À rendre pour le jeudi 11 janvier

EXERCICE COMMUN À TOUS

Dans cet exercice "Algorithme de décomposition primaire d'un entier" , on se propose d'écrire un algorithme pour décomposer un entier en produit de nombres premiers. Les algorithmes demandés doivent être écrits en langage **Python**. On sera très attentif à la rédaction et notamment à l'indentation du code.

On définit la valuation p-adique [de n] pour p nombre premier et n entier naturel non nul.
Si p divise n, on note $v_p(n)$ le plus grand entier k tel que p^k divise n.
Si p ne divise pas n, on pose $v_p(n) = 0$.
L'entier $v_p(n)$ s'appelle la valuation p-adique de n.

1. Écrire une fonction booléenne `estPremier(n)` qui prend en argument un entier naturel non nul n et qui renvoie le booléen `True` si n est premier et le booléen `False` sinon. On pourra utiliser le critère suivant : un entier $n \geq 2$ qui n'est divisible par aucun entier $d \geq 2$ tel que $d^2 \leq n$, est premier.

2. En déduire une fonction `liste_premiers(n)` qui prend en argument un entier naturel non nul n et renvoie la liste des nombres premiers inférieurs ou égaux à n.

3. Pour calculer la valuation 2-adique de 40, on peut utiliser la méthode suivante :

- 40 est divisible par 2 et le quotient vaut 20.
- 20 est divisible par 2 et le quotient vaut 10.
- 10 est divisible par 2 et le quotient vaut 5.
- 5 n'est pas divisible par 2.

La valuation 2-adique de 40 vaut donc 3.

Écrire une fonction `valuation_p_adique(n,p)` qui implémente cet algorithme. Elle prend en arguments un entier naturel n non nul et un nombre premier p et renvoie la valuation p-adique de n. Par exemple, puisque $40 = 2^3 \times 5$, `valuation_p_adique(40,2)` renvoie 3, `valuation_p_adique(40,5)` renvoie 1 et `valuation_p_adique(40, 7)` renvoie 0.

4. Écrire une deuxième fonction cette fois-ci **récursive** `val_p_adique(n,p)` qui renvoie la valuation p-adique de n.

5. En déduire une fonction `decomposition_facteurs_premiers(n)` qui calcule la décomposition en facteurs premiers d'un entier $n \geq 2$.

Cette fonction doit renvoyer la liste des couples $(p, v_p(n))$ pour tous les nombres premiers p qui divisent n.

Par exemple, `decomposition_facteurs_premiers(40)` renvoie la liste `[[2, 3], [5, 1]]`.

PROBLÈME 1

On effectue une succession infinie de lancers indépendants d'une pièce donnant Pile avec la probabilité $p \in]0,1[$ et Face avec la probabilité $q = 1 - p$.
On va s'intéresser dans ce problème aux successions de lancers amenant un même côté.
On dit que la première série est de longueur $n \geqslant 1$ si les n premiers lancers ont amené le même côté de la pièce et le $(n+1)$-ième l'autre côté.
De même la deuxième série commence au lancer suivant la fin de la première série et se termine (si elle se termine) au lancer précédant un changement de côté.
On définit de même les séries suivantes.
Ω désigne l'ensemble des successions infinies de Pile ou Face.
Pour $i \in \mathbb{N}^{\times}$, on note P_i l'événement « le i-ième lancer amène Pile » et F_i l'événement contraire. Les trois parties sont indépendantes.

Partie I : Etude des longueurs de séries.

1. On note L_1 la longueur de la première série.
Exprimer l'événement $(L_1 = n)$ à l'aide des événements P_i et F_i pour i entier naturel variant entre 1 et $n+1$.
En déduire que

$$P(L_1 = n) = p^n q + q^n p$$

Vérifier que

$$\sum_{n=1}^{+\infty} P(L_1 = n) = 1$$

2. On note L_2 la longueur de la deuxième série.

- ***a.*** Exprimer l'événement $(L_1 = n) \cap (L_2 = k)$ à l'aide des événements P_i et F_i pour i entier naturel variant entre 1 et $n+k+1$ puis calculer la probabilité de l'événement $(L_1 = n) \cap (L_2 = k)$.
- ***b.*** En déduire que, pour $k \in \mathbb{N}^{\times}$,

$$P(L_2 = k) = p^2 q^{k-1} + q^2 p^{k-1}$$

- ***c.*** Montrer que $P(L_2 = +\infty) = 0$ (montrer que la probabilité que la deuxième série soit de longueur infinie est nulle).
- ***d.*** Calculer la longueur moyenne de la ducième série qui est donnée par $\displaystyle\sum_{k=1}^{+\infty} kP(L_2 = k)$.

Partie II : Etude du nombre de séries lors des n premiers lancers.

On considère dans toute cette partie que la pièce est **équilibrée, c'est-à-dire que** $p = \dfrac{1}{2}$.
On note N_n le nombre de séries **lors des n premiers lancers** :

- La première série est donc de longueur $k < n$ si les k premiers lancers ont amené le même côté de la pièce et le $(k+1)$-ième l'autre côté et de longueur n si les n premiers lancers ont amené le même côté de la pièce ;
- La dernière série se termine nécessairement au n-ième lancer.

Par exemple, si les lancers successifs donnent : FFPPPPFFPPP...(F désignant Face et P Pile), on a pour une telle succession $\omega \in \Omega$,

$$N_1(\omega) = N_2(\omega) = 1; \quad N_3(\omega) = \cdots = N_6(\omega) = 2; N_7(\omega) = N_8(\omega) = 3; \quad N_9(\omega) = \cdots = N_{11}(\omega) = 4;$$

les données précédentes ne permettant évidemment pas de déterminer $N_{12}(\omega)$.
On admettra que N_n est une variable aléatoire sur $(\Omega, \mathcal{A}, P)$.

1. Déterminer les lois de N_1, N_2 et N_3 et donner leurs espérances.

2. Dans le cas général où $n \in \mathbb{N}^\times$, déterminer $N_n(\Omega)$ (ensemble des valeurs prises par N_n) puis calculer les valeurs de $P(N_n = 1)$ et $P(N_n = n)$.

3. Simulation informatique.
Pour $k \in \mathbb{N}^*$, on note X_k la variable aléatoire qui vaut 1 lorsque le k-ième lancer amène Pile et 0 sinon. On rappelle qu'en langage PYTHON, avec que la commande suivante `import numpy.random as rd` permet d'accéder à la bibliothèque des probabilités et la fonction `rd.randint(0,2)` simule une variable aléatoire de loi uniforme sur $0, 1$ (soit une loi de Bernoulli de paramètre $1/2$). L'entier m inférieure à 100, écrire un programme qui simule les m variables aléatoires $X_1, X_2, \ldots, X_m$ (dont les valeurs seront placées dans une liste `X(m)`) et détermine les valeurs de $N_1, N_2, \ldots, N_m$ (qui seront stockées dans une liste `N(m)`).

4. **Fonctions génératrices de N_n.**
On pose, pour $n \in \mathbb{N}^\times$ et pour $s \in [0, 1]$,

$$G_n(s) = \sum_{k=1}^{n} P(N_n = k)s^k$$

a. Pour $s \in [0, 1]$, comparer l'espérance de la variable aléatoire s^{N_n} avec $G_n(s)$.

b. Que représente $G'_n(1)$?

c. Montrer que pour tout $n \geqslant 2$ et tout $k \in 1, \ldots, n$ on a

$$P((N_n = k) \cap P_n) = \frac{1}{2}P((N_{n-1} = k) \cap P_{n-1}) + \frac{1}{2}P((N_{n-1} = k-1) \cap F_{n-1})$$

On admet que l'on obtiendrait de même

$$P((N_n = k) \cap F_n) = \frac{1}{2}P((N_{n-1} = k) \cap F_{n-1}) + \frac{1}{2}P((N_{n-1} = k-1) \cap P_{n-1})$$

Montrer alors que

$$P(N_n = k) = \frac{1}{2}P(N_{n-1} = k) + \frac{1}{2}P(N_{n-1} = k-1)$$

d. Soit $n \geqslant 2$. Montrer que

$$G_n(s) = \frac{1+s}{2}G_{n-1}(s)$$

Calculer $G_1(s)$ et en déduire que

$$G_n(s) = \left(\frac{1+s}{2}\right)^{n-1} s$$

e. Déterminer le nombre moyen de séries dans les n premiers lancers.

Partie III : Probabilité d'avoir une infinité de fois deux Pile consécutifs.

1. Montrer que pour tout réel x on a

$$1 - x \leqslant e^{-x}$$

2. On considère dans cette question une suite $(A_i)_{i \in \mathbb{N}^\times}$ d'événements indépendants. On suppose que la série de terme général $P(A_i)$ diverge. Soit $k \in \mathbb{N}^\times$ fixé. Pour $n \geqslant k$, on note

$$C_n = \bigcup_{k \leqslant i \leqslant n} A_i = A_k \cup \cdots \cup A_n$$

a. Justifier que

$$\lim_{n\to+\infty} \sum_{i=k}^{n} P(A_i) = +\infty$$

b. Montrer que

$$P(C_n) = 1 - \prod_{i=k}^{n} P(\overline{A_i})$$

puis, en utilisant **III.1**, que

$$P(C_n) \geqslant 1 - \exp(-\sum_{i=k}^{n} P(A_i))$$

En déduire que

$$\lim_{n\to+\infty} P(C_n) = 1$$

c. Comparer pour l'inclusion les événements C_n et C_{n+1}. Que peut-on en déduire pour

$$P(\bigcup_{i=k}^{+\infty} C_i) \text{ ?}$$

d. Justifier que

$$\bigcup_{i=k}^{+\infty} A_i = \bigcup_{n=k}^{+\infty} C_n$$

et en déduire que

$$P(\bigcup_{i=k}^{+\infty} A_i) = 1$$

3. En considérant les événements A_n « on obtient Pile au $(2n)$-ième et au $(2n+1)$-ième lancers », montrer que la probabilité d'avoir deux Pile consécutifs, après n'importe quel lancer, vaut 1.

PROBLÈME 2 (FACULTATIF)

Dans ce problème, n désigne un entier non nul fixé.
On note $\mathcal{M}_n(\mathbb{C})$ (respectivement $\mathcal{M}_n(\mathbb{R})$) l'espace vectoriel des matrices carrées de taille n à coefficients dans $\mathbb{C}$ (respectivement $\mathbb{R}$), $\mathrm{GL}_n(\mathbb{C})$ l'ensemble des matrices inversibles de taille n à coefficients dans $\mathbb{C}$ et $\mathcal{M}_{n,1}(\mathbb{C})$ l'espace vectoriel des matrices colonnes de taille n à coefficients dans $\mathbb{C}$.
Pour toute matrice $M \in \mathcal{M}_n(\mathbb{C})$, on note $\chi_M = \det(XI_n - M)$ son polynôme caractéristique et $\mathrm{Sp}(M)$ l'ensemble de ses valeurs propres complexes. On pourra utiliser librement les produits matriciels par blocs.

Objectifs
On s'intéresse dans la **Partie I** à trois cas particuliers.
On montre d'abord que $\det(I_n + C\overline{C}) \geq 1$ dans le cas particulier des matrices diagonales complexes C, où $\overline{C}$ désigne la matrice conjuguée de C, c'est-à-dire la matrice obtenue en considérant le conjugué de chaque coefficient de C.
On montre ensuite que $\det(I_n + C^2) \geq 1$ dans le cas particulier des matrices symétriques réelles C.
On considère enfin le cas des matrices réelles C pour lesquelles on démontre que $\det(I_n + C^2) \in \mathbb{R}_+$.

La **Partie II** est consacrée au cas général.
On montre que pour toute matrice C de $\mathcal{M}_n(\mathbb{C})$, $\det(I_n + C\overline{C}) \in \mathbb{R}_+$.

Partie I – Trois cas particuliers

1. Écrire en PYTHON une fonction `M(C)` qui prend pour argument C et renvoie la matrice $\begin{pmatrix} I_n & -C \\ \overline{C} & I_n \end{pmatrix}$.

2. ***a.*** On se place dans le cas particulier où C est une matrice de $\mathcal{M}_n(\mathbb{C})$ diagonale. Démontrer que $\det(I_n + C\overline{C}) \in \mathbb{R}$ et que :

$$\det(I_n + C\overline{C}) \geq 1,$$

avec égalité si et seulement si $C = 0_{\mathcal{M}_n(\mathbb{C})}$.

b. On se place dans le cas particulier où C est une matrice de $\mathcal{M}_n(\mathbb{R})$ symétrique. Démontrer que :

$$\det(I_n + C^2) \geq 1,$$

avec égalité si et seulement si $C = 0_{\mathcal{M}_n(\mathbb{R})}$.

3. Démontrer que : $\forall A \in \mathcal{M}_n(\mathbb{C}), \det(\overline{A}) = \overline{\det(A)}$.

4. On suppose dans cette question que C est une matrice de $\mathcal{M}_n(\mathbb{R})$. Déduire de la question précédente que, dans ce cas, on a :

$$\det(I_n + C^2) = |\det(C - iI_n)|^2.$$

En déduire que $\det(I_n + C^2) \in \mathbb{R}_+$ et que $\det(I_n + C^2) = 0$ si et seulement si $i \in \mathrm{Sp}(C)$.

Partie II – Le cas général

On considère dans cette partie une matrice C de $\mathcal{M}_n(\mathbb{C})$ et on démontre que $\det(I_n + C\overline{C}) \in \mathbb{R}_+$.
Seule la **3** de la partie I sera utile pour la suite.

5. En considérant le produit matriciel $\begin{pmatrix} I_n & -C \\ \overline{C} & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -\overline{C} & I_n \end{pmatrix}$, démontrer que :

$$\det(I_n + C\overline{C}) = \det \begin{pmatrix} I_n & -C \\ \overline{C} & I_n \end{pmatrix}$$

On notera désormais : $C_0 = \begin{pmatrix} I_n & -C \\ \overline{C} & I_n \end{pmatrix}$

6. Soient $(r,s,t,u) \in \mathbb{C}^4$ et (e_1,e_2) la base canonique de $\mathbb{C}^2$. On note ϕ l'endomorphisme de $\mathbb{C}^2$ dont la matrice dans la base (e_1,e_2) est $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$. Exprimer la matrice de ϕ dans la base (e_2,e_1).

7. Soit $(R,S,T,U) \in (\mathcal{M}_n(\mathbb{C}))^4$. En s'inspirant de la question précédente, montrer que la matrice $\begin{pmatrix} R & S \\ T & U \end{pmatrix}$ est semblable dans $\mathcal{M}_{2n}(\mathbb{C})$ à la matrice $\begin{pmatrix} U & T \\ S & R \end{pmatrix}$. Montrer de même que $\begin{pmatrix} R & S \\ T & U \end{pmatrix}$ est semblable à la matrice $\begin{pmatrix} R & -S \\ -T & U \end{pmatrix}$.

8. En déduire que le polynôme caractéristique de la matrice C_0 est à coefficients réels.

Pour la suite, nous écrirons les vecteurs de $\mathcal{M}_{2n,1}(\mathbb{C})$ sous la forme $\begin{pmatrix} X \\ Y \end{pmatrix}$, où $(X,Y) \in (\mathcal{M}_{n,1}(\mathbb{C}))^2$. On considère l'application $\Omega : \mathcal{M}_{2n,1}(\mathbb{C}) \to \mathcal{M}_{2n,1}(\mathbb{C})$ définie par :

$$\forall \begin{pmatrix} X \\ Y \end{pmatrix} \in \mathcal{M}_{2n,1}(\mathbb{C}),\ \Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right) = \begin{pmatrix} -\overline{Y} \\ \overline{X} \end{pmatrix}.$$

9. Démontrer les propriétés suivantes de l'application Ω :

a. Pour tout $\begin{pmatrix} X \\ Y \end{pmatrix} \in \mathcal{M}_{2n,1}(\mathbb{C}),\ C_0\Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right) = \Omega\left(C_0\begin{pmatrix} X \\ Y \end{pmatrix}\right)$;

b. $\Omega \circ \Omega = -\mathrm{Id}_{\mathcal{M}_{2n,1}(\mathbb{C})}$;

c. Pour tout $\begin{pmatrix} X \\ Y \end{pmatrix} \in \mathcal{M}_{2n,1}(\mathbb{C})$ et tout $\lambda \in \mathbb{C},\ \Omega\left(\lambda\begin{pmatrix} X \\ Y \end{pmatrix}\right) = \overline{\lambda}\Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right)$

10. Soit $\begin{pmatrix} X \\ Y \end{pmatrix} \in \mathcal{M}_{2n,1}(\mathbb{C}) \setminus \{0_{\mathcal{M}_{2n,1}(\mathbb{C})}\}$.

Montrer que la famille $\left(\begin{pmatrix} X \\ Y \end{pmatrix}, \Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right)\right)$ est libre et que le plan $\mathrm{Vect}\left(\begin{pmatrix} X \\ Y \end{pmatrix}, \Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right)\right)$ est stable par Ω.

11. Soit E un sous-espace vectoriel de$\mathcal{M}_{2n,1}(\mathbb{C})$ stable par Ω et soit $\begin{pmatrix} X \\ Y \end{pmatrix} \in \mathcal{M}_{2n,1}(\mathbb{C}) \setminus E$.

Montrer que :

$$E \cap \mathrm{Vect}\left(\begin{pmatrix} X \\ Y \end{pmatrix}, \Omega\left(\begin{pmatrix} X \\ Y \end{pmatrix}\right)\right) = \{0_{\mathcal{M}_{2n,1}(\mathbb{C})}\}.$$

Pour tout $\lambda \in \mathrm{Sp}(C_0)$, on note $\alpha_\lambda \in \mathbb{N}^*$ sa multiplicité comme racine du polynôme caractéristique. On peut donc écrire : $\chi_{C_0} = \prod_{\lambda\,\mathrm{Sp}(C_0)} (X-\lambda)^{\alpha_\lambda}$. On note alors, pour tout $\lambda \in \mathrm{Sp}(C_0)$:

$$F_\lambda = \mathrm{Ker}\left((\lambda I_{2n} - C_0)^{\alpha_\lambda}\right).$$

12. Montrer que pour tout $\lambda \in \mathrm{Sp}(C_0)$, on a : $\Omega(F_\lambda) = F_{\overline{\lambda}}$.

13. Montrer que si $\lambda \in \mathrm{Sp}(C_0) \cap \mathbb{R}$, alors F_λ est de dimension paire.

14. Soit $\lambda \in Sp(C_0)$. Soit $Q \in \mathbb{C}[X]$ tel que $\chi_{C_0} = (X-\lambda)^{\alpha_\lambda}Q$. Soit f l'endomorphisme canoniquement associé à C_0. On a donc $F_\lambda = \mathrm{Ker}\left((\lambda I_{\mathcal{M}_{2n,1}(\mathbb{C})} - f)^{\alpha_\lambda}\right)$.

a. Montrer que $\mathcal{M}_{2n,1}(\mathbb{C}) = F_\lambda \oplus K$, avec $K = \mathrm{Ker}\,(Q(f))$.

b. Montrer que f induit des endomorphismes sur F_λ et $\mathrm{Ker}\,(Q(f))$, que l'on note respectivement f_1 et f_2.

c. Montrer que λ n'est pas valeur propre de f_2.

d. Montrer que $\chi_{C_0} = (X-\lambda)^{\dim(F_\lambda)}R$, avec R dans $\mathbb{C}[X]$ tel que $R(\lambda) \neq 0$.

e. En déduire que $\dim(F_\lambda) = \alpha_\lambda$.

15. Conclure que : $\det(C_0) \in \mathbb{R}_+$.

PROBLÈME 1

Notations :

- Si x est un nombre réel on note $[x]$ sa partie entière, c'est-à-dire le plus grand entier relatif qui est inférieur ou égal à x.
- On appelle cardinal de l'ensemble fini E le nombre de ses éléments, que l'on note $|E|$.
- On note $\mathcal{P}(E)$ l'ensemble des parties de l'ensemble E.
- Dans tout le problème on identifiera $\mathbb{R}^n$ à l'espace des matrices lignes $\mathcal{M}_{1,n}(\mathbb{R})$ et on notera $\langle x, y\rangle$ le produit scalaire canonique de ces vecteurs, soit
$$\langle x, y\rangle = \sum_{j=1}^{n} x_j y_j,$$
les x_j, y_j étant les composantes de x et y respectivement.
- Si $\mathcal{V}$ est un sous-ensemble de $\mathbb{R}^n$ on note $\mathrm{Vect}(\mathcal{V})$ l'espace vectoriel engendré par $\mathcal{V}$. On note $\mathcal{V}^\perp$ l'orthogonal de $\mathcal{V}$, c'est-à-dire l'ensemble des vecteurs y tels que $\forall x \in \mathcal{V}$, $\langle x, y\rangle = 0$.
- Si M est une matrice carrée de nombres réels, on note $\det(M)$ son déterminant.

Dans tout le problème on pourra utiliser librement la formule de Stirling que l'on rappelle :
$$n! \underset{n\to+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Définition 1 ***(Espace de Rademacher)*** *Si $n, q \in \mathbb{N}^*$, on note*
$$\Omega_{q,n} = \{\omega = (\omega_{i,j},\ 1 \le i \le q,\ 1 \le j \le n) \text{ tels que } :\forall (i,j) \in [\![1,q]\!] \times [\![1,n]\!],\ \omega_{i,j} = \pm 1\}.$$
Pour tout $i \in \{1, \dots, q\}$ et $j \in \{1, \dots, n\}$, on introduit la variable aléatoire $M_{i,j}$ telle que
$$M_{i,j} : \left\{ \begin{array}{ccc} \Omega_{q,n} & \to & \{-1, 1\} \\ \omega & \mapsto & \omega_{i,j} \end{array} \right. .$$
On munit $\Omega_{q,n}$ de la probabilité uniforme P. Cela signifie que les variables $(M_{i,j},\ 1 \le i \le q,\ 1 \le j \le n)$ sont indépendantes et de même loi :
$$P(M_{i,j} = 1) = \frac{1}{2} = P(M_{i,j} = -1).$$
Si $q = n$, on note $M^{(n)}$ la matrice aléatoire
$$M^{(n)} = \begin{pmatrix} M_{1,1} & \cdots & M_{1,n} \\ \vdots & & \vdots \\ M_{n,1} & \cdots & M_{n,n} \end{pmatrix}.$$
On note $L_1^{(n)}, \dots, L_n^{(n)}$ les vecteurs lignes de $M^{(n)}$. Par construction, ce sont des vecteurs aléatoires indépendants et de même loi.

Le but du problème est de démontrer, qu'ainsi construite, une matrice aléatoire est inversible avec forte probabilité quand n est grand :

Théorème 1 ***(Komlós)*** $\displaystyle\lim_{n\to+\infty} P(\det(M^{(n)}) = 0) = 0.$

A 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.

1. Écrire en PYTHON une fonction `modifie_matrice(p, A)` qui prend en argument une probabilité p et un tableau `numpy` représentant une matrice A de $\mathcal{M}_n(\mathbb{R})$ à coefficients dans $\{-1, 1\}$. Cette fonction modifie le tableau a selon le procédé décrit ci-dessus.

2. En utilisant la fonction précédente, écrire en PYTHON une fonction `nb_tours(p, n)` qui prend en argument une probabilité p et l'ordre n des matrices A_k et renvoie le plus petit entier k tel que $A_k = -A_0$, en partant de la matrice A_0.

3. Écrire en PYTHON une fonction `moyenne_tours(p, n, nbe)` qui prend en argument une probabilité p, l'ordre n des matrices A_k et un nombre entier `nbe` et qui renvoie la moyenne, sur `nbe` essais effectués, du nombre d'étapes nécessaires pour passer de A_0 à $-A_0$.

B Coefficients binomiaux

4. Soit $n \in \mathbb{N}^*$: montrer que l'application

$$k \mapsto \binom{n}{k}$$

est croissante sur $\{0, \ldots, [n/2]\}$. En déduire que pour tout $k \in \{0, \ldots, n\}$,

$$\binom{n}{k} \leq \binom{n}{[n/2]}.$$

5. Trouver un équivalent de $\binom{n}{[n/2]}$ quand n tend vers l'infini. En déduire qu'il existe un entier n_0 tel que pour $n \geq n_0$,

$$\binom{n}{[n/2]} \leq \frac{2^n}{\sqrt{n}}. \qquad (1)$$

6. Montrer que pour tout entier non nul n et tout $k \in \{0, \ldots, n\}$,

$$\binom{n}{k} 2^{k-1} \leq n^k.$$

On note $(e_i,\ 1 \leq i \leq n)$ la base canonique de $\mathbb{R}^n$ et $v = \sum_{i=1}^{n} e_i$. On identifie $\Omega_{1,n}$ et le sous-

ensemble de $\mathbb{R}^n$
$$\left\{\sum_{i=1}^{n} \omega_i e_i,\ (\omega_1, \ldots, \omega_n) \in \Omega_{1,n}\right\}.$$

7. Pour tout $i \in \{1, \ldots, n\}$, exprimer e_i en fonction de v et $v - 2e_i$. En déduire que $\mathrm{Vect}(\Omega_{1,n}) = \mathbb{R}^n$.

C Dimension 2

8. Déterminer l'espérance de $\det M^{(2)}$.

9. Montrer que la variance de $\det M^{(2)}$ est égale à 2.

10. Calculer $P(\det M^{(2)} = 0)$.

D Quelques bornes

On suppose dorénavant $n \geq 2$.

11. Quelle est la probabilité que les deux premières lignes de $M^{(n)}$ soit égales ou opposées ? En déduire que $P\left(\det M^{(n)} = 0\right) \geq 2^{1-n}$ si $n \geq 2$.

12. Soient $l_1, \ldots, l_n$ des vecteurs non nuls de $\mathbb{R}^n$. Montrer que ces vecteurs sont liés si et seulement si, il existe $j \in \{1, \ldots, n-1\}$ tel que
$$l_{j+1} \in \mathrm{Vect}(\{l_1, \cdots, l_j\}).$$
En déduire que
$$P(\det M^{(n)} = 0) \leq \sum_{j=1}^{n-1} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)}\right). \qquad (2)$$
Soit $\mathcal{H}$ un sous-espace vectoriel de $\mathbb{R}^n$ de dimension d. On rappelle que $\mathcal{H}^\perp$ est un sous-espace vectoriel de dimension $n - d$ et que $(\mathcal{H}^\perp)^\perp = \mathcal{H}$.

13. Montrer alors qu'il existe des réels $(\alpha_{i,j},\ 1 \leq i \leq n-d,\ 1 \leq j \leq n)$ tels que
$$x = (x_1, \ldots, x_n) \in \mathcal{H} \Leftrightarrow \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \vdots & & \vdots \\ \alpha_{n-d,1} & \cdots & \alpha_{n-d,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

14. Montrer qu'il existe $1 \leq i_1 < \cdots < i_d \leq n$ tel que pour tout $(y_1, \ldots, y_d) \in \mathbb{R}^d$ il existe un unique $x = (x_1, \ldots, x_n) \in \mathcal{H}$ tel que $x_{i_k} = y_k$ pour $k = 1, \ldots, d$.

15. En déduire que
$$P(L_1^{(n)} \in \mathcal{H}) \leq 2^{d-n},$$
puis que pour tout $j \in \{1, \ldots, n-1\}$,
$$P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) \leq 2^{j-n} \qquad (3)$$
Indication : on pourra utiliser la conséquence suivante de la formule des probabilités totales
$$P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) = \sum_{l_1, \ldots, l_j \in \Omega_{1,n}} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)}) | L_1^{(n)} = l_1, \ldots, L_j^{(n)} = l_j\right)$$
$$\times P\left(L_1^{(n)} = l_1, \ldots, L_j^{(n)} = l_j\right)$$
et l'indépendance des vecteurs lignes. Soit $q < n$ et $\omega \in \Omega_{q,n}$. On note $l_1, \cdots, l_q$ ses vecteurs lignes.

16. Montrer que l'on peut trouver un vecteur non nul orthogonal à $\mathrm{Vect}(l_i,\ i = 1, \ldots, q)$ qui soit à coordonnées dans $\mathbb{Z}$.

E Théorème de Erdös-Littlewood-Offord

Définition 2 *Soit n un entier non nul. Soit $\mathcal{A}$ un sous-ensemble de $\mathcal{P}(\{1,\ldots,n\})$. On dit que $\mathcal{A}$ est une anti-chaîne si deux éléments distincts A et B quelconques de $\mathcal{A}$ sont incomparables, c'est-à-dire tels que A n'est pas inclus dans B et B n'est pas inclus dans A.*

Commençons par un exemple. Soit $k \in \{1,\ldots,n\}$ et $\mathcal{A}_k$ l'ensemble des parties de $\{1,\ldots,n\}$ de cardinal k.

17. Montrer que $\mathcal{A}_k$ est une anti-chaîne et que

$$|\mathcal{A}_k| \leq \binom{n}{[n/2]} \leq \frac{2^n}{\sqrt{n}},$$

la deuxième inégalité ayant lieu pour n assez grand.

Définition 3 *Soit $\mathcal{A}$ une anti-chaîne et $A \in \mathcal{A}$, de cardinal noté $|A|$. On note S_A, l'ensemble des bijections σ de $\{1,\ldots,n\}$ dans lui-même telles que la restriction de σ à $\{1,\ldots,|A|\}$ soit une bijection de $\{1,\ldots,|A|\}$ dans A.*

18. Quel est le cardinal de S_A ?

19. Soit $B \in \mathcal{A}$ avec $B \neq A$. Montrer que $S_A \cap S_B = \emptyset$.

20. En déduire que si a_k désigne, pour $k \leq n$, le nombre d'éléments de $\mathcal{A}$ de cardinal k, alors

$$\sum_{k=0}^{n} \frac{a_k}{\binom{n}{k}} \leq 1.$$

21. Montrer que

$$|\mathcal{A}| \leq \binom{n}{[n/2]}.$$

Soit $v = (v_1,\ldots,v_n) \in \mathbb{R}^n$ tel que $v_j \geq 1$ pour tout $j = 1,\ldots,n$. Si $A \subset \{1,\ldots,n\}$ on pose

$$s_A = \sum_{j\in A} v_j - \sum_{j\in A^c} v_j$$

où A^c est le complémentaire de A dans $\{1,\ldots,n\}$.

22. Montrer que si $A \subset B \subset \{1,\ldots,n\}$, $A \neq B$, alors

$$s_B - s_A \geq 2.$$

23. Soit J un intervalle ouvert de $\mathbb{R}$ de longueur 2 : montrer que si n est assez grand alors

$$P(\langle L_1^{(n)}, v\rangle \in J) \leq \frac{1}{\sqrt{n}}.$$

Montrer que cette propriété reste vraie si l'on suppose seulement que pour tout $j \in \{1,\ldots,n\}$, $|v_j| \geq 1$. *Indication : construire une bijection entre $\Omega_{1,n}$ et l'ensemble des parties de $\{1,\ldots,n\}$. Construire une anti-chaîne intéressante.*

F Universalité

Dans tout ce qui suit, k est un entier inférieur à n.

Définition 4 *Soit $\mathcal{V} \subset \Omega_{1,n}$. L'ensemble $\mathcal{V}$ est dit k-universel si pour tous les k-uplets $1 \leq j_1 < j_2 \cdots < j_k \leq n$ et tout $\omega \in \Omega_{1,n}$, il existe $v \in \mathcal{V}$ tel que*

$$v_{j_m} = \omega_{1,j_m}, \text{ pour tout } m = 1, \ldots, k.$$

24. Soit $d \in \{1, \ldots, n\}$. Montrer l'inclusion

$$\left\{\{L_1^{(n)}, \ldots, L_d^{(n)}\} \text{ non } k\text{-universel}\right\} \subset \bigcup_{\substack{(j_1,\ldots,j_k)\in\{1,\ldots,n\}^k \\ j_1<\cdots<j_k}} \bigcup_{\omega\in\Omega_{1,k}} \bigcap_{i=1}^{d} \bigcup_{m=1}^{k} \{M_{i,j_m} \neq \omega_{1,j_m}\}.$$

(On rappelle que $L_i^{(n)} = (M_{i,1}, \ldots, M_{i,n})$).

25. Montrer que la probabilité que $\{L_1^{(n)}, \ldots, L_d^{(n)}\}$ ne soit pas k-universel est majorée par

$$\binom{n}{k} 2^k (1 - 2^{-k})^d.$$

26. En déduire que si $d \geq n/2$ et $k \leq \ln n$, alors, pour n assez grand,

$$P\left(\{L_1^{(n)}, \ldots, L_d^{(n)} \text{ non } k\text{-universel}\right) \leq \frac{1}{n}. \qquad (4)$$

27. Soit $\mathcal{V} \subset \Omega_{1,n}$ un ensemble k-universel tel qu'il existe $v \in \mathcal{V}^\perp \setminus \{0\}$: montrer que v a au moins $k+1$ coordonnées non nulles. En vertu de la question 16, on peut supposer que les coordonnées de v sont des entiers relatifs.

28. Montrer que si k est assez grand

$$P\left(L_1^{(n)} \in \mathrm{Vect}(\mathcal{V})\right) \leq P(\langle L_1^{(n)}, v\rangle = 0) \leq k^{-1/2}. \qquad (5)$$

Soit $(t_n, n \in \mathbb{N})$ une suite croissante d'entiers telle que $t_n/n \to 0$.

29. Montrer que si n est assez grand alors $n - t_n \geq n/2$ et

$$\sum_{j=n-t_n+1}^{n-1} P\left(L_{j+1}^{(n)} \in \mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})\right) \leq \frac{2t_n}{\sqrt{\ln n}}. \qquad (6)$$

Indication : on distinguera les cas selon que $\mathrm{Vect}(L_1^{(n)}, \ldots, L_j^{(n)})$ est k-universel ou pas et l'on prendra $k = [\ln n]$.

G Théorème de Komlós

30. En déduire le théorème de Komlós.
Indication : on pourra partir de (2) et choisir convenablement une suite $(t_n,\ n \geq 1)$.

Dans tout le problème, les espaces vectoriels considérés ont $\mathbb{C}$, le corps des complexes, pour corps de base.
Etant donnés deux entiers naturels n et p non nuls, on note $M_{n,p}(\mathbb{C})$ l'espace vectoriel des matrices à n lignes et p colonnes et à coefficients dans $\mathbb{C}$ (et $0_{n,p}$ sa matrice nulle) et $M_n(\mathbb{C})$ celui des matrices carrées à n lignes et à coefficients dans $\mathbb{C}$ (et 0_n sa matrice nulle).
Soit E un $\mathbb{C}$-espace vectoriel. On note $\mathcal{L}(E)$ l'espace vectoriel des endomorphismes de E.
Un endomorphisme u de E est dit **échangeur** lorsqu'il existe des sous-espaces vectoriels F et G de E tels que

$$E = F \oplus G, \ u(F) \subset G \ \text{ et } \ u(G) \subset F$$

Etant donnés deux endomorphismes u et v de E, on dit que v est **semblable** à u lorsqu'il existe un automorphisme φ de E tel que $v = \varphi \circ u \circ \varphi^{-1}$. On notera que dans ce cas $u = \varphi^{-1} \circ v \circ (\varphi^{-1})^{-1}$, si bien que u est semblable à v.
On dit que u est **de carré nul** lorsque u^2 est l'endomorphisme nul de E. On dit que u est **nilpotent** lorsqu'il existe un entier naturel $n \geq 1$ tel que $u^n = 0$.
Une matrice $A \in M_n(\mathbb{C})$ est dite **de carré nul** lorsque $A^2 = 0$.

L'objectif du problème est d'établir, pour un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie, l'équivalence entre les conditions suivantes :

- **(C1)** l'endomorphisme u est échangeur ;
- **(C2)** il existe $a, b \in \mathcal{L}(E)$, tous deux de carré nul, tels que $u = a + b$;
- **(C3)** les endomorphismes u et $-u$ sont semblables.

Chacune des parties A et B est indépendante des autres. Les résultats de la partie D sont essentiels au traitement des parties E et F.

A. Quelques considérations en dimension 2

On se donne ici un $\mathbb{C}$-espace vectoriel de dimension 2 et un endomorphisme u de E.

1. Montrer que si u vérifie la condition **(C3)** alors u est de trace nulle.
Jusqu'à la fin de cette partie, on suppose u de trace nulle et de déterminant non nul.
On choisit un nombre complexe δ tel que $\delta^2 = -\det(u)$.

2. Déterminer le spectre de u, montrer que $u^2 = \delta^2 \mathrm{I}_E$, et préciser la dimension des sous-espaces propres.

3. Expliciter, à l'aide de vecteurs propres de u, une droite vectorielle D telle que $u(D) \not\subset D$ et en déduire que u est échangeur.

B. La condition (C1) implique (C2) et (C3)

Soient n et p deux entiers naturels non nuls. Soient $A \in M_{p,n}(\mathbb{C})$ et $B \in M_{n,p}(\mathbb{C})$. On considère dans $M_{n+p}(\mathbb{C})$ la matrice

$$M = \begin{pmatrix} 0_n & B \\ A & 0_p \end{pmatrix}$$

4. Calculer le carré de la matrice $\begin{pmatrix} 0_n & B \\ 0_{p,n} & 0_p \end{pmatrix}$ de $M_{n+p}(\mathbb{C})$. Montrer ensuite que M est la somme de deux matrices de carré nul.

5. On considère dans $M_{n+p}(\mathbb{C})$ la matrice diagonale par blocs

$$D = \begin{pmatrix} I_n & 0_{n,p} \\ 0_{p,n} & -I_p \end{pmatrix}$$

Montrer que D est inversible, calculer D^{-1} puis DMD^{-1}, et en déduire que M est semblable à $-M$.

Jusqu'à la fin de cette partie, on se donne un endomorphisme u d'un $\mathbb{C}$-espace vectoriel E de dimension finie. On suppose que u est échangeur et on se donne donc une décomposition $E = F \oplus G$ dans laquelle F et G sont des sous-espaces vectoriels vérifiant $u(F) \subset G$ et $u(G) \subset F$.

6. On suppose ici F et G tous deux non nuls.
On se donne une base $(f_1, \ldots, f_n)$ de F et une base $(g_1, \ldots, g_p)$ de G.
La famille $B = (f_1, \ldots, f_n, g_1, \ldots, g_p)$ est donc une base de E.
Compte-tenu des hypothèses, décrire la forme de la matrice u dans B.

7. Déduire des questions précédentes que u vérifie **(C2)***et*(**C3**). *On n'oubliera pas de considérer le cas où l'un des sous-espaces F ou G est nul.*

C. La condition (C2) implique (C1) : cas d'un automorphisme

Dans cette partie, u désigne un automorphisme d'un $\mathbb{C}$-espace vectoriel E de dimension finie. On suppose qu'il existe deux endomorphismes a et b de E tels que

$$u = a + b \quad \text{et} \quad a^2 = b^2 = 0$$

8. Soit f un endomorphisme de E tel que $f^2 = 0$. Comparer $\operatorname{Ker}(f)$ à $\operatorname{Im}(f)$ et en déduire

$$\dim(\operatorname{Ker}(f)) \geq \frac{1}{2}\dim(E)$$

9. Démontrer que $E = \operatorname{Ker}(a) \oplus \operatorname{Ker}(b)$, et que $\operatorname{Ker}(a) = \operatorname{Im}(a)$ et $\operatorname{Ker}(b) = \operatorname{Im}(b)$.

10. En déduire que u est échangeur.

D. Intermède : un principe de décomposition

On se donne dans cette partie un $\mathbb{C}$-espace vectoriel E de dimension finie, ainsi qu'un endomorphisme f de E. On se donne un nombre complexe arbitraire λ. On pose $v = f - \lambda \mathrm{I}_E$.

11. Montrer que la suite $(\operatorname{Ker}(v^k))_{k\in\mathbb{N}}$ est croissante pour l'inclusion.

12. Montrer qu'il existe un entier naturel p tel que

$$\forall k \geq p,\ \operatorname{Ker}(v^k) = \operatorname{Ker}(v^p)$$

On pourra introduire la plus grande dimension possible pour un sous-espace vectoriel de la forme $\operatorname{Ker}(v^k)$ *pour* $k \in \mathbb{N}$.
Montrer qu'alors

$$\operatorname{Ker}(v^p) = \bigcup_{k\in\mathbb{N}} \operatorname{Ker}(v^k)$$

et que p peut être choisi parmi les entiers pairs.

Dans la suite de cette partie, on fixe un entier naturel pair p donné par la question 12 et l'on pose

$$E_\lambda^c(f) = \bigcup_{k\in\mathbb{N}} \operatorname{Ker}(v^k) = \operatorname{Ker}(v^p)$$

On notera que $E_\lambda^c(f)$ est un sous-espace vectoriel de E.

13. Montrer que $E^c_\lambda(f) = \mathrm{Ker}\,(v^{2p})$ et en déduire

$$E = E^c_\lambda(f) \oplus \mathrm{Im}(v^p)$$

Montrer en outre que les sous-espaces vectoriels $E^c_\lambda(f)$ et $\mathrm{Im}(v^p)$ sont tous deux stables par f.

14. Montrer que λ n'est pas valeur propre de l'endomorphisme induit par f sur $\mathrm{Im}(v^p)$. Montrer que si $E^c_\lambda(f)$ n'est pas nul alors λ est l'unique valeur propre de l'endomorphisme induit par f sur $E^c_\lambda(f)$.

15. On se donne ici un nombre complexe $\mu \neq \lambda$. On suppose que toute valeur propre de f différente de λ est égale à μ.
Montrer que $\mathrm{Im}(v^p) \subset E^c_\mu(f)$.
On pourra adapter les questions 12 et 13 à $g = f|_{\mathrm{Im}(v^p)}$ *en remplaçant* λ *par* μ.
En déduire que $E = E^c_\lambda(f) \oplus E^c_\mu(f)$.

E. La condition (C2) implique (C1) : cas non bijectif

Dans cette partie, on admet la validité de l'énoncé suivant.

Théorème : tout endomorphisme nilpotent d'un espace vectoriel de dimension finie est échangeur.

On se donne ici un endomorphisme non bijectif u d'un $\mathbb{C}$-espace vectoriel E de dimension finie. On suppose qu'il existe deux endomorphismes a et b de E tels que

$$u = a + b \quad \text{et} \quad a^2 = b^2 = 0$$

16. Montrer que a et b commutent avec u^2.
On fixe maintenant un entier pair p tel que $E^c_0(u) = \mathrm{Ker}\,(u^p)$, donné par la question 12.

17. Montrer que le sous-espace vectoriel $G = \mathrm{Im}(u^p)$ est stable par a et b et que les endomorphismes induits a_G et b_G sont de carré nul.

18. En déduire que u est échangeur. *On pourra utiliser, entre autres, le résultat final de la partie C.*

F. La condition (C3) implique (C1)

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie non nulle.
Un endomorphisme u de E est dit **indécomposable** lorsque
(i) la condition **(C3)** est vérifiée par u
(ii) il n'existe aucune décomposition $E = F \oplus G$ dans laquelle F et G sont des sous-espaces non nuls, stables par u et tels que les endomorphismes induits u_F et u_G vérifient tous deux la condition **(C3)**.

Jusqu'à la question 21 incluse, on se donne un endomorphisme indécomposable u de E. On dispose en particulier d'un automorphisme φ de E tel que

$$-u = \varphi \circ u \circ \varphi^{-1}$$

19. Montrer que φ^2 commute avec u.

20. Montrer que φ^2 possède une unique valeur propre λ. En déduire que les valeurs propres de φ sont parmi α et $-\alpha$, pour un certain nombre complexe non nul α.
On utilisera l'indécomposabilité de u ainsi que les résultats des questions 13 et 14.

21. En déduire que u est échangeur.
On pourra appliquer le résultat final de la question 15.

22. En déduire plus généralement que, pour tout endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie, la condition **(C3)** implique la condition **(C1)**.