Centrale 2016 - PSI 1
un corrigé

1 Généralités

A. Propriétés élémentaires

1.A.1 $\mathcal{X}_n$ est en bijection avec $\{0,1\}^{(n^2)}$. C'est donc un ensemble fini et

$$\text{card}(\mathcal{X}_n) = 2^{(n^2)}$$

1.A.2 On procède par récurrence pour montrer que pour tout entier $n \geq 2$ on a

$$\forall M \in \mathcal{Y}_n,\ |\det(M)| < n!$$

- Initialisation : soit $M \in \mathcal{Y}_2$. On a $\det(M) = m_{1,1}m_{2,2} - m_{1,2}m_{2,1} \in [-1,1]$ (car $m_{1,1}m_{2,2}, m_{1,2}m_{2,1} \in [0,1]$). On a donc $|\det(M)| \leq 1 < 2$. Le résultat est donc vrai au rang 1.
- Hérédité : supposons le résultat vrai à un rang $n \geq 1$. Soit $M \in \mathcal{Y}_{n+1}$. Un développement par rapport à la dernière colonne donne

$$\det(M) = \sum_{i=1}^{n+1} (-1)^{n+1+i} m_{i,n+1} \det(M_{n+1,i}) \leq \sum_{i=1}^{n+1} m_{i,n+1} |\det(M_{n+1,i})|$$

où $M_{n+1,i}$ est obtenue à partir de M en supprimant ligne i et colonne $n+1$ et est donc dans $\mathcal{Y}_n$. Par hypothèse de récurrence, on a donc

$$|\det(M)| \leq n! \sum_{i=1}^{n+1} m_{i,n+1} \leq (n+1)!$$

La dernière inégalité n'est une égalité que si la dernière colonne vaut $(1,\dots,1)$ mais dans ce cas $|\det(M)| = 0 < (n+1)!$. On a donc le résultat au rang $n+1$.

On en déduit le résultat demandé qui est moins fort que celui prouvé.

1.A.3 On munit $\mathcal{M}_n(\mathbb{R})$ de la norme $\|M\| = \sup\{|m_{i,j}|/\ 1 \leq i,j \leq n\}$ (cela ne change rien puisque l'on travaille en dimension finie où le choix de la norme est indifférent). On a alors

$$\forall M \in \mathcal{Y}_n,\ \|M\| \leq 1$$

et $\mathcal{Y}_n$ est bornée.
Soit (M_p) une suite convergente d'éléments de $\mathcal{Y}_n$. En notant M la limite, $M_{i,j}$ est la limite le la suite de terme général $(M_p)_{i,j} \in [0,1]$ et on a donc $M_{i,j} \in [0,1]$. Ceci montre que $M \in \mathcal{Y}_n$ et que cet ensemble est fermé. Finalement,

$$\mathcal{Y}_n \text{ est un compact de } \mathcal{M}_n(\mathbb{R})$$

Soient $A, B \in \mathcal{Y}_n$ et $\lambda \in [0,1]$. Posons $M = \lambda A + (1-\lambda)B$. On a

$$\forall i,j \in [|1,n|],\ M_{i,j} = \lambda A_{i,j} + (1-\lambda)B_{i,j} \in [0,1]$$

car $[0,1]$ est convexe. Ainsi $M \in \mathcal{Y}_n$ et

$$\mathcal{Y}_n \text{ est un convexe de } \mathcal{M}_n(\mathbb{R})$$

1.A.4 Soient $M \in \mathcal{Y}_n$ et λ une valeur propre associée. On a $MX = \lambda X$. Il existe un entier i tel que $|x_i| = \max\{|x_k|/\ 0 \le k \le n\}$. On a

$$\lambda x_i = (MX)_i = \sum_{k=1}^{n} m_{i,k} x_k$$

et donc

$$|\lambda|.|x_i| \le \sum_{k=1}^{n} m_{i,k}|x_k| \le |x_i| \sum_{k=1}^{n} m_{i,k} \le n|x_i|$$

Comme $|x_i| > 0$ car $X \neq 0$, on en déduit que $|\lambda| \le n$. Ainsi

$$\forall M \in \mathcal{Y}_n,\ \forall \lambda \in \mathrm{Sp}(M),\ |\lambda| \le n$$

La matrice J_n dont tous les coefficients valent 1 est dans $\mathcal{Y}_n$ et n est valeur propre de J_n (vecteur propre associé $(1, \dots, 1)$).

B. Etude de $\mathcal{X}'_n = \mathcal{X}_n \cap GL_n(\mathbb{R})$

1.B.1 Soit $M \in \mathcal{X}_2$. Si M a 0 ou 1 coefficient non nul, elle est non inversible (de rang 0 ou 1). Si elle en a quatre, elle n'est pas inversible non plus (deux colonnes égales). Il reste à traiter le cas où il y a 2 ou 3 coefficients non nuls. On trouve que

$$\mathcal{X}'_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

Les polynômes caractéristiques de ces matrices sont (dans l'ordre)

$$(X-1)^2,\ X^2-1,\ (X-1)^2,\ X^2-X-1,\ X^2-X-1,\ (X-1)^2$$

Quand ce polynôme a deux racines distinctes, la matrice est diagonalisable (et possède deux sous-espaces propres de dimension 1). Quand il a une racine double, la matrice n'est diagonalisable que si elle est scalaire. Quand il n'y a pas de racine réelle, on a une matrice non diagonalisable. Les éléments diagonalisables de $\mathcal{X}'_2$ sont donc

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

1.B.2 On a

$$E_{1,2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ E_{2,1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$E_{2,2} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ E_{1,1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Les éléments de la base canonique s'expriment donc comme combinaisons d'éléments de $\mathcal{X}'_2$ et $\mathcal{X}'_2$ engendre $\mathcal{M}_2(\mathbb{R})$.

De même, on veut montrer que pour $n \ge 3$, toute matrice $E_{i,j}$ de la base canonique de $\mathcal{M}_n(\mathbb{R})$ peut s'écrire comme combinaison linéaires d'éléments de $\mathcal{X}'_n$. Soient donc $i, j \in [|1, n|]$.

- Si $i \neq j$, $E_{i,j} = (I_n + E_{i,j}) - I_n$ est une décomposition convenable.
- Si $i \neq j$ alors la matrice M obtenue à partir de I_n en permutant les lignes i et j est dans $\mathcal{X}'_n$ et $I_n - M = E_{i,i} + E_{j,j} - E_{i,j} - E_{j,i}$. $E_{i,i} + E_{j,j} = I_n - M + E_{i,j} + E_{j,i}$ est donc combinaison d'éléments de $\mathcal{X}'_n$ avec le premier cas. On a alors

  $$E_{i,i} - E_{j,j} = (E_{i,i} + E_{k,k}) - (E_{j,j} + E_{k,k})$$

  qui est aussi combinaison d'éléments de $\mathcal{X}'_n$ (on peut choisir $k \notin \{i, j\}$ puisque $n \ge 3$).
- Ainsi, pour $i \in [|1, n|]$, $E_{i,i} = \frac{1}{2}((E_{i,i} + E_{j,j}) + (E_{i,i} - E_{j,j}))$ est combinaison d'éléments de $\mathcal{X}'_n$ (on peut choisir $j \neq i$).

2 Deux problèmes d'optimisation

A. Etude de la distance à $\mathcal{Y}_n$

2.A.1 On remarque que

$$(M|N) = \sum_{i=1}^{n} (M^T N)_{i,i} = \sum_{i=1}^{n} \sum_{j=1}^{n} M_{j,i} N_{j,i}$$

Cette application correspond ainsi au produit scalaire canonique en identifiant $\mathcal{M}_n(\mathbb{R})$ et $\mathbb{R}^{(n^2)}$. On trouve d'ailleurs, avec cette formule, facilement les propriétés du produit scalaire (symétrique, linéaire par rapport à la seconde variable, défini positif).

2.A.2 L'application $M \mapsto \|A - M\|$ est continue. Elle est donc bornée et atteint ses bornes sur le compact $\mathcal{Y}_n$. En notant $M \in \mathcal{Y}_n$ un élément où elle atteint son minimum, on a alors

$$\forall N \in \mathcal{Y}_n, \ \|A - M\| \leq \|A - N\|$$

2.A.3 La matrice M doit être dans $\mathcal{Y}_n$, c'est à dire avoir des coefficients dans $[0,1]$ et minimiser la quantité

$$\sum_{1 \leq i,j \leq n} (a_{i,j} - m_{i,j})^2$$

Elle minimise donc chacune des quantités (indépendantes les unes des autres) $(a_{i,j} - m_{i,j})^2$ et minimise donc $|a_{i,j} - m_{i,j}|$. On a donc

$$m_{i,j} = \begin{cases} a_{i,j} & \text{si } \ a_{i,j} \in [0,1] \\ 1 & \text{si } \ a_{i,j} > 1 \\ 0 & \text{si } \ a_{i,j} < 0 \end{cases}$$

Il y a unicité de M car pour tout y, $x \mapsto |y - x|$ atteint son minimum sur $[0,1]$ en un unique point.

B. Maximisation du déterminant sur $\mathcal{X}_n$ et $\mathcal{Y}_n$

2.B.1 Le déterminant est une application multilinéaire en dimension finie et donc continue. Elle est donc bornée et atteint ses bornes sur tout compact. C'est en particulier le cas sur $\mathcal{Y}_n$ et sur $\mathcal{X}_n$ (toute partie finie est évidemment compacte puisque fermée et bornée). On pose

$$x_n = \max_{M \in \mathcal{X}_n} \det(M) \ \text{ et } \ y_n = \max_{M \in \mathcal{Y}_n} \det(M)$$

2.B.2 Soit $k \geq 2$. Soit $M \in \mathcal{Y}_k$; notons $M' = \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$ (définition par blocs). On a évidemment $M' \in \mathcal{Y}_{k+1}$ et $\det(M') = \det(M)$ (déterminant bloc diagonal). Ainsi

$$\det(M) = \det(M') \leq y_{k+1}$$

En passant au maximum, on en déduit que

$$y_k \leq y_{k+1}$$

2.B.3 La matrice M a tous ses coefficients égaux sauf ceux sur la diagonale qui valent 1. On effectue l'opération élémentaire $C_1 \leftarrow C_1 + \cdots + C_n$ ce qui permet de factoriser le déterminant par $n-1$. On soustrait alors la première colonne à toutes les autres. Ces opérations laissent le déterminant invariant et donnent un déterminant triangulaire de coefficients diagonaux $1, -1, \dots, -1$. On a aindi

$$\det(M) = (n-1)(-1)^{n-1}$$

En particulier, $y_{2n+1} \geq 2n$ et $y_{2n+1} \to +\infty$. Par croissance de la suite (y_k), on en déduit que

$$\lim_{n\to+\infty} y_n = +\infty$$

2.B.4 Un développement par rapport à la colonne j donne

$$\det(N) = \sum_{k=1}^{n} (-1)^{k+j} n_{k,j} \det(N_{k,j})$$

où $N_{k,j} \in \mathcal{M}_{n-1}(\mathbb{R})$ est obtenue à partir de N en enlevant colonne j et ligne k. Si $(-1)^{i+j}\det(N_{i,j}) \geq 0$, on pose $n'_{i,j} = 1$ et sinon on pose $n'_{i,j} = 0$. Par ailleurs, on pose $n'_{u,v} = n_{u,v}$ si $(u, v) \neq (i, j)$.
N et N' ayant même colonne j, $\det(N_{k,j}) = \det(N'_{k,j})$ pour tout k.
Par choix de $n'_{i,j}$, on a $(-1)^{i+j}\det(N_{i,j})n_{i,j} \leq (-1)^{i+j}\det(N'_{i,j})n'_{i,j}$.
Enfin, $(-1)^{k+j}\det(N_{k,j})n_{k,j} = (-1)^{k+j}\det(N'_{k,j})n'_{k,j}$ pour $k \neq i$. Ainsi,

$$\det(N) = \sum_{k=1}^{n} (-1)^{k+j} n_{k,j} \det(N_{k,j}) \leq \sum_{k=1}^{n} (-1)^{k+j} n'_{k,j} \det(N'_{k,j}) = \det(N')$$

et bien sûr $N' \in \mathcal{Y}_n$.
En répétant ce processus pour tous les couples (i, j), on trouve une matrice $M \in \mathcal{X}_n$ telle que $\det(N) \leq \det(M)$. On a ainsi

$$\forall N \in \mathcal{Y}_n,\ \det(N) \leq x_n$$

En passant au maximum, on trouve que $y_n \leq x_n$. Comme $\mathcal{X}_n \subset \mathcal{Y}_n$, l'inégalité inverse est évidente et finalement

$$x_n = y_n$$

3 Matrices de permutations

A. Description de $\mathcal{P}_n$

3.A.1 On dit que u est une isométrie vectorielle de $\mathbb{R}^n$ si

$$u \in \mathcal{L}(\mathbb{R}^n) \ \text{ et } \ \forall x, y \in \mathbb{R}^n,\ (u(x)|u(y)) = (x|y) \tag{1}$$

Montrons que ceci équivaut à

$$u \in \mathcal{L}(\mathbb{R}^n) \ \text{ et } \ Mat_{(e_1,\dots,e_n)}(u) \in O_n(\mathbb{R}) \tag{2}$$

- Supposons (1) vérifiée. En particulier, $(u(e_i)|u(e_j)) = (e_i|e_j) = \delta_{i,j}$ et $(u(e_1), \dots, u(e_n))$ est une b.o.n. de $\mathbb{R}^n$. $Mat_{(e_1,\dots,e_n)}(u)$ s'interprétant aussi comme matrice de passage entre $(e_1, \dots, e_n)$ et $(u(e_1), \dots, u(e_n))$, c'est une matrice de passage entre b.o.n. et donc unematrice orthogonale.
- Supposons (2) vérifiée. Les colonnes de $Mat_{(e_1,\dots,e_n)}(u)$ forment alors une b.o.n. de $\mathbb{R}^n$ et cette matrice s'interprère comme matrice de passage entre b.o.n. On en déduit que $(u(e_1), \dots, u(e_n))$ est une b.o.n. de $\mathbb{R}^n$. Soient alors $x, y \in \mathbb{R}^n$. On a

$$(u(x)|u(y)) = \left(\sum_{i=1}^{n} x_i u(e_i) | \sum_{i=1}^{n} y_i u(e_i) \right) = \sum_{i=1}^{n} x_i y_i = (x|y)$$

3.A.2 Si $M \in O_n(\mathbb{R})$ alors $M^T M = I_n$. Le déterminant étant un morphisme multiplicatif invariant par transposition, on en déduit que $\det(M)^2 = 1$ et on a donc

$$\forall M \in O_n(\mathbb{R}),\ \det(M) \in \{1, -1\}$$

La réciproque est fausse comme le montre la matrice $\mathrm{diag}(2, 1/2, 1, \dots, 1)$ qui est de déterminant 1 mais non orthogonale (première colonne non normée).

3.A.3 On doit prouver une double inclusion.

- Soit $M \in \mathcal{P}_n$. Chaque colonne de P est un des e_i (car il y a un unique 1 et des 0) et pour tout i, il existe $s(i)$ tel que la colonne i de P soit $e_{s(i)}$. De plus, deux colonnes sont différentes (car il y a un unique 1 et des 0 sur chaque ligne). Les $s(i)$ sont donc deux à deux distincts et s est une permutation de $[|1, n|]$. Les colonnes de P forment donc une b.o.n. de $\mathbb{R}^n$ et $P \in O_n(\mathbb{R})$. On a aussi $P \in \mathcal{X}_n$.
- Supposons réciproquement que $M \in O_n(\mathbb{R}) \cap \mathcal{X}_n$. Chaque colonne de P est normée et composée de 0 et de 1. Il faut donc qu'il y a ait un unique 1 sur chaque colonne (et des zéros ailleurs). De plus, $M^T \in O_n(\mathbb{R})$ et on a la même propriété sur les lignes. Ainsi, $M \in \mathcal{P}_n$.

On a en fait montré que $\mathcal{P}_n$ est composé des matrices de permutation. Son cardinal est égal à $n!$.

B. Quelques propriétés des éléments de $\mathcal{P}_n$

3.B.1 La j colonne de P_σ est $e_{\sigma(j)}$. u_σ est donc caractérisé par

$$\forall j \in [|1, n|],\ u_\sigma(e_j) = e_{\sigma(j)}$$

On en déduit, pour

•

sigma,$\sigma' \in S_n$, que

$$\forall j,\ u_\sigma \circ u_{\sigma'}(e_j) = u_\sigma(e_{\sigma'(j)}) = e_{\sigma\circ\sigma'(j)}$$

Un endomorphisme étant caractérisé par son action sur une base, on trouve que $u_\sigma \circ u_{\sigma'} = u_{\sigma\circ\sigma'}$ ce qui donne matriciellement

$$P_\sigma P_{\sigma'} = P_{\sigma\circ\sigma'}$$

$k \in \mathbb{Z} \mapsto \sigma^k \in S_n$ ne peut être injective puisque son ensemble de départ est infini alors que son ensemble d'arrivée est fini. Il existe donc $i < j$ tel que $\sigma^i = \sigma^j$ c'est à dire (en composant $i$fois par l'inverse de σ) que $\mathrm{Id}_{\{1,\dots,n\}} = \sigma^{j-i}$. Comme $j - i > 0$, on a montré que

$$\exists\, N \geq 1/\ \sigma^N = \mathrm{Id}_{\{1,\dots,n\}}$$

3.B.2 Soit $M \in \mathcal{P}_n$. On a vu en **3.1.3** qu'il existe $s \in S_n$ telle que $M = P_s$. Comme il existe $N \geq 1$ tel que $s^N = \mathrm{Id}$, on trouve

$$M^N = P_{s^N} = P_{\mathrm{Id}} = I_n$$

et $X^N - 1$ annule M. Ce polynôme étant scindé à racines simples dans $\mathbb{C}$ (les racines N-ièmes de l'unité), M est diagonalisable (dans $\mathbb{C}$).

3.B.3 Il y a autant d'éléments dans $\mathcal{P}_n$ que dans S_n, c'est à dire $n!$. On a

$$\mathcal{P}_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Les vecteurs propres communs à ces deux matrices sont ceux de de la seconde (tout vecteur non nul est propre pour I_2) et ce sont les multiples non nuls de $(1,1)$ et $(1,-1)$.
Passons au cas $n=3$. On a cette fois

$$\mathcal{P}_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}$$

Les sous-espaces propres de la seconde matrice sont $A = \mathrm{Vect}((1,1,1),(0,0,1))$ et $B = \mathrm{Vect}((1,-1,0))$.
Les sous-espaces propres de la troisième matrice sont $C = \mathrm{Vect}((1,1,1),(0,1,0))$ et $D = \mathrm{Vect}((1,0,-1))$.
Un vecteur propre commun à toutes les matrices est donc dans $A\cap C$ ou $A\cap D$ ou $B\cap C$ ou $B\cap D$. Deux de ces espaces sont égaux à $\{0\}$ et deux autres égaux à $\mathrm{Vect}(1,1,1)$. Un vecteur propre commun à tous les éléments de $\mathcal{P}_3$ est donc un multiple non nul de $(1,1,1)$.
Réciproquement, $(1,1,1)$ est propre pour chaque élément de $\mathcal{P}_3$ et il en est donc de même pour tous ses multiples non nuls.

3.B.4 (a) Soit $\sigma \in S_n$. On a immédiatement

$$u_\sigma(\{0\}) = \{0\} \text{ et } u_\sigma(\mathbb{R}^n) \subset \mathbb{R}^n$$

De plus $u_\sigma(e_1+\cdots+e_n) = e_{\sigma(1)}+\cdots+e_{\sigma(n)} = e_1+\cdots+e_n$ et donc

$$u_\sigma(\mathrm{Vect}(e_1+\cdots+e_n)) \subset \mathrm{Vect}(e_1+\cdots+e_n)$$

Soit $x\in H = D^\perp$. Pour tout $y\in D$, on a $u_\sigma(y)=y$ (on vient de le voir) et donc (comme u_σ est une isométrie vectorielle puisqu'elle transforme une b.o.n. en b.o.n.)

$$(u_\sigma(x)|y) = (u_\sigma(x)|u_\sigma(y)) = (x|y) = 0$$

Ceci montre que $u_\sigma(x) \in D^\perp = H$ et on a donc

$$u_\sigma(H) \subset H$$

(b) Comme V est un sous-espace de $\mathbb{R}^n$ non contenu dans D, il existe des scalaires $x_1,\dots,x_n$ non tous égaux tels que $x = \sum_{i=1}^n x_i e_i \in V$.
Les x_i n'étant pas tous égaux, il existe $i<j$ tels que $x_i \neq x_j$. Soit s l'application qui échange i et j et laisse les autres éléments invariants. Comme $s\in S_n$, on a $u_s(x)\in V$ et donc $x-u_s(x)\in V$. Ceci donne $(x_i-x_j)(e_i-e_j)\in V$ et comme $x_i\neq x_j$, $e_i-e_j\in V$.
Soit alors $k\notin\{i,j\}$. Utilisons l'application σ qui permute i et k et laisse les autre éléments invariants (et donc en particulier j). On a $u_\sigma(e_i-e_j) = e_k-e_j\in V$. On a donc montré que

$$\exists\, j\in [|1,n|]/\ \forall k\neq j,\ e_k-e_j\in V$$

(c) La famille $(e_k-e_j)_{k\neq j}$ est libre, et composée de $n-1$ éléments tous dans H (orthogonaux à $e_1+\cdots+e_n$). Comme $\dim(H)=n-1$, cette famille est une base de H. On a donc $H\subset V$. Or, H est un hyperplan et les seuls sous-espaces qui contiennent H sont donc H et $\mathbb{R}^n$.
On vient de voir qu'un sous-espace qui est laissé stable par tous les u_σ est soit inclus dans D et donc égal à $\{0\}$ ou D, soit égal à H ou $\mathbb{R}^n$. C'est la réciproque voulue.

C. Une caractérisation des éléments de $\mathcal{P}_n$

Avec l'hypothèse faite, les matrices M^k ne peuvent prendre qu'un nombre fini de valeurs. Or $\mathbb{N}$ est infini. Comme en **3.B.1**, on va donc avoir deux puissances égales et trouver $N \geq 1$ tel que $M^N = 1$. On a alors $M{-}1 = M^{N-1}$ qui est à coefficients dans $\mathbb{N}$ (comme toutes les M^k pour $k \in \mathbb{N}$ et par récurrence).
Notons $M^{-1} = (n_{i,j})$ et $M = (m_{i,j})$. Comme $MM^{-1} = I_n$, on a

$$\forall i, j, \ \sum_{k=1}^{n} m_{i,k} n_{k,j} = \delta_{i,j}$$

Les quantités $m_{i,k}n_{k,j}$ étant entières naturelles, la somme ne peut valoir 0 que si toutes les quantités sont nulles et ne peut valoir 1 que si elle sont toutes nulles sauf une qui vaut 1.
Pour chaque i, on trouve donc $s(i)$ tel que $m_{i,s(i)} = n_{s(i),i} = 1$. On a alors, en utilisant $(MN)_{j,s(i)} = 0$ pour $j \neq s(i)$:

$$\forall i, \ \forall j \neq s(i), \ \forall k \in [|1, n|], \ m_{j,k} n_{k,s(i)} = 0$$

et donc, en particulier $k = i$, $m_{j,i} = 0$. Sur la colonne i, tous les termes sont nuls sauf celui en position $s(i)$ qui vaut 1. Comme M est inversible, les $s(i)$ sont ainsi seux à deux distincts (sinon deux colonnes sont égales) et $s \in S_n$ et $M = P_s$.
Réciproquement, les P_σ sont à coefficients entiers naturels et les coefficients de toutes les puissances de P_σ valent 0 ou 1 et sont donc dans un ensemble fini.

4 Matrices aléatoires de $\mathcal{X}_n$

A. Génération par une colonne aléatoire

4.A.1 La probabilité que les X_i soient égales est

$$\mathbb{P}((X_1 = 0 \cap \dots \cap X_n = 0) \cup (X_1 = 1 \cap \dots \cap X_n = 1))$$

Par incompatibilité des événements de la réunion et indépendance des X_i, cette probabilité vaut

$$\prod_{i=1}^{n} \mathbb{P}(X_i = 0) + \prod_{i=1}^{n} \mathbb{P}(X_i = 1) = p^n + (1-p)^n$$

4.A.2 Le cours indique que $X_1 + \dots + X_n$ suit une loi binomiale de paramètres n et p, c'est à dire que

$$\forall k \in [|0, n|], \ \mathbb{P}(X_1 + \dots + X_n = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Justifions ce résultat. Les X_i étant à valeurs dans $\{0, 1\}$, $X_1 + \dots + X_n$ est à valeurs dans $[|0, n|]$. De plus

$$(X_1 + \dots + X_n = k) = \bigcup_{j_1+\dots+j_n=k} \mathbb{P}(X_1 = j_1 \cap \dots \cap X_n = j_n)$$

Comme en question précédente (incompatibilité puis indépendance)

$$(X_1 + \dots + X_n = k) = \sum_{j_1+\dots+j_n=k} \mathbb{P}(X_1 = j_1) \dots \mathbb{P}(X_n = j_n) = \sum_{j_1+\dots+j_n=k} p^k (1-p)^{n-k}$$

puisque k des valeurs j_i valent 1 et $n-k$ valent 0. Il y a autant de termes dans la somme que de façon de répartir les 1, c'est à dire $\binom{n}{k}$. Ceci donne la formule annoncée.

4.A.3 $X_{i,j}$ est une variable de Bernoulli (prend la valeur 0 ou 1) de paramètre $\mathbb{P}(X_iX_j) = 1$. Deux cas sont possibles

$$\forall i \neq j,\ \mathbb{P}(X_iX_j = 1) = \mathbb{P}(X_1 = 1 \cap X_j = 1) = \mathbb{P}(X_i = 1)\mathbb{P}(X_j = 1) = p^2$$

$$\forall i,\ \mathbb{P}(X_iX_i = 1) = \mathbb{P}(X_i = 1) = p$$

4.A.4 (a) On a

$$\forall \omega \in \Omega,\ M(\omega)_{i,j} = X_i(\omega)X_j(\omega) \in \{0,1\}$$

Ainsi, M est à valeurs dans $\mathcal{X}_x$.

(b) On a de façon immédiate

$$\forall A \in \mathcal{X}_n,\ \mathrm{Tr}(A) = \sum_{i=1}^{n} a_{i,i} \in \{0,\dots,n\}$$

puisque l'on somme des 0 ou 1.
$M(\omega)$ étant un produit de matrice de rang 1, son rang est inférieur à 1 (toutes ses colonnes sont des multiples de $U(\omega)$). Distinguons deux cas.

- Si $U(\omega) = 0$ alors $M(\omega) = 0$ est diagonale (et donc diagonalisable).
- Sinon, il existe i tel que $X_i(\omega) = 1$ et $M(\Omega)_{i,i} = 1$. $M(\omega)$ est ainsi de rang 1 (non nulle et de rang ≤ 1). 0 est valeur propre et le sous-espace propre associé est de dimension $n-1$. On vérifie que $U(\omega)$ est vecteur propre associé à $\mathrm{Tr}(M(\omega)) = \sum_{i=1}^{n} X_i(\omega)^2 > 0$. On a donc un second sous-espace propre de dimension au moins 1. Les sous-espaces propres étant en somme directe, on a finalement deux sous-espaces propres : celui associé à 0 de dimension $n-1$ et celui associé à $\mathrm{Tr}(M(\omega)) > 0$ de dimension 1. $M(\omega)$ est donc diagonalisable et semblable à $\mathrm{diag}(0,\dots,0,\mathrm{Tr}(M(\omega)))$.

(c) On a

$$M(\omega)^2 = (U(\omega)U(\omega)^T)(U(\omega)U(\omega)^T) = U(\omega)(U(\omega)^TU(\omega))U(\omega)^T$$

Le produit intermédiaire est un scalaire égal à $\sum_{i=1}^{n} X_i(\omega)^2$ et donc

$$M(\omega)^2 = \left(\sum_{i=1}^{n} X_i(\omega)^2\right) M(\omega)$$

- Si $M(\omega)$ est une matrice de projection orthogonale, c'est une matrice de projecteur et donc égale à son carré. Ainsi, $\sum_{i=1}^{n} X_i(\omega)^2 \in \{0,1\}$ (1 si $M(\omega) \neq 0$ et 0 si $M(\omega) = 0$ auquel cas les $X_i(\omega)$ sont tous nuls). Dans le premier cas, les $X_i(\omega)$ valent tous 0 sauf l'un qui vaut 1 et donc $S(\omega) = 1$. Dans le second il sont tous nuls et $S(\omega) = 0$.
- Réciproquement, si $S(\omega) = 0$ alors les $X_i(\omega)$ sont tous nuls et donc $M(\omega) = 0$ qui est la matrice de projection orthogonale sur $\{0\}$.
  Si $S(\omega) = 1$ alors les $X_i(\omega)$ valent tous 0 sauf l'un qui vaut 1 et alors $\sum_{i=1}^{n} X_i(\omega)^2 = 1$ ce qui indique que $M(\omega)$ est une matrice de projection. L'image de $M(\omega)$ est égale à $\mathrm{Vect}(U(\omega))$ (vu plus haut) qui est de dimension 1 (car $U(\omega) \neq 0$). Si $(V|U(\omega)) = 0$ alors $U(\omega)^TV = 0$ et $M(\omega)V = 0$. Le noyau de $M(\omega)$ contient donc $\mathrm{Vect}(U(\omega))^\perp$ et il y a égalité par dimension (théorème du rang). $M(\omega)$ est la matrice d'une projection orthogonale.

4.A.5 On a $\mathrm{Tr}(M(\omega)) = \sum_{i=1}^{n} X_i(\omega)^2 = S(\omega)$ (car $X_i = X_i^2$). $\mathrm{Tr}(M)$ suit donc une loi binomiale de paramètres n et p et

$$\mathbb{E}(\mathrm{Tr}(M)) = np,\ \mathbb{V}(\mathrm{Tr}(M)) = np(1-p)$$

Le rang de $M(\omega)$ valant 0 ou 1, $\text{rg}(M)$ est une variable de Bernoulli de paramètre

$$1-\mathbb{P}(\text{rg}(M)=0)=1-\mathbb{P}\left(\bigcap_{i=1}^{n} X_i(\omega)=0\right)=1-(1-p)^n$$

et on a donc

$$\mathbb{E}(\text{rg}(M))=1-(1-p)^n,\ \mathbb{V}(\text{rg}(M))=(1-(1-p)^n)(1-p)^n$$

4.A.6 On a vu plus haut que $M^2=SM$. Une récurrence immédiate donne

$$\forall k\geq 1,\ M^k=S^{k-1}M$$

et on a bien sûr $M^0=I_n$.
La suite $(M(\omega)^k)$ convergera ssi $M(\omega)=0$ ou $S(\omega)\in]-1,1]$, c'est à dire en fait ssi $M(\omega)=0$ ou $S(\omega)\in\{0,1\}$ ce qui équivaut à $S(\omega)\in\{0,1\}$. La probabilité de convergence est donc

$$\begin{aligned}\mathbb{P}((\text{Tr}(M)=0)\ \cup\ (\text{Tr}(M)=1)) &= \mathbb{P}(\text{Tr}(M)=0)+\mathbb{P}(\text{Tr}(M)=1)\\ &= (1-p)^n+np(1-p)^{n-1}\\ &= (1-p)^{n-1}(1-p+np)\end{aligned}$$

S'il y a convergence alors la limite est $M(\omega)$ si $S(\omega)=1$ et 0 si $S(\omega)=0$. Dans tous les cas, la limite est $M(\omega)$ (nulle dans le second cas) et comme $S(\omega)\in\{0,1\}$, c'est une matrice de projection orthogonale.

4.A.7 On a vu plus haut que $M(\omega)$ possédait deux valeurs propres distinctes si et seulement si $U(\omega)\neq 0$, c'est à dire ssi $S(\omega)\neq 0$. La probabilité que M possède deux valeurs propres distinctes est donc

$$\mathbb{P}(S\neq 0)=1-\mathbb{P}(S=0)=1-(1-p)^n$$

B. Génération par remplissage aléatoire

4.B.1 (a)
```
def Somme(M):
    n=len(M)
    s=0
    for i in range(n):
        for j in range(n):
            s=s+M[i,j]
    return(s)
```
(b)
```
def Bernoulli(p):
    if random()<=p:
        return(1)
    else:
        return(0)
```
(c)
```
def Modifie(M,p):
    n=len(M)
    for i in range(n):
        for j in range(n):
            if M[i,j]==0:
                M[i,j]=Bernoulli(p)
```
(d) On commence par écrire une fonction `EstRemplie` qui prend en argument une matrice carrée et renvoie `True` si et seulement si ses coefficients sont tous non nuls. On se permet une interruption prématurée de boucle `for` par utilisation d'un `return` dans la boucle pour plus de lisibilité (une boucle conditionnelle est en fait plus naturelle).

```
def EstRemplie(M):
    n=len(M)
    for i in range(n):
        for j in range(n):
            if M[i,j]==0:
                return(False)
    return(True)
```

On gère alors un compteur et on itère en l'incrémentant tant que les modifications n'amènent pas la matrice avec que des 1.

```
def simulation(n,p):
    M=zeros((n,n))
    k=0
    while not(EstRemplie(M)):
        Modifie(M,p)
        k=k+1
    return(k)
```

4.B.2 N_1 est la somme des coefficients de M_1. C'est donc une somme de $m = n^2$ variables qui suivent des lois de Bernoulli de même paramètre p et qui sont indépendantes. Ainsi

$$N_1 \hookrightarrow \mathcal{B}(m, p)$$

Si $(N_1 = i)$ avec $i \in [|0, m|]$, on effectue $m - i$ nouvelles expériences de Bernoulli indépendantes de même paramètre p et pour $\mathbb{P}_{(N_1=i)}$, N_2 suit une loi $\mathcal{B}(m - i, p)$.
La loi de N_2 conditionnée par $(N_1 = i)$ dépend donc de i et les variables N_1 et N_2 ne sont pas indépendantes.

4.B.3 i et j étant fixés, on effectue une suite d'expériences de Bernoulli indépendantes et de même paramètre p et $T_{i,j}$ est le rang du premier succès. On sait alors que

$$T_{i,j} \hookrightarrow \mathcal{G}(p)$$

c'est à dire que $T_{i,j}$ sui une loi géométrique de paramètre p.

4.B.4 On a ainsi

$$\mathbb{P}(T_{i,j} \geq k) = \sum_{l=k}^{\infty} \mathbb{P}(T_{i,j} = l) = \sum_{l=k}^{\infty} p(1-p)^{l-1} = (1-p)^{k-1}$$

On peut obtenir le résultat en constatant que $(T_{i,j} \geq k)$ correspond à $k - 1$ échecs consécutifs.

4.B.5 S_r est le nombre de coefficients valant 1 après r étapes. $(S_r = l)$ signifie que $(T_{i,j} < r + 1)$ pour exactement l couples (i, j) et $(T_{i,j} \geq r + 1)$ pour les $m - l$ autres. Il y a $\binom{m}{l}$ façons de choisir l couples. Par indépendance des $T_{i,j}$ (et incompatibilité des situations pour deux choix différents des couples) et commes ces $T_{i,j}$ suivent tous la même loi (celle de $T_{1,1}$) on a donc

$$\mathbb{P}(S_r = l) = \binom{m}{l} \mathbb{P}(T_{1,1} < r+1)^l \mathbb{P}(T_{1,1} \geq r+1)^{m-l} = \binom{m}{l} (1 - (1-p)^r)^l (1-p)^{r(m-l)}$$

4.B.6 (a) On effectue un grand nombre de simulations et on calcule la moyenne des résultats obtenus. Avec 1000 simulation, cela donne la fonction suivante.

```
def esperance(n,p):
    s=0
    for i in range(1000):
        s=s+simulation(n,p)
    return(s/1000)
```

(b) On a

$$\mathbb{E}(N) = \sum_{k=1}^{+\infty} k\mathbb{P}(N = k) = \sum_{k=1}^{+\infty} \mathbb{P}(N \geq k)$$

L'événement $(N \geq k)$ signifie qu'au bout de $k-1$ étapes, tout n'était pas rempli et équivaut à $(S_{k-1} < m)$. Sa probabilité est $1 - \mathbb{P}(S_k = m)$ et avec la question précédente,

$$\mathbb{E}(N) = \sum_{k=1}^{\infty}(1 - (1 - q^k)^m)$$