes à n lignes et à coefficients dans $\{-1, 1\}$.

Pour $i \in [\![1,n]\!]$, $\boxed{E_i = \dfrac{V}{2} - \dfrac{V-2E_i}{2}.}$ On a donc $E_i \in \text{Vect}(V, V-2E_i)$. Or $V \in \mathcal{V}_{n,1}$ et $V-2E_i \in \mathcal{V}_{n,1}$.
On a donc $\forall i \in [\![1,n]\!] \quad E_i \in \text{Vect}\left(\mathcal{V}_{n,1}\right)$.

On en déduit que $\mathcal{M}_{n,1}(\mathbb{R}) = \text{Vect}\left(E_1, \dots, E_n\right) \subset \text{Vect}\left(\mathcal{V}_{n,1}\right)$. Et comme $\mathcal{V}_{n,1} \subset \mathcal{M}_{n,1}(\mathbb{R})$, on a finalement $\boxed{\mathcal{M}_{n,1}(\mathbb{R}) = \text{Vect}\left(\mathcal{V}_{n,1}\right).}$

Soient $C_1, \dots, C_n$, n matrices colonnes de $\mathcal{M}_{n,1}(\mathbb{R})$, avec C_1 non nulle.

Q 14. On suppose que la famille $(C_1, \dots, C_n)$ est liée.

Remarquons que $(C_1, \dots, C_j)$ est libre et $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$ signifie que $(C_1, \dots, C_j)$ est libre et $(C_1, \dots, C_j, C_{j+1})$ n'est pas (plus) libre. Et si $(C_1, \dots, C_{j+1})$ est liée alors $(C_1, \dots, C_k)$ est liée pour tout $k \geqslant j+1$.

Notons alors $I = \{i \in [\![1,n]\!], \quad (C_1, \dots, C_i) \text{ est libre}\}$.
Par hypothèse $C_1 \neq 0$ donc (C_1) est libre et donc $1 \in I$, de plus $(C_1, \dots, C_n)$ est liée donc $n \notin I$, I est alors une partie non vide de $[\![1, n-1]\!]$. I admet donc un maximum que l'on note j. Par définition de maximum, j est l'unique entier de $[\![1, n-1]\!]$ qui vérifie : $(C_1, \dots, C_j)$ est libre $(j \in I)$ et $(C_1, \dots, C_{j+1})$ est liée $(j+1 \notin I)$, donc $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$.

Il existe bien un unique $j \in [\![1, n-1]\!]$ tel que

$$\begin{cases} (C_1, \dots, C_j) \text{ est libre} \\ C_{j+1} \in \text{Vect}(C_1, \dots, C_j) \end{cases}$$

Soit $d \in [\![1,n]\!]$, $(U_1, \dots, U_d)$ une famille libre de $\mathcal{M}_{n,1}(\mathbb{R})$ et $H = \text{Vect}(U_1, \dots, U_d)$.

Q 15. Puisque $(U_1, \dots, U_d)$ est libre, on sait que H est un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{R})$ de dimension d et donc $dim(H) = dim(\mathcal{M}_{d,1}(\mathbb{R}))$.

La matrice écrite par blocs colonnes $M = (U_1 \dots U_d) \in \mathcal{M}_{n,p}(\mathbb{R})$ est de rang d puisque $(U_1, \dots, U_d)$ est une famille libre. On sait que le rang de M est aussi égal au rang des lignes de M, il existe donc des entiers $i_1, \dots, i_d$ avec $1 \leqslant i_1, < \dots < i_d \leqslant n$ tels que les lignes $L_{i_1}, \dots, L_{i_d}$ de M forment une famille libre et $\forall k \notin \{i_1, \dots, i_d\}, \quad (L_{i_1}, \dots, L_{i_d}, L_k)$ est liée.

Considérons alors l'application

$$\varphi : \left| \begin{array}{ccc} H & \to & \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{array} \right.$$

Cette application est linéaire, par opérations sur les matrices-colonnes.
Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in H$, il existe $(a_1, \dots, a_d) \in \mathbb{R}^d$ tel que $X = \sum_{k=1}^{d} a_k U_k = M. \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} . \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$

avec M écrite par blocs-lignes. Alors $\varphi(X) = \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} = \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_d} \end{pmatrix} . \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$.

Si $X \in \mathrm{Ker}(\varphi)$ alors $\begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_d} \end{pmatrix} . \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = 0$, or la matrice, écrite par blocs-lignes, $M_d = \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_d} \end{pmatrix}$ est carrée d'ordre d et est de rang d, donc M_d est inversible. On a donc :

$$\varphi(X) = 0 \iff M_d . \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = 0 \iff \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} = 0 \iff X = \sum_{k=1}^{d} a_k U_k = 0$$

On a obtenu : $\mathrm{Ker}(\varphi) = \{0\}$ et φ est une application linéaire injective de H dans $\mathcal{M}_{d,1}(\mathbb{R})$. Puisque $dim(H) = dim\left(\mathcal{M}_{d,1}(\mathbb{R})\right)$, le théorème du rang donne que φ est aussi sujective ($Im(\varphi) = \mathcal{M}_{d,1}(\mathbb{R})$).

L'application $\varphi : \left| \begin{array}{ccc} H & \to & \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{array} \right.$ est donc bijective.

Q 16. Soit $\mathcal{W}$ un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{R})$ de dimension d. Comme dans la question précédente, il existe des entiers $i_1, \ldots, i_d$ avec $1 \leqslant i_1, < \cdots < i_d \leqslant n$ tels que l'application $\varphi : \left| \begin{array}{ccc} \mathcal{W} & \to & \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{array} \right.$ soit bijective. On a alors $\mathrm{card}\left(\mathcal{W} \cap \mathcal{V}_{n,1}\right) = \mathrm{card}\,\varphi\left(\mathcal{W} \cap \mathcal{V}_{n,1}\right)$.

Or par définition de φ, $\varphi\left(\mathcal{W} \cap \mathcal{V}_{n,1}\right) \subset \mathcal{V}_{d,1}$ avec $\mathcal{V}_{d,1} = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}, \quad \forall i \in [\![1, d]\!] \quad a_i \in \{-1, 1\} \right\}$, donc $\mathrm{card}\left(\mathcal{V}_{d,1}\right) = 2^d$ et $\mathrm{card}\,\varphi\left(\mathcal{W} \cap \mathcal{V}_{n,1}\right) \leqslant 2^d$. On en déduit que $\boxed{\mathrm{card}\left(\mathcal{W} \cap \mathcal{V}_{n,1}\right) \leqslant 2^d.}$

II.B – Une loi de probabilité

On dit qu'une variable réelle X suit la loi $\mathcal{R}$ si

$$X(\Omega) = \{-1, 1\}, \qquad \mathbb{P}(X = -1) = \mathbb{P}(X = 1) = \frac{1}{2}.$$

Q 17. Si X suit la loi $\mathcal{R}$, notons $U = \frac{1}{2}(X + 1)$. Puisque $X(\Omega) = \{-1, 1\}$, on a $U(\Omega) = \{0, 1\}$ donc U suit une loi de Bernoulli. De plus $(U = 1) = (X = 1)$ donc $\mathbb{P}(U = 1) = \mathbb{P}(X = 1) = \frac{1}{2}$.

$\frac{X+1}{2}$ suit la loi de Bernoulli de paramètre $\frac{1}{2}$.

Q 18. On déduit de la question précédente que $\mathbb{E}\left(\dfrac{X+1}{2}\right) = \dfrac{1}{2}$ et par linéarié de l'espérance

$$\boxed{\mathbb{E}(X) = 2.\mathbb{E}\left(\frac{X+1}{2}\right) - 1 = 2.\frac{1}{2} - 1 = 0.}$$

On a aussi $\dfrac{1}{2}.\left(1-\dfrac{1}{2}\right) = \mathbb{V}\left(\dfrac{X+1}{2}\right) = \dfrac{1}{2^2}\mathbb{V}(X)$ donc $\boxed{\mathbb{V}(X) = 1.}$

Autre méthode : à écrire en détails

$X(\Omega)$ est fini donc $\mathbb{E}(X) = \displaystyle\sum_{x\in X(\Omega)} x\mathbb{P}(X=x) = -\mathbb{P}(X=-1) + \mathbb{P}(X=1) = 0.$
$\mathbb{V}(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2 = \mathbb{E}(X^2)$ et par le théorème du transfert
$\mathbb{E}(X^2) = \displaystyle\sum_{x\in X(\Omega)} x^2\mathbb{P}(X=x) = \mathbb{P}(X=-1) + \mathbb{P}(X=1) = 1.$

Q 19. Soient X et Y deux variables aléatoires réelles indépendantes, suivant chacune la loi $\mathcal{R}$. Puisque $X(\Omega) = Y(\Omega) = \{-1,1\}$, on a $XY(\Omega) = \{-1,1\}$ et par la formule des probabilités totales avec le système complet d'événements associé à X

$$\begin{aligned}
\mathbb{P}(XY=1) &= \mathbb{P}(X=1, XY=1) + \mathbb{P}(X=-1, XY=1)\\
&= \mathbb{P}(X=1, Y=1) + \mathbb{P}(X=-1, Y=-1)\\
&\quad \text{et par indépendance de } X \text{ et } Y\\
&= \mathbb{P}(X=1).\mathbb{P}(Y=1) + \mathbb{P}(X=-1).\mathbb{P}(Y=-1)\\
&= \frac{1}{4} + \frac{1}{4}\\
\mathbb{P}(XY=1) &= \frac{1}{2}
\end{aligned}$$

Par passage au complémentaire $\mathbb{P}(XY=-1) = 1-\mathbb{P}(XY=1) = \dfrac{1}{2}.$ $\boxed{\text{La variable aléatoire } XY \text{ suit la loi } \mathcal{R}.}$

II.C – Un premier procédé de génération de matrices aléatoires à coefficients dans $\{-1,1\}$

Jusqu'à la fin de la partie II, n est un entier naturel non nul et $m_{i,j}$ $(1 \leqslant i,j \leqslant n)$ sont n^2 variables aléatoires réelles mutuellement indépendantes suivant toutes la loi $\mathcal{R}$. La variable aléatoire matricielle $M_n = (m_{i,j})_{1\leqslant i,j\leqslant n}$ est alors à valeurs dans $\mathcal{V}_{n,n}$.

On pose $\tau_n = \operatorname{tr}(M_n)$ et $\delta_n = \det(M_n)$.

Q 20. Par définition $\tau_n = \displaystyle\sum_{i=1}^{n} m_{i,i}$ et par linéarité de l'espérance avec le résultat de la question 18, on a :

$$\mathbb{E}(\tau_n) = \sum_{i=1}^{n}\mathbb{E}(m_{i,i}) = \sum_{i=1}^{n} 0 = 0$$

On a aussi par indépendance des variables $m_{1,1},\dots,m_{n,n}$ et la question 19 :

$$\mathbb{V}(\tau_n)=\sum_{i=1}^{n}\mathbb{V}(m_{i,i})=\sum_{i=1}^{n}1=n$$

Q 21. Par développement du déterminant δ_n par rapport à sa première colonne on sait que

$$\delta_n=\sum_{i=1}^{n}(-1)^{i+1}m_{i,1}\Delta_{i,1}$$

où $\Delta_{i,1}$ est le déterminant de la matrice obtenue à partir de M_n en supprimant sa première colonne et sa $i^{\text{ème}}$ ligne. Par linéarité de l'espérance on a alors :

$$\mathbb{E}(\delta_n)=\sum_{i=1}^{n}(-1)^{i+1}\mathbb{E}\left(m_{i,1}\Delta_{i,1}\right)$$

Or pour $i\in[\![1,n]\!]$, $\Delta_{i,1}$ est le déterminant d'une matrice ayant des coefficients $m_{k,j}$ avec $(k,j)\neq(i,1)$, alors par le lemme des colations on sait que $\Delta_{i,1}$ est une variable aléatoire indépendante de $m_{i,1}$, et donc $\mathbb{E}(m_{i,1}\Delta_{i,1})=\mathbb{E}(m_{i,1}).\mathbb{E}(\Delta_{i,1})=0$ puisque $m_{i,1}\sim\mathcal{R}$ (question 19), donc

$$\mathbb{E}(\delta_n)=\sum_{i=1}^{n}(-1)^{i+1}\mathbb{E}\left(m_{i,1}\right).\mathbb{E}\left(\Delta_{i,1}\right)=0$$

Q 22. • Pour $n=1$, on a $\delta_1=m_{1,1}$ et donc $\mathbb{V}(\delta_1)=\mathbb{V}(m_{1,1})=1=1!$ par la question 19.

• Soit $n\in\mathbb{N}^*$, on suppose que la variance du déterminant d'une matrice aléatoire d'ordre n dont les coefficients sont des variables aléatoires indépendantes suivant la loi $\mathcal{R}$ est égal à $n!$.

Par développement par rapport à la dernière colonne, on a :

$$\delta_{n+1}=\det(M_{n+1})=\sum_{i=1}^{n+1}(-1)^{n+1+i}m_{i,n+1}\Delta_{i,n+1}$$

avec $\Delta_{i,n+1}$ le déterminant de la matrice obtenue à partir de la matrice M_{n+1} en supprimant sa dernière colonne et sa $i^{\text{ème}}$ ligne.
On a vu précédemment que $\mathbb{E}(\delta_{n+1})=0$ donc

$$\mathbb{V}(\delta_{n+1})=\mathbb{E}(\delta_{n+1}^2)-\left(\mathbb{E}(\delta_{n+1})\right)^2=\mathbb{E}(\delta_{n+1}^2)$$

Et

$$\delta_{n+1}^2=\delta_{n+1}.\delta_{n+1}=\sum_{i=1}^{n+1}\sum_{j=1}^{n+1}(-1)^{i+j}m_{i,n+1}m_{j,n+1}\Delta_{i,n+1}\Delta_{j,n+1}$$

Par linéarité de l'espérance :

$$\mathbb{V}(\delta_{n+1})=\sum_{i=1}^{n+1}\sum_{j=1}^{n+1}(-1)^{i+j}\mathbb{E}\left(m_{i,n+1}m_{j,n+1}\Delta_{i,n+1}\Delta_{j,n+1}\right)$$

Par le lemme des coalitions $m_{i,n+1}.m_{j,n+1}$ et $\Delta_{i,n+1}\Delta_{j,n+1}$ sont indépendantes (déterminants d'une matrice n'ayant pas les coefficients de la colonne $n+1$ de M_{n+1}), donc

$$\mathbb{V}(\delta_{n+1})=\sum_{i=1}^{n+1}\sum_{j=1}^{n+1}(-1)^{i+j}\mathbb{E}\left(m_{i,n+1}m_{j,n+1}\right).\mathbb{E}\left(\Delta_{i,n+1}\Delta_{j,n+1}\right)$$

Si $j \neq i$ alors $\mathbb{E}(m_{i,n+1}.m_{j,n+1}) = \mathbb{E}(m_{i,n+1}).\mathbb{E}(m_{j,n+1}) = 0$.
Si $j = i$ alors $\mathbb{E}(m_{i,n+1}m_{j,n+1}) = \mathbb{E}(m_{i,n+1}^2) = \mathbb{V}(m_{i,n+1}) = 1$ donc

$$\mathbb{V}(\delta_{n+1}) = \sum_{i=1}^{n+1}(-1)^{i+i}\mathbb{E}\left(\Delta_{i,n+1}^2\right)$$

Pour $i \in [\![1, n+1]\!]$, $\Delta_{i,n+1}$ est le déterminant d'une matrice carrée aléatoire d'ordre n dont les coefficients sont des variables aléatoires indépendantes suivant la loi $\mathcal{R}$ alors $\mathbb{E}(\Delta_{i,n+1}) = 0$ (question 21) et par hypothèse de récurrence $\mathbb{V}(\Delta_{i,n+1}) = n!$, ce qui donne $\mathbb{E}\left(\Delta_{i,n+1}^2\right) = \mathbb{V}(\Delta_{i,n+1}) = n!$ et finalement

$$\mathbb{V}(\delta_{n+1}) = \sum_{i=1}^{n+1} n! = (n+1).n! = (n+1)!$$

On a donc montré par récurrence que $\boxed{\forall n \in \mathbb{N}^* \quad \mathbb{V}(\delta_n) = n!.}$

Dans le cas particulier $n = 2$, m_{11}, m_{12}, m_{21} et m_{22} sont quatre variables aléatoires réelles, mutuellement indépendantes, suivant toutes la loi $\mathcal{R}$ et $M_2 = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$.

Q 23. D'après le résultat de la question 9, $M_2 \in \mathcal{N}_2 \iff \text{tr}(M_2) = 0 = det(M_2)$, ce qui donne :

$$\begin{aligned}
\mathbb{P}(M_2 \in \mathcal{N}_2) &= \mathbb{P}\left(\tau_2 = 0, \delta_2 = 0\right) \\
&= \mathbb{P}\left((m_{2,2} = -m_{1,1}) \cap (m_{1,1}m_{2,2} = m_{1,2}.m_{2,1})\right) \\
&\quad \text{avec le système complet d'événements associé à } m_{1,1} \\
&= \mathbb{P}(m_{1,1} = 1, m_{2,2} = -1, m_{1,2}m_{2,1} = -1) + \mathbb{P}(m_{1,1} = -1, m_{2,2} = 1, m_{1,2}m_{2,1} = -1) \\
&\quad \text{par indépendance des variables aléatoires} \\
\mathbb{P}(M_2 \in \mathcal{N}_2) &= \mathbb{P}(m_{1,1} = 1)\mathbb{P}(m_{2,2} = -1)\mathbb{P}(m_{1,2}m_{2,1} = -1) + \mathbb{P}(m_{1,1} = -1)\mathbb{P}(m_{2,2} = 1)\mathbb{P}(m_{1,2}m_{2,1} = -1) \\
&\quad \text{par le résultat de la question 19} \\
\mathbb{P}(M_2 \in \mathcal{N}_2) &= \frac{1}{8} + \frac{1}{8}
\end{aligned}$$

$$\boxed{\mathbb{P}(M_2 \in \mathcal{N}_2) = \frac{1}{4}}$$

Q 24. $(M_2 \in \mathcal{G}\ell_2(\mathbb{R})) = (\delta_2 \neq 0)$ alors $\mathbb{P}\left(M_2 \in \mathcal{G}\ell_2(\mathbb{R})\right) = 1 - \mathbb{P}(\delta_2 = 0)$.
Par le résultat de la question 19 et le lemme des coalitions, on sait que $m_{1,1}m_{2,2}$ et $m_{1,2}m_{2,1}$ sont

indépendantes et suivent la loi $\mathcal{R}$, alors avec le système complet d'événements associé à $m_{1,1}m_{2,2}$:

$$\begin{aligned}
\mathbb{P}(\delta_2 = 0) &= \mathbb{P}(m_{1,1}m_{2,2} = m_{1,2}m_{2,1}) \\
&= \mathbb{P}(m_{1,1}m_{2,2} = -1, m_{1,1}m_{2,2} = m_{1,2}m_{2,1}) + \mathbb{P}(m_{1,1}m_{2,2} = 1, m_{1,2}m_{2,1} = m_{1,1}m_{2,2}) \\
&= \mathbb{P}(m_{1,1}m_{2,2} = -1, m_{1,2}m_{2,1} = -1) + \mathbb{P}(m_{1,1}m_{2,2} = 1, m_{1,2}m_{2,1} = 1) \\
&= \mathbb{P}(m_{1,1}m_{2,2} = -1).\mathbb{P}(m_{1,2}m_{2,1} = -1) + \mathbb{P}(m_{1,1}m_{2,2} = 1).\mathbb{P}(m_{1,2}m_{2,1} = 1) \\
&= \frac{1}{2}.\frac{1}{2} + \frac{1}{2}.\frac{1}{2} \\
\mathbb{P}(\delta_2 = 0) &= \frac{1}{2}
\end{aligned}$$

On a donc $\mathbb{P}\left(M_2 \in \mathcal{GL}_2(\mathbb{R})\right) = \dfrac{1}{2}$.

II.D – Une généralisation

L'objectif de cette sous-partie est de prolonger le dernier résultat de la partie précédente, en trouvant, dans le cas général où n est un entier naturel supérieur ou égal à 2 , un minorant de la probabilité de l'évènement $M_n \in \mathcal{GL}_n(\mathbb{R})$.

II.D.1) On considère $2n$ variables aléatoires réelles $c_1, c_2, \ldots, c_n$ et $c'_1, c'_2, \ldots, c'_n$ mutuellement indépendantes, suivant toutes la loi $\mathcal{R}$.

Q 25. Soit $(\varepsilon_1, \ldots, \varepsilon_n) \in \{-1, 1\}^n$. Par indépendance des variables aléatoires et la loi $\mathcal{R}$, on a :

$$\mathbb{P}\big((c_1 = \varepsilon_1) \cap \cdots \cap (c_n = \varepsilon_n)\big) = \prod_{i=1}^{n} \mathbb{P}(c_i = \varepsilon_i) = \frac{1}{2^n}.$$

On considère les matrices colonnes aléatoires $C = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ et $C' = \begin{pmatrix} c'_1 \\ \vdots \\ c'_n \end{pmatrix}$.

Q 26. Pour tout $\omega \in \Omega$, la famille $\big(C(\omega), C'(\omega)\big)$ est liée si et seulement si $C(\omega) = 0$ ou il existe $\lambda \in \mathbb{R}$ tel que $C'(\omega) = \lambda C(\omega)$.
Par définition $C'(\omega)$ et $C(\omega)$ sont dans $\mathcal{V}_{n,1}$ donc $C(\omega) \neq 0$ et $C'(\omega) = \lambda C(\omega) \Longrightarrow \lambda \in \{-1, 1\}$.

On a donc pour tout $\omega \in \Omega$, la famille $\big(C(\omega), C'(\omega)\big)$ est liée si et seulement s'il existe $\varepsilon \in \{-1, 1\}$ tel que $C'(\omega) = \varepsilon C(\omega)$.

Q 27. On déduit de la question précédente que

$$\begin{aligned}\mathbb{P}\big((C,C') \text{ est liée}\big) &= \mathbb{P}(C'=C)+\mathbb{P}(C'=-C)\\ &= \mathbb{P}\left(\bigcap_{i=1}^{n}(c'_i=c_i)\right)+\mathbb{P}\left(\bigcap_{i=1}^{n}(c'_i=-c_i)\right)\\ &\quad \text{par indépendance des variables}\\ &= \prod_{i=1}^{n}\mathbb{P}(c'_i=c_i)+\prod_{i=1}^{n}\mathbb{P}(c'_i=-c_i)\end{aligned}$$

Pour $i\in[\![1,n]\!]$, par la formule des probabilités totales avec le système complet $((c_i=1),(c_i=-1))$ et l'indépendance des variables, on a :

$$\mathbb{P}(c'_i=c_i)=\mathbb{P}(c_i=1,c'_i=1)+\mathbb{P}(c_i=-1,c'_i=-1)=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

et de même $\mathbb{P}(c'_i=-c_i)=\dfrac{1}{2}$, donc $\boxed{\mathbb{P}\big((C,C') \text{ est liée}\big)=\dfrac{2}{2^n}=\dfrac{1}{2^{n-1}}.}$

II.D.2) On rappelle que $m_{i,j}$ $(1\leqslant i,j\leqslant n)$ sont n^2 variables aléatoires réelles mutuellement indépendantes suivant toutes la loi $\mathcal{R}$, que $M_n=(m_{i,j})_{1\leqslant i,j\leqslant n}$ est la matrice aléatoire à valeurs dans $\mathcal{V}_{n,n}$ dont, pour tout $(i,j)\in[\![1,n]\!]^2$, le coefficient situé à la ligne i et la colonne j est égal à $m_{i,j}$.

On note

$$C_1=\begin{pmatrix}m_{1,1}\\ \vdots\\ m_{n,1}\end{pmatrix},\dots,C_n=\begin{pmatrix}m_{1,n}\\ \vdots\\ m_{n,n}\end{pmatrix}$$

les variables aléatoires à valeurs dans $\mathcal{V}_{n,1}$ constituées par les colonnes de la matrice M_n.

Pour tout $j\in[\![1,n-1]\!]$, on note R_j l'événement

$$(C_1,\dots,C_j) \text{ est libre et } C_{j+1}\in \mathrm{Vect}(C_1,\dots,C_j)$$

et R_n l'événement

$$(C_1,\dots,C_n) \text{ est libre.}$$

Q 28. Une matrice carrée à coefficients dans $\{-1,1\}$ est soit inversible, soit non inversible, donc les événements (M est inversible) et (M n'est pas inversible) forment un système complet d'événements.

Or (M est inversible)$=R_n$ et $\overline{R_n}=$(M est non inversible)$=$ $((C_1,\dots,C_n)$ est liée). D'après le résultat de la question 14, puisque $C_1\neq 0$ (coefficients dans $\{-1,1\}$), $(C_1,\dots,C_n)$ est liée si et seulement si il existe un unique $j\in[\![1,n-1]\!]$ tel que R_j soit réalisé, donc $\overline{R_n}=\bigsqcup_{j=1}^{n-1}R_j$ (union disjointe).

$\boxed{(R_1,\dots,R_n) \text{ est un système complet d'événements.}}$

II.D.3)

Q 29. D'après ce qui précède, $\mathbb{P}\big(M \notin \mathcal{G}\ell_n(\mathbb{R})\big) = \mathbb{P}\left(\bigsqcup_{j=1}^{n-1} R_j\right) = \sum_{j=1}^{n-1} \mathbb{P}(R_j)$.

Or par définition, $\forall j \in [\![1, n-1]\!] \quad R_j \subset \big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big)$, donc
$\mathbb{P}(R_j) \leqslant \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big)$ et par somme :

$$\mathbb{P}\big(M \notin \mathcal{G}\ell_n(\mathbb{R})\big) \leqslant \sum_{j=1}^{n-1} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big).$$

Q 30. Soit $j \in [\![1, n-1]\!]$. $\forall k \in [\![1, j]\!] \quad C_k(\Omega) = \{-1, 1\}$, donc $\big(\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big)\big)_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j}$ est un système complet d'événements et par la formule des probabilités totales on a :

$$\begin{aligned}
\mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big) &= \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j) \cap (C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big) \\
&= \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(v_1, \dots, v_j) \cap (C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big)
\end{aligned}$$

par indépendance des variables $C_1, \dots, C_{j+1}$ on a finalement

$$\mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big) = \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(v_1, \dots, v_j)\big)\mathbb{P}\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big)$$

Q 31. Pour $(v_1, \dots, v_j) \in \mathcal{V}_{n,1}^j$, $\mathrm{Vect}(v_1, \dots, v_j) = \mathrm{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}$.
On a $dim\,(\mathrm{Vect}(v_1, \dots, v_j)) \leqslant j$, donc il existe $\mathcal{W}$ un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{R})$ de dimension j tel que $\mathrm{Vect}(v_1, \dots, v_j) \subset \mathcal{W}$, alors par le résultat de la question 16, on a $\mathrm{card}\,(\mathcal{W} \cap \mathcal{V}_{n,1}) \leqslant 2^j$, donc $\mathrm{card}\,(\mathrm{Vect}(v_1, \dots, v_j) \cap \mathcal{V}_{n,1}) \leqslant 2^j$, ce qui donne $\mathrm{card}\,(\mathrm{Vect}(v_1, \dots, v_j)) \leqslant 2^j$ et
$\mathbb{P}(C_{j+1} \in \mathrm{Vect}(v_1, \dots, v_j) = \sum_{v\in\mathrm{Vect}\,(v_1,\dots,v_n)} \mathbb{P}(C_{j+1} = v)$.

Par le résultat de la question 25, pour $v \in \mathrm{Vect}(v_1, \dots, v_j)$, $\mathbb{P}(C_{j+1} = v) = \dfrac{1}{2^n}$, donc

$$\mathbb{P}(C_{j+1} \in \mathrm{Vect}(v_1, \dots, v_j) = \sum_{v\in\mathrm{Vect}\,(v_1,\dots,v_n)} \frac{1}{2^n} = \frac{\mathrm{card}\,\mathrm{Vect}(v_1, \dots, v_j)}{2^n} \leqslant \frac{2^j}{2^n}$$

On en déduit que pour tout $j \in [\![1, n-1]\!]$,

$$\begin{aligned}
\mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big) &= \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(v_1, \dots, v_j)\big)\mathbb{P}\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big) \\
&\leqslant \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} 2^{j-n}\mathbb{P}\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big) \\
&\leqslant 2^{j-n} \sum_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j} \mathbb{P}\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big)
\end{aligned}$$

et puisque $\big(\big((C_1 = v_1) \cap \cdots \cap (C_j = v_j)\big)\big)_{(v_1,\dots,v_j)\in\mathcal{V}_{n,1}^j}$ est un système complet d'événeme

$$\mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big) \leqslant 2^{j-n}$$

Q 32. On déduit des questions 29 et 31 que

$$\begin{aligned}
\mathbb{P}\big(M \notin \mathcal{GL}_n(\mathbb{R})\big) &\leqslant \sum_{j=1}^{n-1} \mathbb{P}\big(C_{j+1} \in \mathrm{Vect}(C_1, \dots, C_j)\big) \\
&\leqslant \sum_{j=1}^{n} 2^{j-n} \\
&\qquad \text{on pose } k = n - j \\
&\leqslant \sum_{k=1}^{n-1} \left(\frac{1}{2}\right)^k \\
&\leqslant \frac{1 - (1/2)^n}{1 - 1/2} - 1 \\
&\leqslant 1 - \frac{1}{2^{n-1}}
\end{aligned}$$

Et par passage au complémentaire : $\boxed{\mathbb{P}\big(M \in \mathcal{GL}_n(\mathbb{R})\big) \geqslant \frac{1}{2^{n-1}}}$

III Un autre procédé de construction de matrices aléatoires à coefficients dans $\{-1, 1\}$

Soit $p \in]0, 1[$. On définit une suite (A_k) de matrices aléatoires d'ordre n à coefficients dans $\{-1, 1\}$ selon le procédé suivant :

— on note A_0 la matrice réelle d'ordre n dont tous les coefficients sont égaux à 1 ;

— pour tout entier naturel k, on construit la matrice A_{k+1} à partir de la matrice A_k en conservant chaque coefficient de A_k égal à -1 et en changeant en -1 avec la probabilité p chaque coefficient de A_k égal à 1. Chaque coefficient égal à 1 a donc la probabilité $q = 1 - p$ de ne pas être modifié ;

— le processus s'arrête quand la matrice obtenue est égale à $-A_0$.

On suppose avoir utilisé l'instruction

```
import numpy as np, numpy.random as rd
```

pour charger les bibliothèques `numpy` et `numpy.random`. Voici quelques fonctions de ces bibliothèques qui peuvent être utiles dans cette partie :

— `np.ones((n,n))` crée un tableau `numpy` de taille $n \times n$ dont tous les éléments valent 1 ;

— `A.shape` est un tuple qui contient les dimensions du tableau `A` ;

— `A.size` donne le nombre total d'éléments du tableau `A` ;

— `A.sum()` renvoie la somme de tous les éléments du tableau `A` ;

— `rd.binomial(1, p)` simule une variable aléatoire suivant la loi de Bernoulli de paramètre p.

Q 33. *Le sujet est mal posé. Je pense qu'il faut comprendre que l'on souhaite une fonction qui renvoie la matrice A_{k+1} lorsque l'on a donné la matrice A_k, sinon la question suivante est incohérente avec celle-ci. Et on part d'une matrice de $\mathcal{V}_{n,n}$ donc d'une matrice carrée d'ordre n*

`rd.binomial(1, p)` simule une variable aléatoire suivant la loi de Bernoulli de paramètre p, ce qui signifie que `rd.binomial(1, p)` renvoie la valeur 1 (avec une probabilité p) ou la valeur 0 (avec une probabilité 1-p).

Voici donc une proposition :

```
def modifie_matrice(p,A) :
    n=len(A) (ou n,m=A.shape  si on a peur que la matrice ne soit pas carrée)
    for i in range(n) :
        for j in range(n) (ou m) :
            if A[i][j]==1 : ( on va potentiellement changé ce coefficient)
                if rd.binomial(1,p)==1 : ( on change le coefficient en -1 avec la probabilité p)
                    A[i][j]=-1
    return A
```

Q 34. Cette fois les matrices seront carrées d'ordre n. Comme on n'a pas donné la syntaxe pour vérifier si deux matrices sont égales ou pas, pour comparer les matrices A_k avec la matrice $-A_0$ on peut calculer la somme des coefficients (on donne la syntaxe) qui doit valoir $-n^2$ (chaque coefficient de $-A_0$ est égal à -1, et ceux des matrices A_k valent 1 ou -1).

```
def nb_tours(p, n) :
    A=np.ones((n,n)) (création de la matrice A_0)
    k=0
    While A.sum() !=-n**2 :
        A=modifie_matrice(p,A)
        k=k+1
    return k
```

Q 35. Calcul classique d'une moyenne : on fait nbe fois la fonction précédente et on somme successivement les valeurs obtenues puis on divise par nbe.

```
def moyenne_tours(p, n, nbe) :
    s=0
    for i in range(nbe) :
        s+ =nb_tours(p, n)
    return s/nbe
```

IV Vecteurs aléatoires unitaires

On suppose que n est un entier naturel supérieur ou égal à 1.

On désigne par I un sous-ensemble de $\mathbb{N}$ ayant au moins deux éléments et par $u = (u_i)_{i\in I}$ une suite de vecteurs unitaires de $\mathcal{M}_{n,1}(\mathbb{R})$.

Q 36. Par inégalité de Cauchy-Schwarz, on sait que

$$\forall (i,j) \in I^2 \quad |\langle u_i \mid u_j\rangle| \leqslant \|u_i\|.\|u_j\|$$

Or les vecteurs étant normés on a :

$$\forall (i,j) \in I^2 \quad 0 \leqslant |\langle u_i \mid u_j \rangle| \leqslant 1$$

$\left\{ |\langle u_i \mid u_j \rangle|,\ (i,j) \in I^2,\ i \neq j \right\}$ est donc une partie non vide (I contient au moins deux éléments) de $\mathbb{R}^+$ et majorée par 1, alors $\boxed{C(u) = \sup \left\{ |\langle u_i \mid u_j \rangle|,\ (i,j) \in I^2,\ i \neq j \right\} \text{ existe et appartient à l'intervalle } [0,1].}$

$C(u)$ s'appelle paramètre de cohérence de la suite $(u_i)_{i \in I}$.

Q 37. Par définition de $C(u)$, on a :

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \Longrightarrow 0 \leqslant |\langle u_i \mid u_j \rangle| \leqslant C(u)$$

Si $C(u) = 0$, alors $\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \Longrightarrow |\langle u_i \mid u_j \rangle| = 0$, donc la famille $(u_i)_{i \in I}$ est une famille orthonormée de $\mathcal{M}_{n,1}(\mathbb{R})$, c'est donc une famille libre de $\mathcal{M}_{n,1}(\mathbb{R})$. On sait alors qu'elle contient au maximum n vecteurs ($n = dim \mathcal{M}_{n,1}(\mathbb{R})$).

$\boxed{\text{Si } C(u) = 0 \text{ alors } \{u_i, \quad i \in I\} \text{ est fini et de cardinal inférieur ou égal à } n.}$

Q 38. Pour $t \in \mathbb{R}$, on a $\text{ch}(t) = \displaystyle\sum_{n=0}^{+\infty} \frac{t^{2n}}{(2n)!}$ et $\exp\left(\frac{t^2}{2}\right) = \displaystyle\sum_{n=0}^{+\infty} \frac{1}{n!}\left(\frac{t^2}{2}\right)^n = \sum_{n=0}^{+\infty} \frac{t^{2n}}{2^n n!}$.

Par définition $(2n)! = \displaystyle\prod_{i=1}^{2n} i = \prod_{k=1}^{n} (2k) . \prod_{k=0}^{n-1} (2k+1) = 2^n n! \prod_{k=0}^{n-1} (2k+1) \geqslant 2^n n! > 0$, alors $\dfrac{1}{(2n)!} \leqslant \dfrac{1}{2^n n!}$ et $t^{2n} \geqslant 0$, donc

$$\forall n \in \mathbb{N} \quad \frac{t^{2n}}{(2n)!} \leqslant \frac{t^{2n}}{2^n n!}$$

Par somme pour $n = 0$ à N et passage à la limite lorsque $N \to +\infty$, on obtient $\boxed{\text{ch}(t) \leqslant \exp\left(\frac{t^2}{2}\right).}$

Soient $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ des variables aléatoires mutuellement indépendantes de même loi $\mathcal{R}$ (définie dans la sous-partie II.B). On définit les vecteurs aléatoires, $X = \dfrac{1}{\sqrt{n}}(X_1, \ldots, X_n)^\mathsf{T}$ et $Y = \dfrac{1}{\sqrt{n}}(Y_1, \ldots, Y_n)^\mathsf{T}$ à valeurs dans $\mathcal{M}_{n,1}(\mathbb{R})$.

Q 39. Soit un réel t. Par définition $t\langle X \mid Y \rangle = t \displaystyle\sum_{k=1}^{n} \frac{X_k}{\sqrt{n}} . \frac{Y_k}{\sqrt{n}} = \sum_{k=1}^{n} \frac{t}{n} X_k Y_k$, alors

$$\exp(t\langle X \mid Y \rangle) = \exp\left(\sum_{k=1}^{n} X_k Y_k \frac{t}{n}\right) = \prod_{k=1}^{n} \exp\left(\frac{t}{2} X_k Y_k\right)$$

Les variables aléatoires $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ sont indépendantes et suivent la loi $\mathcal{R}$, alors par le lemme des coalitions $\exp\left(\dfrac{t}{n} X_1 Y_1\right), \ldots, \exp\left(\dfrac{t}{n} X_n Y_n\right)$ sont indépendantes et finies donc par propriété de l'espérance :

$$\mathbb{E}\big(\exp(t\langle X \mid Y \rangle)\big) = \prod_{k=1}^{n} \mathbb{E}\left(\exp\left(X_k Y_k \frac{t}{n}\right)\right)$$

par la question 19, on sait que $\forall k \in [\![1,n]\!] \quad X_kY_k \sim \mathcal{R}$, alors $\mathbb{E}\big(\exp(t\langle X \mid Y\rangle)\rangle\big) = \left(\mathbb{E}\left(\exp\left(X_1Y_1\frac{t}{n}\right)\right)\right)^n$.
Par le théorème du transfert pour $Z = X_1Y_1$, $\mathbb{E}(f(Z)) = \sum_{a\in Z(\Omega)} f(a)\mathbb{P}(Z=a)$:

$$\mathbb{E}\left(\exp\left(X_1Y_1\frac{t}{n}\right)\right) = \exp\left(-\frac{t}{n}\right)\mathbb{P}(X_1Y_1=-1) + \exp\left(\frac{t}{n}\right)\mathbb{P}(X_1Y_1=1) = \operatorname{ch}\left(\frac{t}{n}\right)$$

Donc finalement $\boxed{\mathbb{E}\big(\exp(t\langle X \mid Y\rangle)\rangle\big) = \left(\operatorname{ch}\left(\frac{t}{n}\right)\right)^n}$

Q 40. Pour pour tout nombre réel t, par la question 38 on a $0 \leqslant \operatorname{ch}\left(\frac{t}{n}\right) \leqslant \exp\left(\frac{t^2}{2n^2}\right)$, alors $\left(\operatorname{ch}\left(\frac{t}{n}\right)\right)^n \leqslant \left(\exp\left(\frac{t^2}{2n^2}\right)\right)^n$ et le résultat de la question 39 donne : $\boxed{\mathbb{E}\big(\exp(t\langle X \mid Y\rangle)\big) \leqslant \exp\left(\frac{t^2}{2n}\right).}$

Soient σ et λ deux nombres réels strictement positifs et Z une variable aléatoire réelle telle que $\exp(tZ)$ est d'espérance finie et vérifie

$$\forall t \in \mathbb{R}, \qquad \mathbb{E}\big(\exp(tZ)\big) \leqslant \exp\left(\frac{\sigma^2t^2}{2}\right).$$

Q 41. • Si $t = 0$ alors $\exp\left(\frac{\sigma^2t^2}{2} - \lambda t\right) = 1$ et donc $\mathbb{P}(Z \geqslant \lambda) \leqslant \exp\left(\frac{\sigma^2t^2}{2} - \lambda t\right)$.

• Si $t > 0$ alors pour tout réel a on a :

$$a \geqslant \lambda \iff ta \geqslant t\lambda \iff \exp(ta) \geqslant \exp(t\lambda)$$

donc $(Z \geqslant \lambda) = (tZ \geqslant t\lambda) = (\exp(tZ) \geqslant \exp(t\lambda))$ et donc $\mathbb{P}(Z \geqslant \lambda) = \mathbb{P}(\exp(tZ) \geqslant \exp(t\lambda))$.

La variable aléatoire $\exp(tZ)$ est positive et d'espérance finie par hypothèse et $\exp(t\lambda) > 0$, alors par l'inégalité de Markov on sait que $\mathbb{P}\left(\exp(tZ) \geqslant \exp(t\lambda)\right) \leqslant \dfrac{\mathbb{E}(\exp(tZ))}{\exp(t\lambda)}$.

Par hypothèse on a aussi $\mathbb{E}(\exp(tZ)) \leqslant \exp\left(\frac{\sigma^2t^2}{2}\right)$ donc $\mathbb{P}(Z \geqslant \lambda) \leqslant \dfrac{\exp\left(\frac{\sigma^2t^2}{2}\right)}{\exp(\lambda t)}$.

$\boxed{\text{Finalement } \forall t \in \mathbb{R}^+, \qquad \mathbb{P}(Z \geqslant \lambda) \leqslant \exp\left(\frac{\sigma^2t^2}{2} - \lambda t\right).}$

Q 42. Par définition de la valeur absolue, on a : $(|Z| \geqslant \lambda) = (Z \geqslant \lambda) \cup (-Z \geqslant \lambda)$, λ étant un réel strictement positif, les deux événements de l'union sont incompatibles et

$$\mathbb{P}(|Z| \geqslant \lambda) = \mathbb{P}(Z \geqslant \lambda) + \mathbb{P}(-Z \geqslant \lambda)$$

Par hypothèse $\forall t \in \mathbb{R} \quad \mathbb{E}(\exp(tZ)) \leqslant \exp\left(\frac{\sigma^2t^2}{2}\right)$, alors $\mathbb{E}(\exp(t(-Z))) = \mathbb{E}(\exp((-t)Z)) \leqslant \exp\left(\frac{\sigma^2t^2}{2}\right)$ et le raisonnement fait en question 41 s'applique pour la variable aléatoire $(-Z)$, ce qui donne $\forall t \in \mathbb{R} \quad \mathbb{P}(-Z \geqslant \lambda) \leqslant \exp\left(\frac{\sigma^2t^2}{2} - \lambda t\right)$, donc

$$\forall t \in \mathbb{R} \quad \mathbb{P}(|Z| \geqslant \lambda) \leqslant 2\exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right) \quad (**)$$

$(**)$ est vraie pour tout $t \in \mathbb{R}$, cherchons t tel que $\frac{\sigma^2 t^2}{2} - \lambda t = -\frac{\lambda^2}{2\sigma^2}$:

$$\frac{\sigma^2 t^2}{2} - \lambda t = -\frac{\lambda^2}{2\sigma^2} \iff \frac{(\sigma^2 t - \lambda)^2}{2\sigma^2} = 0 \iff t = \frac{\lambda}{\sigma^2}$$

alors en prenant $t = \frac{\lambda}{\sigma^2}$ on a $\exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right) = \exp\left(-\frac{\lambda^2}{2\sigma^2}\right)$ et $(**)$ donne : $\boxed{\mathbb{P}(|Z| \geqslant \lambda) \leqslant \exp\left(-\frac{\lambda^2}{2\sigma^2}\right)}$

Q 43. On pose $Z = \langle X \mid Y \rangle$, alors le résultat de la question 40 donne $\mathbb{E}(\exp(tZ)) \leqslant \exp\left(\frac{\sigma^2 t^2}{2}\right)$

pour $\sigma = \frac{1}{\sqrt{n}}$, et le résultat de la question 42 avec $\lambda = \varepsilon$ permet d'obtenir : $\boxed{\mathbb{P}(|\langle X \mid Y \rangle| \geqslant \varepsilon) \leqslant 2\exp\left(-\frac{\varepsilon^2 n}{2}\right).}$

N étant un entier naturel non nul, $\left(X_j^i\right)_{1 \leqslant i \leqslant N, 1 \leqslant j \leqslant n}$ est une famille de $n \times N$ variables aléatoires réelles mutuellement indépendantes de même loi $\mathcal{R}$. Pour tout $i \in [\![1, N]\!]$, on pose $X^i = \frac{1}{\sqrt{n}}(X_1^i, \ldots, X_n^i)^\mathsf{T}$.

Q 44. Par sous-additivité de la probabilité on sait que

$$\mathbb{P}\left(\bigcup_{1 \leqslant i < j \leqslant N} \left(|\langle X^i \mid X^j \rangle| \geqslant \varepsilon\right)\right) \leqslant \sum_{1 \leqslant i < j \leqslant N} \mathbb{P}\left(|\langle X^i \mid X^j \rangle| \geqslant \varepsilon\right)$$

Par le résultat de la question 43 on a alors

$$\mathbb{P}\left(\bigcup_{1 \leqslant i < j \leqslant N} \left(|\langle X^i \mid X^j \rangle| \geqslant \varepsilon\right)\right) \leqslant \sum_{1 \leqslant i < j \leqslant N} 2\exp\left(-\frac{\varepsilon^2 n}{2}\right)$$

$$\sum_{1 \leqslant i < j \leqslant N} 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) = 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) \sum_{1 \leqslant i < j \leqslant N} 1.$$

$$\sum_{1 \leqslant i < j \leqslant N} 1 = \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} 1 = \sum_{i=1}^{N-1} (N - (i+1) + 1) = \sum_{i=1}^{N-1} (N - i) = \sum_{k=1}^{N-1} k = \frac{(N-1)N}{2} = \binom{N}{2}$$

On peut aussi raisonner comme suit : il y a autant de couples (i, j) de $[\![1, N]\!]^2$ vérifiant $i < j$ que de parties à deux éléments de $[\![1, N]\!]$, en effet une partie de $[\![1, N]\!]$ à deux éléments $\{i, j\}$ permet de définir un et un seul couple (i, j) avec $i < j$ et réciproquement.

On a donc

$$\sum_{1 \leqslant i < j \leqslant N} 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) = 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) \sum_{1 \leqslant i < j \leqslant N} 1 = 2\exp\left(-\frac{\varepsilon^2 n}{2}\right) \cdot \binom{N}{2} = N(N-1)\exp\left(-\frac{\varepsilon^2 n}{2}\right)$$

Finalement on obtient : $\boxed{\mathbb{P}\left(\bigcup_{1 \leqslant i < j \leqslant N} \left(|\langle X^i \mid X^j \rangle| \geqslant \varepsilon\right)\right) \leqslant N(N-1)\exp\left(-\frac{\varepsilon^2 n}{2}\right)}$

Q 45. On suppose que $n \geqslant 4\dfrac{\ln N}{\varepsilon^2}$, alors $\dfrac{\varepsilon^2 n}{2} \geqslant 2\ln N$ et donc $\exp\left(-\dfrac{\varepsilon^2 n}{2}\right) \leqslant \exp(-2\ln N)$. On déduit de l'inégalité de la question 44 que :

$$\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N}\left(|\langle X^i \mid X^j\rangle| \geqslant \varepsilon\right)\right) \leqslant \frac{N-1}{N} < 1$$

Q 46. Pour tout entier naturel N inférieur ou égal à $\exp\left(\dfrac{\varepsilon^2 n}{4}\right)$, on a $n \geqslant 4\dfrac{\ln N}{\varepsilon^2}$ et d'après ce qui précède : $\mathbb{P}\left(\bigcup_{1\leqslant i<j\leqslant N}\left(|\langle X^i \mid X^j\rangle| \geqslant \varepsilon\right)\right) < 1$, ce qui donne par passage au complémentaire :

$$\mathbb{P}\left(\bigcap_{1\leqslant i<j\leqslant N}\left(|\langle X^i \mid X^j\rangle| < \varepsilon\right)\right) > 0$$

L'événement $\left(\bigcap_{1\leqslant i<j\leqslant N}\left(|\langle X^i \mid X^j\rangle| < \varepsilon\right)\right)$ n'est donc pas vide, alors il existe $\omega \in \Omega$ tel que la famille $u_1 = X^1(\omega), \ldots, u_N = X^N(\omega)$ est une famille de N vecteurs unitaires de $\mathbb{R}^n$ vérifiant :
$\forall (i,j) \in [\![1,N]\!]^2 \quad i \neq j \Longrightarrow |\langle u_i \mid u_j\rangle| < \varepsilon$ et donc $C(u) \leqslant \varepsilon$.
Le paramètre de cohérence de la famille $(u_1, \ldots, u_N)$ est majoré par ε.

Fin