

**Exercice 1**

Soit  $f$  un endomorphisme d'un espace vectoriel  $E$  de dimension finie  $n$ .

1. Démontrer que :  $E = \text{Im}(f) \oplus \text{Ker}(f) \Rightarrow \text{Im}(f) = \text{Im}(f^2)$ .
2. (a) Démontrer que :  $\text{Im}(f) = \text{Im}(f^2) \Leftrightarrow \text{Ker}(f) = \text{Ker}(f^2)$ .
- (b) Démontrer que :  $\text{Im}(f) = \text{Im}(f^2) \Rightarrow E = \text{Im}(f) \oplus \text{Ker}(f)$ .

**Exercice 2**

1. Démontrer que l'application

$$\begin{cases} \mathcal{M}_n(\mathbb{R}) & \rightarrow \mathbb{R} \\ M & \mapsto \text{tr}(M) \end{cases}$$

est une forme linéaire et que :

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

2. Montrer que l'application

$$\begin{cases} \mathcal{M}_n(\mathbb{R})^2 & \rightarrow \mathbb{R} \\ (A, B) & \mapsto \text{tr}(A^T B) \end{cases}$$

définit un produit scalaire sur  $\mathcal{M}_n(\mathbb{R})$ .

3. En déduire que si  $A$  est une matrice de  $\mathcal{M}_n(\mathbb{R})$  vérifiant  $A^T A = 0$  alors  $A = 0$ .

**Problème - Autour des matrices aléatoires**

*D'après Centrale PSI 2022*

On s'intéresse dans ce problème à des variables aléatoires dont les valeurs sont des matrices à coefficients dans  $\{-1, 1\}$ . Dans la partie I, on étudie un procédé de génération de telles matrices aléatoires et on s'intéresse à la probabilité d'obtenir une matrice inversible. La partie II est consacrée à une démonstration probabiliste d'un résultat de nature euclidienne.

Pour tous  $n, p \in \mathbb{N}^*$ , on note  $\mathcal{V}_{n,p}$  l'ensemble des matrices à  $n$  lignes et  $p$  colonnes à coefficients dans  $\{-1, 1\}$ . Toutes les variables aléatoires de ce problème sont définies sur un même espace probabilisé fini  $(\Omega, \mathcal{P})$ . Dans tout ce problème,  $n$  désigne un entier naturel non nul.

On rappelle que la fonction cosinus hyperbolique est définie par  $\forall t \in \mathbb{R}, \text{ch}(t) = \frac{e^t + e^{-t}}{2}$ .

**I. Matrices aléatoires à coefficients dans  $\{-1, 1\}$** 

*I.A Une loi de probabilité*

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

$$X(\Omega) = \{-1, 1\} \quad \text{et} \quad P(X = -1) = P(X = 1) = \frac{1}{2}$$

1. Si  $X$  est une variable aléatoire suivant la loi  $\mathcal{R}$ , préciser la loi de la variable aléatoire  $\frac{1}{2}(X + 1)$ .
2. Calculer l'espérance et la variance d'une variable aléatoire suivant la loi  $\mathcal{R}$ .
3. Soient  $X$  et  $Y$  deux variables aléatoires réelles indépendantes suivant chacune la loi  $\mathcal{R}$ . Déterminer la loi de leur produit  $XY$ .

*I.B Quelques résultats algébriques*

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

4. (a) Pour tout  $i \in \llbracket 1, n \rrbracket$ , exprimer  $E_i$  en fonction de  $V$  et de  $V - 2E_i$ .
- (b) En déduire que  $\mathcal{M}_{n,1}(\mathbb{R}) = \text{Vect}(\mathcal{V}_{n,1})$ .

5. Soient  $C_1, \dots, C_n \in \mathcal{M}_{n,1}(\mathbb{R})$  avec  $C_1$  non nulle, telle que la famille  $(C_1, \dots, C_n)$  est liée. Montrer qu'il existe un unique  $j \in \llbracket 1, n-1 \rrbracket$  tel que

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

6. Soient  $d \in \llbracket 1, n \rrbracket$ ,  $(U_1, \dots, U_d)$  une famille libre de  $\mathcal{M}_{n,1}(\mathbb{R})$ , et  $H = \text{Vect}(U_1, \dots, U_d)$ . Montrer qu'il existe des entiers  $i_1, \dots, i_d$  vérifiant  $1 \leq i_1 < \dots < i_d \leq n$  tels que l'application

$$h \left\{ \begin{array}{l} H \rightarrow \mathcal{M}_{d,1}(\mathbb{R}) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{pmatrix} \end{array} \right.$$

soit bijective.

On pourra considérer le rang de la matrice dont les colonnes sont  $U_1, \dots, U_d$ .

7. Soit  $\mathcal{W}$  un sous-espace vectoriel de  $\mathcal{M}_{n,1}(\mathbb{R})$  de dimension  $d$ . Démontrer que  $\text{Card}(\mathcal{W} \cap \mathcal{V}_{n,1}) \leq 2^d$ .

### I.C Un procédé de génération de matrices aléatoires

Jusqu'à la fin de cette partie, on considère des variables aléatoires mutuellement indépendantes  $m_{i,j}$  (avec  $1 \leq i, j \leq n$ ) suivant toutes la loi  $\mathcal{R}$ . La variable aléatoire matricielle  $M_n = (m_{i,j})_{1 \leq i, j \leq n}$  est alors à valeurs dans  $\mathcal{V}_{n,n}$ .

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

8. Calculer l'espérance et la variance de la variable aléatoire  $\tau_n$ .

9. Calculer l'espérance de  $\delta_n$ .

10. Démontrer que la variance de  $\delta_n$  est égale à  $n!$ .

On pourra développer  $\delta_n$  par rapport à une rangée et raisonner par récurrence.

11. Dans le cas particulier  $n = 2$ ,  $m_{11}, m_{12}, m_{21}, m_{22}$  sont quatre variable aléatoires réelles, mutuellement indépendantes, suivant toutes la loi  $\mathcal{R}$ , et  $M_2 = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ . Calculer la probabilité de l'événement  $M_2 \in GL_2(\mathbb{R})$ .

### I.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  $n \geq 2$ , un minorant de la probabilité de l'événement  $M_n \in GL_n(\mathbb{R})$ .

12. On considère  $2n$  variables aléatoires réelles  $c_1, \dots, c_n, c'_1, \dots, c'_n$  mutuellement indépendantes suivant toutes la loi  $\mathcal{R}$ .

- (a) Soit  $(\varepsilon_1, \dots, \varepsilon_n) \in \{-1, 1\}^n$ . Calculer  $P((c_1 = \varepsilon_1) \cap \dots \cap (c_n = \varepsilon_n))$ .

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

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

- (c) En déduire  $P((C, C') \text{ est liée})$ .

On note  $C_1, \dots, C_n \in \mathcal{V}_{n,1}(\mathbb{R})$  les colonnes de la matrice aléatoire  $M_n$ . Pour tout  $j \in \llbracket 1, n-1 \rrbracket$ , on note  $R_j$  l'événement «  $(C_1, \dots, C_j)$  est libre et  $C_{j+1} \in \text{Vect}(C_1, \dots, C_j)$  », et  $R_n$  l'événement «  $(C_1, \dots, C_n)$  est libre ».

13. Montrer que  $(R_1, \dots, R_n)$  forme un système complet d'événements.

14. (a) Montrer que  $P(M_n \notin GL_n(\mathbb{R})) \leq \sum_{j=1}^{n-1} P(C_{j+1} \in \text{Vect}(C_1, \dots, C_j))$ .

- (b) Justifier que, pour tout  $j \in \llbracket 1, n-1 \rrbracket$ ,

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

- (c) En déduire que, pour tout  $j \in \llbracket 1, n-1 \rrbracket$ ,  $P(C_{j+1} \in \text{Vect}(C_1, \dots, C_j)) \leq 2^{j-n}$ .

- (d) En déduire que  $P(M_n \in GL_n(\mathbb{R})) \geq \frac{1}{2^{n-1}}$ .

## II. Vecteurs aléatoires unitaires

Cette partie est indépendante des sous-parties I.B à I.D.

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

15. Démontrer que le nombre réel  $C(u) = \sup \{ |\langle u_i, u_j \rangle|, (i, j) \in I^2, i \neq j \}$  existe et appartient à l'intervalle  $[0, 1]$ .

$C(u)$  est appelé *paramètre de cohérence* de la famille  $(u_i)_{i \in I}$ .

16. Montrer que si  $C(u) = 0$ , alors l'ensemble  $\{u_i, i \in I\}$  est fini et donner un majorant de son cardinal.

On se propose de démontrer que, pour tout  $\varepsilon \in ]0, 1]$  et tout entier naturel  $N$  inférieur ou égal à  $\exp\left(\frac{\varepsilon^2 n}{4}\right)$ , il existe une famille  $u$  de  $N$  vecteurs unitaires de  $\mathcal{M}_{n,1}(\mathbb{R})$  vérifiant  $C(u) \leq \varepsilon$ . On dit alors que  $u$  est une famille de vecteurs « presque orthogonale ».

17. Démontrer que pour tout nombre réel  $t$ ,  $\text{ch}(t) \leq \exp\left(\frac{t^2}{2}\right)$ .

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

18. Démontrer que, pour tout nombre réel  $t$ ,  $E(\exp(t \langle X, Y \rangle)) = \text{ch}\left(\frac{t}{n}\right)^n$ .

19. En déduire que, pour tout nombre réel  $t$ ,  $E(\exp(t \langle X, Y \rangle)) \leq \exp\left(\frac{t^2}{2n}\right)^n$ .

Soient  $\sigma$  et  $\lambda$  deux nombres réels strictement positifs et  $Z$  une variable aléatoire réelle telle que

$$\forall t \in \mathbb{R}, \quad E(\exp(tZ)) \leq \exp\left(\frac{\sigma^2 t^2}{2}\right)$$

20. En appliquant l'inégalité de Markov à une variable aléatoire bien choisie, démontrer que

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

21. En déduire que  $P(|Z| \geq \lambda) \leq 2 \exp\left(-\frac{\lambda^2}{2\sigma^2}\right)$ .

22. Avec les notations et hypothèses de la question 20, démontrer que

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

$N$  étant un entier naturel non nul,  $(X_j^i)_{1 \leq i \leq N, 1 \leq j \leq n}$  est une famille de  $n \times N$  variables aléatoires mutuellement indépendantes de même loi  $\mathcal{R}$ . Pour tout  $i \in \llbracket 1, N \rrbracket$ , on pose  $X^i = \frac{1}{\sqrt{n}}(X_1^i, \dots, X_n^i)^T$ .

23. Déduire des questions précédentes que

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

24. On suppose que  $n \geq \frac{4 \ln(N)}{\varepsilon^2}$ . Démontrer que  $P\left(\bigcup_{1 \leq i < j \leq N} (|\langle X^i, X^j \rangle| \geq \varepsilon)\right) < 1$

25. En déduire que, pour tout entier naturel  $N$  inférieur ou égal à  $\exp\left(\frac{\varepsilon^2 n}{4}\right)$ , il existe une famille de  $N$  vecteurs unitaires de  $\mathbb{R}^n$  dont le paramètre de cohérence est majoré par  $\varepsilon$ .