

## Corrigé du DS 9 - MPSI A - 2021-2022

### Exercice 1

Voir exercice 64 de la banque CCINP.

### Exercice 2

**1** Remarquons d'abord que pour tout  $A \in \mathcal{M}_n(\mathbb{R})$ ,  $\text{Tr}(A) \in \mathbb{R}$ . Soient maintenant  $A, B \in \mathcal{M}_n(\mathbb{R})$  et  $\lambda \in \mathbb{R}$ . On calcule

$$\begin{aligned} \text{Tr}(\lambda A + B) &= \sum_{i=1}^n (\lambda A + B)_{ii} \\ &= \sum_{i=1}^n (\lambda A_{ii} + B_{ii}) \\ &= \lambda \sum_{i=1}^n A_{ii} + \sum_{i=1}^n B_{ii} \\ \text{Tr}(\lambda A + B) &= \lambda \text{Tr}(A) + \text{Tr}(B) \end{aligned}$$

On conclut que

L'application Trace est une forme linéaire sur  $\mathcal{M}_n(\mathbb{R})$ .

En outre, pour  $A, B \in \mathcal{M}_n(\mathbb{R})$ ,

$$\begin{aligned} \text{Tr}(AB) &= \sum_{i=1}^n (AB)_{ii} \\ &= \sum_{i=1}^n \sum_{k=1}^n A_{ik} B_{ki} \\ &= \sum_{k=1}^n \sum_{i=1}^n B_{ki} A_{ik} \\ &= \sum_{k=1}^n (BA)_{kk} \\ \text{Tr}(AB) &= \text{Tr}(BA) \end{aligned}$$

La permutation des deux sommes (finies) étant possible du fait que leurs indices sont indépendants. On a ainsi montré que

$$\forall (A, B) \in \mathcal{M}_n(\mathbb{R})^2 \quad \text{Tr}(AB) = \text{Tr}(BA)$$

**2** Rappelons qu'un produit scalaire est une forme bilinéaire symétrique définie positive. Notons  $\varphi$  l'application introduite dans l'énoncé par

$$\forall (A, B) \in \mathcal{M}_n(\mathbb{R})^2 \quad \varphi(A, B) = \text{Tr}(A^T B)$$

Soient  $A, B \in \mathcal{M}_n(\mathbb{R})$ . Étant donné que la trace est invariante par transposition,

$$\varphi(A, B) = \text{Tr}(A^T B) = \text{Tr}\left((A^T B)^T\right) = \text{Tr}(B^T A) = \varphi(B, A)$$

L'application  $\varphi$  est par conséquent symétrique.

Soient maintenant  $A, B, C \in \mathcal{M}_n(\mathbb{R})$  et  $\lambda \in \mathbb{R}$ . On a, par linéarité de la trace,

$$\begin{aligned}\varphi(A, \lambda B + C) &= \text{Tr}(A^T(\lambda B + C)) \\ &= \lambda \text{Tr}(A^T B) + \text{Tr}(A^T C) \\ \varphi(A, \lambda B + C) &= \lambda \varphi(A, B) + \varphi(A, C)\end{aligned}$$

ce qui prouve que  $\varphi$  est linéaire à droite. Comme elle est symétrique, on en déduit la linéarité à gauche, c'est donc une forme bilinéaire.

Enfin, soit  $A \in \mathcal{M}_n(\mathbb{R})$ . On remarque que

$$\varphi(A, A) = \text{Tr}(A^T A) = \sum_{i=1}^n (A^T A)_{ii} = \sum_{i=1}^n \sum_{j=1}^n (A^T)_{ij} A_{ji} = \sum_{i=1}^n \sum_{j=1}^n A_{ji}^2 \geq 0$$

puisque une somme de carrés de réels est un réel positif. Cela montre que  $\varphi$  est positive. Et comme une somme de réels positifs est nulle si, et seulement si, tous les termes sont nuls,

$$\begin{aligned}\varphi(A, A) = 0 &\Leftrightarrow \forall (i, j) \in \llbracket 1; n \rrbracket^2 \quad A_{ji}^2 = 0 \\ &\Leftrightarrow \forall (i, j) \in \llbracket 1; n \rrbracket^2 \quad A_{ji} = 0 \\ \varphi(A, A) = 0 &\Leftrightarrow A = 0_n\end{aligned}$$

Autrement dit,  $\varphi$  est définie positive. En conclusion,

L'application  $(A, B) \mapsto \text{Tr}(A^T B)$  définit un produit scalaire sur  $\mathcal{M}_n(\mathbb{R})$ .

**3** Soit  $A \in \mathcal{M}_n(\mathbb{R})$  telle que  $A^T A = 0_n$ . Alors

$$\varphi(A, A) = \text{Tr}(A^T A) = \text{Tr}(0_n) = 0$$

Compte tenu du caractère défini positif du produit scalaire, il s'ensuit

Si  $A \in \mathcal{M}_n(\mathbb{R})$  vérifie  $A^T A = 0_n$  alors  $A = 0_n$ .

## Problème - Autour des matrices aléatoires

### I. MATRICES ALÉATOIRES À COEFFICIENTS DANS $\{-1, 1\}$

**1** Si  $X$  suit la loi  $\mathcal{R}$ , elle prend ses valeurs dans  $\{-1, 1\}$ . La variable aléatoire  $\frac{1}{2}(X+1)$  prend donc ses valeurs dans  $\{0, 1\}$  et sa loi est donnée par

$$\mathbb{P}\left(\frac{1}{2}(X+1) = 0\right) = \mathbb{P}(X = -1) = \frac{1}{2} \quad \mathbb{P}\left(\frac{1}{2}(X+1) = 1\right) = \mathbb{P}(X = 1) = \frac{1}{2}$$

Autrement dit,

La variable aléatoire  $\frac{1}{2}(X+1)$  suit la loi de Bernoulli de paramètre  $\frac{1}{2}$ .

**2** Soit  $X$  une variable aléatoire suivant la loi  $\mathcal{R}$ . Par définition de l'espérance,

$$\mathbb{E}(X) = -1 \times \mathbb{P}(X = -1) + 1 \times \mathbb{P}(X = 1) = -\frac{1}{2} + \frac{1}{2} = 0$$

En outre, si  $X$  suit la loi  $\mathcal{R}$ , la variable aléatoire  $X^2$  est constante égale à 1. On en déduit  $\mathbb{E}(X^2) = 1$  puis par la formule de König-Huygens,

$$\mathbb{V}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2 = 1 - 0 = 1$$

On a montré que

Une variable aléatoire suivant la loi  $\mathcal{R}$  a une espérance nulle et une variance égale à 1.

**3** Si  $X$  et  $Y$  sont à valeurs dans  $\{-1, 1\}$ , leur produit est également à valeurs dans  $\{-1, 1\}$ . L'événement  $\{XY = 1\}$  est alors l'union disjointe des événements  $\{X = 1, Y = 1\}$  et  $\{X = -1, Y = -1\}$  et par indépendance de  $X$  et  $Y$ ,

$$\begin{aligned} \mathbb{P}(XY = 1) &= \mathbb{P}(\{X = 1, Y = 1\} \cup \{X = -1, Y = -1\}) \\ &= \mathbb{P}(X = 1, Y = 1) + \mathbb{P}(X = -1, Y = -1) \\ &= \mathbb{P}(X = 1)\mathbb{P}(Y = 1) + \mathbb{P}(X = -1)\mathbb{P}(Y = -1) \\ &= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \\ \mathbb{P}(XY = 1) &= \frac{1}{2} \end{aligned}$$

De même,  $\mathbb{P}(XY = -1) = \mathbb{P}(\{X = 1, Y = -1\} \cup \{X = -1, Y = 1\})$

$$\begin{aligned} &= \mathbb{P}(X = 1, Y = -1) + \mathbb{P}(X = -1, Y = 1) \\ &= \mathbb{P}(X = 1)\mathbb{P}(Y = -1) + \mathbb{P}(X = -1)\mathbb{P}(Y = 1) \\ &= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \\ \mathbb{P}(XY = -1) &= \frac{1}{2} \end{aligned}$$

La variable aléatoire  $XY$  suit également la loi  $\mathcal{R}$ .

**4a** Un calcul rapide donne

$$\forall i \in \llbracket 1; n \rrbracket \quad E_i = \frac{1}{2}(V - (V - 2E_i))$$

**4b** Remarquons que  $V$  est la matrice colonne dont tous les coefficients sont égaux à 1, et que pour tout  $i \in \llbracket 1; n \rrbracket$ ,  $V - 2E_i$  est la matrice colonne dont tous les coefficients sont égaux à 1 sauf celui en  $i$ -ème position qui vaut  $-1$ . Toutes ces matrices colonnes sont donc des éléments de  $\mathcal{V}_{n,1}(\mathbb{R})$ . Il s'ensuit

$$\mathcal{M}_{n,1}(\mathbb{R}) = \text{Vect}(E_1, \dots, E_n) \subset \text{Vect}(V, V - 2E_1, \dots, V - 2E_n) \subset \text{Vect}(\mathcal{V}_{n,1}(\mathbb{R}))$$

Mais comme  $\mathcal{V}_{n,1}(\mathbb{R}) \subset \mathcal{M}_{n,1}(\mathbb{R})$  qui est un  $\mathbb{R}$ -espace vectoriel, on a aussi l'inclusion réciproque  $\text{Vect}(\mathcal{V}_{n,1}(\mathbb{R})) \subset \mathcal{M}_{n,1}(\mathbb{R})$ . En conclusion,

$$\mathcal{M}_{n,1}(\mathbb{R}) = \text{Vect}(\mathcal{V}_{n,1}(\mathbb{R}))$$

**5** Posons  $\mathcal{A} = \{k \in \mathbb{N}^*, (C_1, \dots, C_k) \text{ est libre}\}$  et raisonnons par analyse-synthèse. Supposons qu'il existe un tel  $j$ . L'ensemble  $\mathcal{A}$  est une partie de  $\mathbb{N}$ , non vide étant donné qu'elle contient 1 (puisque  $C_1$  est supposée non nulle). De plus,  $\mathcal{A}$  est majoré par  $n$  puisque par hypothèse la famille  $(C_1, \dots, C_n)$  est liée. L'ensemble  $\mathcal{A}$  possède donc un maximum, appelons-le  $j'$ .

Comme la famille  $(C_1, \dots, C_j)$  est libre, on a  $j \in \mathcal{A}$ , et par conséquent  $j \leq j'$ . Mais la famille  $(C_1, \dots, C_{j+1})$  est liée, donc  $j+1$  est un majorant de  $\mathcal{A}$  qui n'appartient pas à cet ensemble. Il s'ensuit  $j' < j+1$ , autrement dit  $j' \leq j$ . En conclusion,  $j = j'$  et  $j$  est défini de façon unique.

Réciproquement, si on pose  $j = \max \mathcal{A}$ , celui-ci vérifie  $j \in \llbracket 1, n-1 \rrbracket$  puisque  $n$  n'appartient pas à l'ensemble  $\mathcal{A}$ . Par maximalité de  $j$ , l'élément  $j+1$  n'appartient pas à l'ensemble  $\mathcal{A}$  donc la famille  $(C_1, \dots, C_{j+1})$  est liée. Comme  $(C_1, \dots, C_j)$  est libre, cela signifie que  $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$ .

Il existe un unique  $j \in \llbracket 1; n-1 \rrbracket$  tel que la famille  $(C_1, \dots, C_j)$  est libre et  $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$ .

**6** Suivons l'indication de l'énoncé. Appelons  $A$  la matrice de  $\mathcal{M}_{n,d}(\mathbb{R})$  dont les colonnes sont  $U_1, \dots, U_d$ . Le rang de cette matrice est égal au rang de la famille  $(U_1, \dots, U_d)$ , autrement dit à  $d$  puisque cette famille est libre par hypothèse. Par conséquent, la famille des lignes de  $A$  est aussi de rang  $d$ . En notant  $L_1, \dots, L_n$  les lignes de  $A$ , il existe  $i_1, \dots, i_d \in \llbracket 1; n \rrbracket$  vérifiant  $i_1 < \dots < i_d$  tels que toute ligne de  $A$  soit combinaison linéaire de  $L_{i_1}, \dots, L_{i_d}$ . Pour tout  $j \in \llbracket 1; n \rrbracket$ , soient  $\lambda_{j,1}, \dots, \lambda_{j,d} \in \mathbb{R}$  tels que

$$L_j = \sum_{k=1}^d \lambda_{j,k} L_{i_k}$$

Considérons désormais l'application

$$h: \begin{cases} \text{H} & \longrightarrow \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{cases}$$

Pour tous  $\lambda \in \mathbb{R}$  et  $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ,  $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \text{H}$ ,

$$h(\lambda x + y) = h \begin{pmatrix} \lambda x_1 + y_1 \\ \vdots \\ \lambda x_n + y_n \end{pmatrix} = \begin{pmatrix} \lambda x_{i_1} + y_{i_1} \\ \vdots \\ \lambda x_{i_d} + y_{i_d} \end{pmatrix} = \lambda \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} + \begin{pmatrix} y_{i_1} \\ \vdots \\ y_{i_d} \end{pmatrix} = \lambda h(x) + h(y)$$

ce qui prouve que  $h$  est linéaire.

Soit maintenant  $X \in \text{Ker}(h)$ . Comme  $X \in \text{H}$ , il existe  $z_1, \dots, z_d \in \mathbb{R}$  tels que

$$X = \sum_{k=1}^d z_k U_k = AZ \quad \text{en posant } Z = \begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix}$$

Par suite,

$$X = AZ = \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} Z = \begin{pmatrix} L_1 Z \\ \vdots \\ L_n Z \end{pmatrix}$$

On en déduit

$$0 = h(X) = \begin{pmatrix} L_{i_1} Z \\ \vdots \\ L_{i_d} Z \end{pmatrix}$$

autrement dit  $L_{i_1}Z = \dots = L_{i_d}Z = 0$ . Mais alors, pour tout  $j \in \llbracket 1; n \rrbracket$ ,

$$L_j Z = \sum_{k=1}^d \lambda_{j,k} L_{i_k} Z = \sum_{k=1}^d \lambda_{j,k} \times 0 = 0$$

ce qui prouve que  $X = 0$  donc que  $h$  est injective. Comme la famille  $(U_1, \dots, U_d)$  est libre,  $\dim(H) = d = \dim(\mathcal{M}_{d,1}(\mathbb{R}))$  ce qui permet de conclure que  $h$  réalise un isomorphisme d'espaces vectoriels. En particulier,

L'application  $h$  est bijective.

**7** Le sous-espace vectoriel  $\mathcal{W}$  est engendré par une famille libre de  $d$  matrices de  $\mathcal{M}_{n,1}(\mathbb{R})$ . D'après la question précédente, il existe  $i_1, \dots, i_d \in \llbracket 1; n \rrbracket$  vérifiant  $i_1 < \dots < i_d$  tels que l'application

$$h: \begin{cases} \mathcal{W} & \longrightarrow \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \longmapsto \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{cases}$$

est bijective. Par conséquent, sa restriction à  $\mathcal{W} \cap \mathcal{V}_{n,1}$  est injective, elle réalise donc une bijection entre  $\mathcal{W} \cap \mathcal{V}_{n,1}$  et  $h(\mathcal{W} \cap \mathcal{V}_{n,1})$ . Il s'ensuit

$$\text{Card}(\mathcal{W} \cap \mathcal{V}_{n,1}) = \text{Card}(h(\mathcal{W} \cap \mathcal{V}_{n,1}))$$

Tous les éléments de  $\mathcal{W} \cap \mathcal{V}_{n,1}$  ayant leurs coefficients à valeurs dans  $\{-1, 1\}$ , on a  $h(\mathcal{W} \cap \mathcal{V}_{n,1}) \subset \mathcal{V}_{d,1}$  d'où  $\text{Card}(h(\mathcal{W} \cap \mathcal{V}_{n,1})) \leq \text{Card}(\mathcal{V}_{d,1})$ . Enfin, choisir un élément de  $\mathcal{V}_{d,1}$  revient à choisir une  $d$ -liste d'éléments de  $\{-1, 1\}$ , ce qui donne  $\text{Card}(\mathcal{V}_{d,1}) = 2^d$ . En résumé

$$\text{Card}(\mathcal{W} \cap \mathcal{V}_{n,1}) \leq 2^d$$

**8** Par linéarité de l'espérance,

$$\mathbb{E}(\tau_n) = \mathbb{E}(\text{Tr}(M_n)) = \mathbb{E}\left(\sum_{i=1}^n m_{i,i}\right) = \sum_{i=1}^n \mathbb{E}(m_{i,i}) = 0$$

puisque les  $m_{i,i}$  sont toutes d'espérance nulle d'après la question 2. En outre, les variables aléatoires  $m_{1,1}, \dots, m_{n,n}$  étant mutuellement indépendantes,

$$\mathbb{V}(\tau_n) = \mathbb{V}(\text{Tr}(M_n)) = \mathbb{V}\left(\sum_{i=1}^n m_{i,i}\right) = \sum_{i=1}^n \mathbb{V}(m_{i,i}) = \sum_{i=1}^n 1 = n$$

L'espérance de  $\tau_n$  est nulle et sa variance vaut  $n$ .

**9** Pour tous  $i, j \in \llbracket 1; n \rrbracket$ , on note  $(\widehat{M}_n)_{i,j}$  la matrice obtenue en supprimant la  $i$ -ème ligne et la  $j$ -ème colonne de la matrice  $M_n$ . En développant le déterminant par rapport à la première ligne, on obtient par linéarité de l'espérance

$$\begin{aligned} \mathbb{E}(\delta_n) &= \mathbb{E}(\det(M_n)) \\ &= \mathbb{E}\left(\sum_{j=1}^n (-1)^{1+j} m_{1,j} \det((\widehat{M}_n)_{1,j})\right) \\ \mathbb{E}(\delta_n) &= \sum_{j=1}^n (-1)^{1+j} \mathbb{E}(m_{1,j} \det((\widehat{M}_n)_{1,j})) \end{aligned}$$

Mais pour tout  $j \in \llbracket 1; n \rrbracket$ ,  $\det((\widehat{M}_n)_{1,j})$  s'exprime en fonction des variables aléatoires  $m_{i,k}$  où  $i, k \in \llbracket 1; n \rrbracket$ ,  $i \neq 1$  et  $k \neq j$ . D'après le lemme des coalitions rappelé en préambule, les variables aléatoires  $m_{1,j}$  et  $\det((\widehat{M}_n)_{1,j})$  sont indépendantes, et il s'ensuit

$$\mathbb{E}(\delta_n) = \sum_{j=1}^n (-1)^{1+j} \mathbb{E}(m_{1,j}) \mathbb{E}(\det((\widehat{M}_n)_{1,j})) = 0$$

puisque pour tout  $j \in \llbracket 1; n \rrbracket$ ,  $\mathbb{E}(m_{1,j}) = 0$ .

La variable aléatoire  $\delta_n$  a une espérance nulle.

Autre méthode :

$$\begin{aligned} \mathbb{E}(\delta_n) &= \mathbb{E}(\det(M_n)) \\ &= \mathbb{E} \left( \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^n m_{\sigma(k),k} \right) \\ &= \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \mathbb{E} \left( \prod_{k=1}^n m_{\sigma(k),k} \right) \\ &= \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{k=1}^n \mathbb{E}(m_{\sigma(k),k}) \\ \mathbb{E}(\delta_n) &= 0 \end{aligned}$$

puisque les  $m_{i,j}$  sont indépendantes et sont toutes d'espérance nulle.

**10** Suivons l'indication et montrons par récurrence sur  $n \in \mathbb{N}^*$  la proposition  $\mathcal{P}(n)$  : « Pour toutes variables aléatoires  $(m_{i,j})_{1 \leq i, j \leq n}$  mutuellement indépendantes de loi  $\mathcal{R}$ , si  $M_n = (m_{i,j})_{1 \leq i, j \leq n}$ , on a  $\mathbb{V}(\det(M_n)) = n!$  ».

- $\mathcal{P}(1)$  est vraie puisque si  $m_{1,1}$  est une variable aléatoire de loi  $\mathcal{R}$ , on a

$$\mathbb{V}(\det(M_1)) = \mathbb{V}(m_{1,1}) = 1 = 1!$$

d'après la question 2.

- $\mathcal{P}(n) \implies \mathcal{P}(n+1)$  : soit  $n \in \mathbb{N}^*$  tel que  $\mathcal{P}(n)$  soit vraie. Soient des variables aléatoires  $(m_{i,j})_{1 \leq i, j \leq n+1}$  mutuellement indépendantes de loi  $\mathcal{R}$ , soit  $M_{n+1} = (m_{i,j})_{1 \leq i, j \leq n+1}$ . En développant par rapport à la première ligne, on peut écrire

$$\det(M_{n+1}) = \sum_{j=1}^{n+1} (-1)^{1+j} m_{1,j} \det \left( (\widehat{M}_{n+1})_{1,j} \right)$$

D'après la question précédente, l'espérance de  $\det(M_{n+1})$  est nulle. Par le théorème de König-Huygens, la variance s'écrit alors

$$\mathbb{V}(\det(M_{n+1})) = \mathbb{E}(\det(M_{n+1})^2)$$

Or

$$\det(M_{n+1})^2 = \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} (-1)^{i+j+2} m_{1,i} m_{1,j} \det \left( (\widehat{M}_{n+1})_{1,i} \right) \det \left( (\widehat{M}_{n+1})_{1,j} \right)$$

et en outre, les variables aléatoires  $m_{1,i}$  et  $m_{1,j}$  n'apparaissent pas dans les déterminants mineurs puisque l'on a supprimé la première ligne. D'après le

lemme des coalitions, pour tous  $i, j \in \llbracket 1; n+1 \rrbracket$  avec  $i \neq j$ , les variables aléatoires  $m_{1,i}m_{1,j}$  et  $\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,j}\right)$  sont indépendantes. Par conséquent, pour tous  $i, j \in \llbracket 1; n+1 \rrbracket$  avec  $i \neq j$ ,

$$\begin{aligned} \mathbb{E}\left(m_{1,i}m_{1,j}\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,j}\right)\right) \\ = \mathbb{E}(m_{1,i}m_{1,j})\mathbb{E}\left(\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,j}\right)\right) \end{aligned}$$

Comme  $\mathbb{E}(m_{1,i}m_{1,j}) = \mathbb{E}(m_{1,i})\mathbb{E}(m_{1,j}) = 0$  par indépendance de  $m_{1,i}$  et  $m_{1,j}$ , on en déduit

$$\mathbb{E}\left(m_{1,i}m_{1,j}\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,j}\right)\right) = 0$$

Par linéarité de l'espérance, en repartant de  $\mathbb{V}(\det(\mathbb{M}_{n+1})) = \mathbb{E}(\det(\mathbb{M}_{n+1})^2)$ , il s'ensuit

$$\mathbb{V}(\det(\mathbb{M}_{n+1})) = \sum_{i=1}^{n+1} (-1)^{2i} \mathbb{E}((m_{1,i})^2) \mathbb{E}\left(\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)^2\right)$$

puisque tous les termes de la somme double correspondant à des indices différents sont nuls au vu de ce qui précède. Mais on a aussi, pour tout  $i \in \llbracket 1; n+1 \rrbracket$ ,

$$\mathbb{E}((m_{1,i})^2) = \mathbb{V}(m_{1,i}) = 1$$

et par hypothèse de récurrence,

$$\mathbb{E}\left(\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)^2\right) = \mathbb{V}\left(\det\left(\widehat{(\mathbb{M}_{n+1})}_{1,i}\right)\right) = n!$$

étant donné que ces déterminants mineurs sont de taille  $n$ .

Il vient finalement

$$\mathbb{V}(\det(\mathbb{M}_{n+1})) = \sum_{i=1}^{n+1} (1 \times n!) = (n+1)n! = (n+1)!$$

ce qui prouve que  $\mathcal{P}(n+1)$  est vraie.

- **Conclusion** : Pour tout  $n \in \mathbb{N}^*$  et toutes variables aléatoires  $(m_{i,j})_{1 \leq i, j \leq n}$  mutuellement indépendantes de loi  $\mathcal{R}$ , si  $\mathbb{M}_n = (m_{i,j})_{1 \leq i, j \leq n}$ , on a

$$\mathbb{V}(\det(\mathbb{M}_n)) = n!$$

En particulier

$$\boxed{\mathbb{V}(\delta_n) = n!}$$

**11** Remarquons d'abord que

$$\mathbb{M}_2 \notin \text{GL}_2(\mathbb{R}) \iff \det(\mathbb{M}_2) = 0 \iff m_{11}m_{22} = m_{21}m_{12}$$

Mais d'après la question 3, les variables aléatoires  $m_{11}m_{22}$  et  $m_{21}m_{12}$  suivent aussi la loi  $\mathcal{R}$ , et elles sont indépendantes d'après le lemme des coalitions. Par conséquent, si on pose  $p_1 = m_{11}m_{22}$  et  $p_2 = m_{21}m_{12}$ ,

$$\begin{aligned} \mathbb{P}(p_1 = p_2) &= \mathbb{P}(p_1 = 1, p_2 = 1) + \mathbb{P}(p_1 = -1, p_2 = -1) \\ &= \mathbb{P}(p_1 = 1)\mathbb{P}(p_2 = 1) + \mathbb{P}(p_1 = -1)\mathbb{P}(p_2 = -1) \\ &= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} \\ \mathbb{P}(p_1 = p_2) &= \frac{1}{2} \end{aligned}$$

Ainsi  $\mathbb{P}(M_2 \notin \text{GL}_2(\mathbb{R})) = \mathbb{P}(p_1 = p_2) = 1/2$  d'où en passant au complémentaire,

$$\mathbb{P}(M_2 \in \text{GL}_2(\mathbb{R})) = 1 - \mathbb{P}(M \notin \text{GL}_2(\mathbb{R})) = \frac{1}{2}$$

**12a** Par indépendance mutuelle des variables aléatoires considérées,

$$\mathbb{P}\left(\bigcap_{k=1}^n \{c_k = \varepsilon_k\}\right) = \prod_{k=1}^n \mathbb{P}(c_k = \varepsilon_k) = \prod_{k=1}^n \frac{1}{2} = \frac{1}{2^n}$$

**12b** Soit  $\omega \in \Omega$ . S'il existe  $\varepsilon \in \{-1, 1\}$  telle que  $C'(\omega) = \varepsilon C(\omega)$ , la famille de vecteurs  $(C(\omega), C'(\omega))$  est liée puisque ses deux vecteurs sont colinéaires. Réciproquement, supposons que la famille  $(C(\omega), C'(\omega))$  soit liée. Ces deux matrices colonnes étant non nulles, il existe  $\varepsilon \in \mathbb{R}^*$  tel que  $C'(\omega) = \varepsilon C(\omega)$ . En particulier,  $c_1(\omega) = \varepsilon c'_1(\omega)$  donc comme  $c'_1(\omega) \neq 0$ ,

$$\varepsilon = \frac{c_1(\omega)}{c'_1(\omega)} \in \{-1, 1\}$$

En conclusion,

Pour tout  $\omega \in \Omega$ , la famille  $(C(\omega), C'(\omega))$  est liée si, et seulement si, il existe  $\varepsilon \in \{-1, 1\}$  telle que  $C'(\omega) = \varepsilon C(\omega)$ .

**12c** D'après la question précédente,

$$\mathbb{P}((C, C') \text{ est liée}) = \mathbb{P}(\{C = C'\} \cup \{C = -C'\}) = \mathbb{P}(C = C') + \mathbb{P}(C = -C')$$

Comme  $C(\Omega) = \mathcal{V}_{n,1}(\mathbb{R})$ , la famille  $(\{C = c\})_{c \in \mathcal{V}_{n,1}(\mathbb{R})}$  forme un système complet d'événements. Il s'ensuit avec la formule des probabilités totales :

$$\mathbb{P}(C = C') = \sum_{c \in \mathcal{V}_{n,1}(\mathbb{R})} \mathbb{P}(C = C' | C = c) \mathbb{P}(C = c) = \sum_{c \in \mathcal{V}_{n,1}(\mathbb{R})} \mathbb{P}(C' = c) \mathbb{P}(C = c)$$

Mais, d'après la question 12a, pour tout  $c \in \mathcal{V}_{n,1}(\mathbb{R})$ ,

$$\mathbb{P}(C = c) = \mathbb{P}(C' = c) = \frac{1}{2^n}$$

$$\text{d'où} \quad \mathbb{P}(C = C') = \text{Card}(\mathcal{V}_{n,1}(\mathbb{R})) \frac{1}{2^n} \frac{1}{2^n} = \frac{1}{2^n}$$

puisque  $\text{Card}(\mathcal{V}_{n,1}(\mathbb{R})) = 2^n$  (voir la question 7). On trouve de la même manière que  $\mathbb{P}(C = -C') = 1/2^n$ . En conclusion,

$$\mathbb{P}((C, C') \text{ est liée}) = \frac{1}{2^n} + \frac{1}{2^n} = \frac{1}{2^{n-1}}$$

**13** Soit  $\omega \in \Omega$ . Si la famille  $(C_1(\omega), \dots, C_n(\omega))$  est libre, alors  $\omega \in R_n$  et pour tout  $j \in \llbracket 1; n-1 \rrbracket$ ,  $\omega \notin R_j$  puisque l'événement  $R_j$  est inclus dans l'événement  $\{(C_1(\omega), \dots, C_n(\omega)) \text{ est liée}\} = \overline{R_n}$ . A contrario, si  $(C_1(\omega), \dots, C_n(\omega))$  est liée, d'après la question 5 il existe un unique  $j \in \llbracket 1; n-1 \rrbracket$  tel que  $(C_1(\omega), \dots, C_j(\omega))$  soit libre et  $C_{j+1}(\omega) \in \text{Vect}(C_1(\omega), \dots, C_j(\omega))$ , autrement dit il existe un unique  $j \in \llbracket 1; n-1 \rrbracket$  tel que  $\omega \in R_j$ .



Dans tous les cas, il existe un unique  $j \in \llbracket 1; n \rrbracket$  tel que  $\omega \in R_j$ , ce qui prouve que

$$\Omega = \bigcup_{j=1}^n R_j$$

et par unicité de  $j$  dans le raisonnement précédent, cette union est disjointe. On en conclut que

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

**14a** Remarquons tout d'abord que, d'après la question précédente,

$$\{M_n \notin \text{GL}_n(\mathbb{R})\} = \{(C_1, \dots, C_n) \text{ est liée}\} = \overline{R_n} = \bigcup_{j=1}^{n-1} R_j$$

L'union étant disjointe, il s'ensuit

$$\mathbb{P}(M_n \notin \text{GL}_n(\mathbb{R})) = \sum_{j=1}^{n-1} \mathbb{P}(R_j)$$

Or, pour tout  $j \in \llbracket 1; n-1 \rrbracket$ ,  $R_j \subset \{C_{j+1} \in \text{Vect}(C_1, \dots, C_j)\}$ . D'où, par croissance de la probabilité,

$$\forall j \in \llbracket 1; n-1 \rrbracket \quad \mathbb{P}(R_j) \leq \mathbb{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j))$$

En conclusion,

$$\boxed{\mathbb{P}(M_n \notin \text{GL}_n(\mathbb{R})) \leq \sum_{j=1}^{n-1} \mathbb{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j))}$$

**14b** Soit  $j \in \llbracket 1; n-1 \rrbracket$ . Notons  $p_j = \mathbb{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j))$ . Comme les matrices colonnes aléatoires  $C_1, \dots, C_j$  prennent leurs valeurs dans  $\mathcal{V}_{n,1}$ , la famille d'événements

$$\left\{ (C_1 = v_1) \cap \dots \cap (C_j = v_j) \right\}_{(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j}$$

forme un système complet d'événements. On en déduit, grâce à la formule des probabilités totales,

$$p_j = \sum_{(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j} \mathbb{P} \left( C_{j+1} \in \text{Vect}(C_1, \dots, C_j) \mid \bigcap_{k=1}^j \{C_k = v_k\} \right) \mathbb{P} \left( \bigcap_{k=1}^j \{C_k = v_k\} \right)$$

Or, pour tout  $(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j$ ,

$$\begin{aligned} & \mathbb{P} \left( C_{j+1} \in \text{Vect}(C_1, \dots, C_j) \mid \bigcap_{k=1}^j \{C_k = v_k\} \right) \\ &= \mathbb{P} \left( C_{j+1} \in \text{Vect}(v_1, \dots, v_j) \mid \bigcap_{k=1}^j \{C_k = v_k\} \right) \end{aligned}$$

Puisque la variable aléatoire  $C_{j+1}$  est indépendante de  $C_1, \dots, C_j$ , il s'ensuit

$$\mathbb{P} \left( C_{j+1} \in \text{Vect}(C_1, \dots, C_j) \mid \bigcap_{k=1}^j \{C_k = v_k\} \right) = \mathbb{P}(C_{j+1} \in \text{Vect}(v_1, \dots, v_j))$$

ce qui permet de conclure que

$$p_j = \sum_{(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j} \mathbb{P}(C_{j+1} \in \text{Vect}(v_1, \dots, v_j)) \mathbb{P}\left(\bigcap_{k=1}^j \{C_k = v_k\}\right)$$

**14c** Les variables aléatoires  $C_1, \dots, C_j$  étant mutuellement indépendantes, pour tout  $(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j$ ,

$$\mathbb{P}\left(\bigcap_{k=1}^j \{C_k = v_k\}\right) = \prod_{k=1}^j \mathbb{P}(C_k = v_k) = \prod_{k=1}^j \frac{1}{2^n} = \frac{1}{2^{nj}}$$

Par ailleurs, soient  $\mathcal{W} = \text{Vect}(v_1, \dots, v_j)$  et  $d$  la dimension de ce sous-espace vectoriel de  $\mathcal{M}_{n,1}(\mathbb{R})$ . Celle-ci vérifie  $d \leq j$  puisque la famille  $(v_1, \dots, v_j)$  est génératrice de  $\mathcal{W}$  et de cardinal  $j$ . D'après la question 7,

$$\text{Card}(\mathcal{W} \cap \mathcal{V}_{n,1}(\mathbb{R})) \leq 2^d \leq 2^j$$

Les variables aléatoires  $m_{1,j+1}, \dots, m_{n,j+1}$  étant mutuellement indépendantes,  $C_{j+1}$  suit une loi uniforme sur  $\mathcal{V}_{n,1}$  d'après la question 12a. Par conséquent,

$$\mathbb{P}(C_{j+1} \in \mathcal{W}) = \mathbb{P}(C_{j+1} \in \mathcal{W} \cap \mathcal{V}_{n,1}(\mathbb{R})) = \frac{\text{Card}(\mathcal{W} \cap \mathcal{V}_{n,1}(\mathbb{R}))}{\text{Card}(\mathcal{V}_{n,1}(\mathbb{R}))} \leq \frac{2^j}{2^n} = 2^{j-n}$$

En utilisant le résultat de la question précédente, il s'ensuit

$$\begin{aligned} \mathbb{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j)) &\leq \sum_{(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j} 2^{j-n} \mathbb{P}\left(\bigcap_{k=1}^j \{C_k = v_k\}\right) \\ &= \sum_{(v_1, \dots, v_j) \in (\mathcal{V}_{n,1})^j} 2^{j-n} \frac{1}{2^{nj}} \\ &= \text{Card}((\mathcal{V}_{n,1})^j) 2^{j-n} \frac{1}{2^{nj}} \\ &= 2^{j-n} \end{aligned}$$

donc

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

**14d** D'après la question 14a,

$$\mathbb{P}(M_n \in \text{GL}_n(\mathbb{R})) = 1 - \mathbb{P}(M_n \notin \text{GL}_n(\mathbb{R})) \geq 1 - \sum_{j=1}^{n-1} \mathbb{P}(C_{j+1} \in \text{Vect}(C_1, \dots, C_j))$$

En introduisant le résultat de la question précédente, on en déduit

$$\mathbb{P}(M_n \in \text{GL}_n(\mathbb{R})) \geq 1 - \sum_{j=1}^{n-1} 2^{j-n}$$

Par suite, en effectuant le changement d'indice  $\alpha = j - 1$ ,

$$1 - \sum_{j=1}^{n-1} 2^{j-n} = 1 - \sum_{j=1}^{n-1} \frac{2^{j-1}}{2^{n-1}} = 1 - \frac{1}{2^{n-1}} \sum_{\alpha=0}^{n-2} 2^\alpha = 1 - \frac{1}{2^{n-1}} \frac{2^{n-1} - 1}{2 - 1} = \frac{1}{2^{n-1}}$$

En conclusion,

$$\mathbb{P}(M_n \in \text{GL}_n(\mathbb{R})) \geq \frac{1}{2^{n-1}}$$

## II. VECTEURS ALÉATOIRES UNITAIRES

**15** Remarquons d'abord que l'ensemble  $\{|\langle u_i | u_j \rangle|, (i, j) \in I^2, i \neq j\}$  est non vide puisque  $I$  possède au moins deux éléments. En outre, il est majoré par 1 puisque pour tout  $(i, j) \in I^2$  avec  $i \neq j$ , d'après l'inégalité de Cauchy-Schwarz,

$$|\langle u_i | u_j \rangle| \leq \|u_i\| \|u_j\| = 1$$

Cet ensemble possède par conséquent une borne supérieure, qui est inférieure ou égale à 1. En outre, tous les éléments de l'ensemble étant positifs ou nuls, cette borne supérieure est elle aussi positive ou nulle.

Le nombre réel  $C(u)$  existe et appartient à l'intervalle  $[0; 1]$ .

**16** Supposons  $C(u) = 0$ . Alors, pour tous  $i, j \in I$  avec  $i \neq j$ ,

$$0 \leq |\langle u_i | u_j \rangle| \leq C(u) = 0$$

dont on déduit  $\langle u_i | u_j \rangle = 0$ . Autrement dit, la famille  $(u_i)_{i \in I}$  est orthogonale, donc libre : ainsi elle est finie et de cardinal inférieur ou égal à la dimension de  $\mathcal{M}_{n,1}(\mathbb{R})$ , c'est-à-dire

L'ensemble  $\{u_i, i \in I\}$  est fini et de cardinal inférieur ou égal à  $n$ .

**17** Introduisons la fonction

$$f: \begin{cases} \mathbb{R} \longrightarrow \mathbb{R} \\ t \longmapsto \operatorname{ch}(t)e^{-t^2/2} \end{cases}$$

Cette fonction  $t \mapsto e^{-t^2/2}$  étant dérivable sur  $\mathbb{R}$  comme composée de deux fonctions dérivables, la fonction  $f$  est elle aussi dérivable sur  $\mathbb{R}$  comme produit de deux fonctions dérivables. Pour tout  $t \in \mathbb{R}$ ,

$$f'(t) = \operatorname{sh}(t)e^{-t^2/2} - t \operatorname{ch}(t)e^{-t^2/2} = (\operatorname{sh}(t) - t \operatorname{ch}(t))e^{-t^2/2}$$

Posons alors, pour tout  $t \in \mathbb{R}$ ,  $g(t) = \operatorname{sh}(t) - t \operatorname{ch}(t)$ . La fonction  $g$  ainsi définie est également dérivable sur  $\mathbb{R}$  et pour tout  $t \in \mathbb{R}$ ,

$$g'(t) = \operatorname{ch}(t) - \operatorname{ch}(t) - t \operatorname{sh}(t) = -t \operatorname{sh}(t) \leq 0$$

puisque  $t$  et  $\operatorname{sh}(t)$  sont toujours de même signe. Par conséquent la fonction  $g$  est décroissante sur  $\mathbb{R}$ , et comme  $g(0) = 0$ , elle est positive sur  $\mathbb{R}_-$  et négative sur  $\mathbb{R}_+$ . Or, l'exponentielle étant toujours strictement positive, la fonction  $f'$  est de même signe que  $g$ . On en déduit que  $f$  est croissante sur  $\mathbb{R}_-$  et décroissante sur  $\mathbb{R}_+$ , donc qu'elle admet un maximum en 0 qui vaut  $f(0) = 1$ . Ces informations sont résumées dans le tableau de variations ci-dessous.

	$-\infty$	$0$	$+\infty$
$g'$	$-$	$\vdots$	$-$
$g$			
$f'$	$+$	$0$	$-$
$f$			

Ainsi, pour tout  $t \in \mathbb{R}$ ,  $f(t) \leq 1$  ce qui signifie que

Pour tout réel  $t$ ,  $\text{ch}(t) \leq \exp\left(\frac{t^2}{2}\right)$ .

**18** Calculons pour commencer

$$\langle X | Y \rangle = \frac{1}{n} \sum_{i=1}^n X_i Y_i$$

d'où, pour tout  $t \in \mathbb{R}$ ,

$$\exp(t\langle X | Y \rangle) = \prod_{i=1}^n \exp\left(\frac{t}{n} X_i Y_i\right)$$

Or les variables aléatoires  $X_1 Y_1, \dots, X_n Y_n$  sont mutuellement indépendantes d'après le lemme des coalitions, et de loi  $\mathcal{R}$  d'après la question 3. Il s'ensuit

$$\begin{aligned} \mathbb{E}(\exp(t\langle X | Y \rangle)) &= \mathbb{E}\left(\prod_{i=1}^n \exp\left(\frac{t}{n} X_i Y_i\right)\right) \\ &= \prod_{i=1}^n \mathbb{E}\left(\exp\left(\frac{t}{n} X_i Y_i\right)\right) \\ \mathbb{E}(\exp(t\langle X | Y \rangle)) &= \prod_{i=1}^n \left(\frac{1}{2} \exp\left(\frac{t}{n}\right) + \frac{1}{2} \exp\left(\frac{-t}{n}\right)\right) \end{aligned}$$

la dernière égalité étant obtenue grâce au théorème de transfert.

Ainsi, Pour tout réel  $t$ ,  $\mathbb{E}(\exp(t\langle X | Y \rangle)) = \prod_{i=1}^n \text{ch}\left(\frac{t}{n}\right) = \text{ch}\left(\frac{t}{n}\right)^n$ .

**19** Soit  $t \in \mathbb{R}$ . D'après la question précédente,

$$\mathbb{E}(\exp(t\langle X | Y \rangle)) = \text{ch}\left(\frac{t}{n}\right)^n$$

Or, d'après la question 17 et la croissance sur  $\mathbb{R}_+$  de la fonction  $u \mapsto u^n$ ,

$$\text{ch}\left(\frac{t}{n}\right)^n \leq \exp\left(\frac{1}{2} \left(\frac{t}{n}\right)^2\right)^n = \exp\left(\frac{t^2}{2n}\right)$$

On a donc prouvé que

$$\text{Pour tout réel } t, \mathbb{E}(\exp(t\langle X | Y \rangle)) \leq \exp\left(\frac{t^2}{2n}\right).$$

**20** Soit  $t \in \mathbb{R}_+$ . Par stricte croissance sur  $\mathbb{R}$  de la fonction  $u \mapsto \exp(tu)$ , on a

$$\mathbb{P}(Z \geq \lambda) = \mathbb{P}(\exp(tZ) \geq \exp(t\lambda))$$

Et d'après l'inégalité de Markov, la variable aléatoire  $\exp(tZ)$  étant à valeurs positives,

$$\mathbb{P}(\exp(tZ) \geq \exp(t\lambda)) \leq \frac{\mathbb{E}(\exp(tZ))}{\exp(t\lambda)} \leq \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$$

En conclusion,

$$\forall t \in \mathbb{R}_+ \quad \mathbb{P}(Z \geq \lambda) \leq \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$$

**21** On remarque d'abord que

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

Or, pour tout  $t \in \mathbb{R}$ ,  $\exp(t(-Z)) = \exp((-t)Z)$  donc par hypothèse, cette variable aléatoire possède une espérance qui vérifie

$$\exp(t(-Z)) = \exp((-t)Z) \leq \exp\left(\frac{\sigma^2 (-t)^2}{2}\right) = \exp\left(\frac{\sigma^2 t^2}{2}\right)$$

Par conséquent, on peut également appliquer le résultat de la question 20 à la variable aléatoire  $-Z$ , ce qui donne

$$\forall t \in \mathbb{R}_+ \quad \mathbb{P}(-Z \geq \lambda) \leq \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$$

Il s'ensuit  $\forall t \in \mathbb{R}_+ \quad \mathbb{P}(|Z| \geq \lambda) \leq 2 \exp\left(\frac{\sigma^2 t^2}{2} - \lambda t\right)$

Cette inégalité est valable pour tout  $t \in \mathbb{R}_+$ . Or, la fonction

$$t \mapsto \frac{\sigma^2 t^2}{2} - \lambda t$$

est polynomiale de degré 2, et son coefficient dominant est strictement positif puisque  $\sigma$  est non nul par hypothèse. Elle possède donc un minimum en

$$t_0 = \frac{-(-\lambda)}{2 \frac{\sigma^2}{2}} = \frac{\lambda}{\sigma^2} \in \mathbb{R}_+$$

En appliquant en  $t_0$  l'inégalité précédemment démontrée, on trouve

$$\mathbb{P}(|Z| \geq \lambda) \leq 2 \exp\left(\frac{\sigma^2 \lambda^2}{2 \sigma^4} - \lambda \frac{\lambda}{\sigma^2}\right) = 2 \exp\left(-\frac{\lambda^2}{2\sigma^2}\right)$$

**22** Posons  $Z = \langle X | Y \rangle$ . D'après la question 19, pour tout  $t \in \mathbb{R}$ , en posant  $\sigma = 1/\sqrt{n}$ ,

$$\mathbb{E}(\exp(tZ)) \leq \exp\left(\frac{t^2}{2n}\right) = \exp\left(\frac{\sigma^2 t^2}{2}\right)$$

Ceci nous autorise à appliquer à  $Z$  le résultat de la question 21, pour cette valeur de  $\sigma$ . Cela donne

$$\forall \lambda > 0 \quad \mathbb{P}(|\langle X | Y \rangle| \geq \lambda) = \mathbb{P}(|Z| \geq \lambda) \leq 2 \exp\left(-\frac{\lambda^2}{2\sigma^2}\right) = 2 \exp\left(-\frac{\lambda^2 n}{2}\right)$$

En appliquant le résultat précédent avec  $\lambda = \varepsilon$ , on obtient

$$\boxed{\mathbb{P}(|\langle X | Y \rangle| \geq \varepsilon) \leq 2 \exp\left(-\frac{\varepsilon^2 n}{2}\right)}$$

**23** D'après la question précédente, pour tous  $i, j \in \llbracket 1; N \rrbracket$  avec  $i < j$ ,

$$\mathbb{P}(|\langle X^i | X^j \rangle| \geq \varepsilon) \leq 2 \exp\left(-\frac{\varepsilon^2 n}{2}\right)$$

Il s'ensuit, par la propriété de sous-additivité de la probabilité,

$$\begin{aligned} \mathbb{P}\left(\bigcup_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| \geq \varepsilon\}\right) &\leq \sum_{1 \leq i < j \leq N} \mathbb{P}(|\langle X^i | X^j \rangle| \geq \varepsilon) \\ &\leq \sum_{1 \leq i < j \leq N} 2 \exp\left(-\frac{\varepsilon^2 n}{2}\right) \end{aligned}$$

Comme cette dernière somme comporte  $N(N-1)/2$  termes tous indépendants des indices, on conclut que

$$\boxed{\mathbb{P}\left(\bigcup_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| \geq \varepsilon\}\right) \leq N(N-1) \exp\left(-\frac{\varepsilon^2 n}{2}\right)}$$

**24** Comme  $n \geq 4 \ln(N)/\varepsilon^2$ , on a  $-\varepsilon^2 n/2 \leq -2 \ln(N)$  et par croissance de l'exponentielle,

$$\exp\left(-\frac{\varepsilon^2 n}{2}\right) \leq \exp(-2 \ln(N)) = \frac{1}{N^2}$$

En combinant ce résultat avec celui de la question précédente, on obtient

$$\mathbb{P}\left(\bigcup_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| \geq \varepsilon\}\right) \leq \frac{N(N-1)}{N^2} = 1 - \frac{1}{N}$$

ce qui permet de conclure

$$\boxed{\mathbb{P}\left(\bigcup_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| \geq \varepsilon\}\right) < 1}$$

**25** Soit  $N$  un entier naturel inférieur ou égal à  $\exp(\varepsilon^2 n/4)$ . Alors  $n \geq 4 \ln(N)/\varepsilon^2$  et en passant au complémentaire dans le résultat précédent, on peut écrire

$$\mathbb{P}\left(\bigcap_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| < \varepsilon\}\right) = 1 - \mathbb{P}\left(\bigcup_{1 \leq i < j \leq N} \{|\langle X^i | X^j \rangle| \geq \varepsilon\}\right) > 1 - 1 = 0$$

Or, tout événement de probabilité non nulle est non vide. Par conséquent, il existe  $\omega \in \Omega$  tel que

$$\omega \in \left( \bigcap_{1 \leq i < j \leq n} |\langle X^i \mid X^j \rangle| < \varepsilon \right)$$

Fixons un tel  $\omega$  et posons  $u = (X^1(\omega), \dots, X^n(\omega))$ . C'est une famille de vecteurs unitaires de  $\mathcal{M}_{n,1}(\mathbb{R})$ . En effet, pour tout  $i \in \llbracket 1; n \rrbracket$ ,

$$\|X^i(\omega)\|^2 = \left( \frac{1}{\sqrt{n}} \right)^2 (X_1^i(\omega)^2 + \dots + X_n^i(\omega)^2) = \frac{1}{n} \sum_{j=1}^n 1 = 1$$

puisque pour tout  $j \in \llbracket 1; n \rrbracket$ ,  $X_j^i(\omega) \in \{-1, 1\}$ . En outre, au vu de ce qui précède, pour tous  $i, j \in \llbracket 1; N \rrbracket$  avec  $i < j$ ,

$$|\langle X^i(\omega) \mid X^j(\omega) \rangle| < \varepsilon$$

Notons que ce résultat reste vrai pour tous  $i, j \in \llbracket 1; N \rrbracket$  tels que  $i \neq j$  par symétrie du produit scalaire. Le paramètre de cohérence  $C(u)$  est donc majoré par  $\varepsilon$ . On a montré que

Pour tout entier naturel  $N$  inférieur ou égal à  $\exp(\varepsilon^2 n/4)$ , il existe une famille de  $N$  vecteurs unitaires de  $\mathbb{R}^n$  (qui s'identifie à  $\mathcal{M}_{n,1}(\mathbb{R})$ ) dont le paramètre de cohérence est majoré par  $\varepsilon$ .