

Exercice 1. On note E_1, \dots, E_n les vecteurs élémentaires de \mathbb{R}^n . On considère $\Delta = \{X \in \mathbb{R}^n \mid \forall i, x_i \geq 0 \text{ et } x_1 + \dots + x_n = 1\}$. On note $X \leq Y$ si $\forall i, x_i \leq y_i$, et $E \in \mathbb{R}^n$ le vecteur dont toutes les coordonnées valent 1.

I. Étude des ensembles donnés

- 1) Vérifier brièvement que \leq est une relation d'ordre sur \mathbb{R}^n . Est-elle totale ?
- 2) On identifie l'ensemble \mathbb{R}^n à des matrices colonnes, et l'ensemble $\mathcal{M}_{1,1}(\mathbb{R})$ à \mathbb{R} .
 - a) Pour $X, Y \in \mathbb{R}^n$, calculer $X^T Y$. Pour $X \in \Delta$, que dire de $X^T E$?
 - b) Pour $A \in \mathcal{M}_n(\mathbb{R})$, donner une expression de $X^T A Y$. En déduire la valeur de $E_i^T A E_j$.

Dans tout le problème, on considère, pour une matrice de $A \in \mathcal{M}_n(\mathbb{R})$, les quantités

$$\text{maximin}(A) = \sup_{X \in \Delta} \left(\inf_{Y \in \Delta} X^T A Y \right) \quad \text{et} \quad \text{minimax}(A) = \inf_{Y \in \Delta} \left(\sup_{X \in \Delta} X^T A Y \right)$$

II. Étude de matrices particulières. On considère $S = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}$ et $J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$.

- 1) Etude des puissances de S .
 - a) Décrire les puissances de J . La matrice J est-elle inversible ?
 - b) Exprimer S en fonction de J et J^2 . En déduire que $S^3 = -3S$.
 - c) La matrice S est-elle inversible ?
 - d) Exprimer, pour $k \geq 1$, la matrice S^k simplement, en fonction de la parité de k .
- 2) Dans cette partie, on prend $n = 3$. On considère $X \in \Delta$, que l'on écrit $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.
 - a) Montrer que pour tout $i, j \in \llbracket 1, 3 \rrbracket$, $x_i - x_j \in [-1, 1]$ et calculer $(x_3 - x_2) + (x_1 - x_3) + (x_2 - x_1)$.
 - b) Donner, pour tout $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \Delta$ l'expression de $X^T S Y$. En déduire que :

$$\inf_{Y \in \Delta} X^T S Y = \min(x_3 - x_2, x_1 - x_3, x_2 - x_1)$$

Indication : Ici pour montrer que $\inf A = \alpha$: montrer que α est un minorant, et qu'il est atteint ($\alpha \in A$).

- c) Montrer que $\text{maximin}(S) = 0$ et que cette valeur est atteinte pour un vecteur X à préciser.
 Un raisonnement similaire permettrait de montrer que $\text{minimax}(S) = 0$, donc que l'on a $\text{minimax}(S) = \text{maximin}(S)$, qui est un cas particulier du théorème du minimax de von Neumann.

Exercice 2. Soit $k \geq 3$. On considère une suite $(x_n)_{n \geq 0}$ définie par x_0, \dots, x_{k-1} et la relation de récurrence

$$\forall n \in \mathbb{N}, x_{n+k} = \frac{x_n + x_{n+1} + \dots + x_{n+k-1}}{k}.$$

On considère alors, pour tout $n \geq 0$, $M_n = \max(x_n, x_{n+1}, \dots, x_{n+k-1})$ et $m_n = \min(x_n, x_{n+1}, \dots, x_{n+k-1})$.

1. Montrer que $\forall n \in \mathbb{N}, M_n \geq x_{n+k} \geq m_n$. En déduire que (M_n) est décroissante et que (m_n) est croissante.
2. Montrer que (M_n) et (m_n) sont convergentes. On note L et ℓ leurs limites. Montrer que $L \geq \ell$.
3. Montrer que $\forall n \geq 0, x_{n+k} \geq \frac{M_n + (k-1)m_n}{k}$.
4. On procède par l'absurde pour montrer que $L = \ell$. On suppose que $L > \ell$ et on pose $\varepsilon = L - \ell > 0$.
 - (a) Montrer qu'il existe n_0 tel que $\forall n \geq n_0, m_n \geq \ell - \frac{\varepsilon}{k}$.
 - (b) En déduire que pour $n \geq n_0, x_{n+k} \geq \ell + \frac{\varepsilon}{k} - (k-1)\frac{\varepsilon}{k^2}$, et aboutir à une contradiction.
5. Montrer que (x_n) converge.
6. Pour $n \geq 0$, on pose $y_n = \sum_{j=0}^{k-1} (j+1)x_{n+j}$.
 - (a) Montrer que (y_n) est constante.
 - (b) En déduire que $x_n \xrightarrow{n \rightarrow +\infty} \frac{x_0 + 2x_1 + \dots + kx_{k-1}}{1 + 2 + \dots + k}$.

7. Interprétation matricielle de la récurrence, et calcul de la limite. Pour $n \in \mathbb{N}$, on pose $V_n = \begin{pmatrix} x_n \\ x_{n+1} \\ \vdots \\ x_{n+k-1} \end{pmatrix} \in \mathbb{R}^k$.

- (a) Expliciter une matrice $A \in \mathcal{M}_k(\mathbb{R})$ telle que $\forall n \in \mathbb{N}, V_{n+1} = A V_n$.
- (b) Résoudre l'équation $A^T X = X$, d'inconnue $X \in \mathbb{R}^k$. Expliciter en particulier un vecteur X_\perp à coefficients entiers non nul vérifiant $A^T X_\perp = X_\perp$.
- (c) Montrer que $(X_\perp^T V_n)_{n \in \mathbb{N}}$ est constante.
- (d) En déduire que $x_n \xrightarrow{n \rightarrow +\infty} \frac{x_0 + 2x_1 + \dots + kx_{k-1}}{1 + 2 + \dots + k}$.

Exercice 3. L'objectif est l'étude des ensembles $\mathcal{N}_2 = \{a^2 + b^2, (a, b) \in \mathbb{N}^2\}$ et $\mathcal{N}_4 = \{a^2 + b^2 + c^2 + d^2, (a, b, c, d) \in \mathbb{N}^4\}$.

I. Préliminaires sur \mathcal{N}_2 .

- 1) Montrer que $3 \notin \mathcal{N}_2$, et plus généralement, que si $n \equiv 3[4]$, $n \notin \mathcal{N}_2$.
- 2) En remarquant que les éléments de \mathcal{N}_2 sont exactement les modules au carré de nombres complexes à coefficients entiers, montrer que \mathcal{N}_2 est stable par produit, c'est-à-dire que si $n, m \in \mathcal{N}_2$, alors $nm \in \mathcal{N}_2$.

II. Stabilité par produit de \mathcal{N}_4 . On considère l'ensemble $\mathcal{H} = \left\{ \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}, z_1, z_2 \in \mathbb{C} \right\}$.

- a) Montrer que \mathcal{H} est stable par produit.
- b) Pour $M \in \mathcal{H}$, calculer $\det M$. En utilisant $\det(AB) = \det A \det B$, montrer que \mathcal{N}_4 est stable par produit.

III. Deux théorèmes de géométrie des nombres de Minkowski.

Une partie de $A \subset \mathbb{R}^2$ est dite

- (i) symétrique par rapport à l'origine si $\forall x \in A, -x \in A$.
- (ii) convexe si $\forall u, v \in A, \forall \lambda \in [0, 1], \lambda u + (1 - \lambda)v \in A$ (l'addition est l'addition vectorielle dans \mathbb{R}^2).

Dans la suite, on considère une partie A non vide, convexe, bornée et symétrique par rapport à l'origine.

1) Préliminaires.

- a) Montrer que $(0, 0) \in A$.
- b) Soit $M \in \mathcal{M}_2(\mathbb{R})$, et $m: X \mapsto MX$ l'application linéaire associée. Montrer que $m^{-1}(A)$ est convexe.

2) On suppose que A est d'aire > 4 . On veut montrer que A contient un point de \mathbb{Z}^2 différent de l'origine.

- a) Pour $(i, j) \in \mathbb{Z}^2$, on considère $C_{(i,j)}$ le carré plein de centre $(2i, 2j)$ et de côté de longueur 2.

Justifier brièvement l'existence d'un ensemble fini $K \subset \mathbb{Z}^2$ tel que $A = \bigcup_{(i,j) \in K} (A \cap C_{(i,j)})$.

- b) Pour $(i, j) \in K$, on note $\tilde{C}_{i,j}^A$ l'image de $A \cap C_{(i,j)}$ par la translation de vecteur $(-2i, -2j)$.

En utilisant que $\sum_{(i,j) \in K} \text{Aire}(\tilde{C}_{i,j}^A) > 4$, justifier l'existence de $u_1 \neq u_2 \in A$ tels que $u_1 - u_2$ soit à coordonnées entières paires.

- c) Conclure.

Le résultat reste valable en dimension n , si le volume de A est $> 2^n$, c'est un théorème de Minkowski.

3) Soient $v_1 = \begin{pmatrix} a \\ b \\ c \end{pmatrix}, v_2 = \begin{pmatrix} b \\ c \\ d \end{pmatrix}$ deux vecteurs de \mathbb{R}^3 non colinéaires et $\mathcal{R} = \mathbb{Z}v_1 + \mathbb{Z}v_2$ le réseau engendré par v_1 et v_2 .

On admet que si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, l'application linéaire $m: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ multiplie les aires par $|ad - bc|$, c'est-à-dire que pour toute partie $A \subset \mathbb{R}^2$ admettant une aire, $\text{Aire}(m(A)) = |ad - bc| \text{Aire}(A)$.

- a) On considère $\mathcal{P} = \{x_1v_1 + x_2v_2, (x_1, x_2) \in [0, 1]^2\}$. Représenter \mathcal{P} dans un cas particulier au choix.

Expliciter une application linéaire m telle que $\mathcal{P} = m([0, 1]^2)$. Quelle est l'aire de \mathcal{P} ?

- b) En appliquant III.2), montrer que si $\text{Aire}(A) > 4|ad - bc|$, alors $A \cap \mathcal{R}$ contient au moins deux éléments.

Le résultat s'étend en dimension n , en remplaçant le facteur 4 par 2^n .

IV. On considère un nombre premier p vérifiant $p \equiv 1[4]$, l'objectif est de montrer que $p \in \mathcal{N}_2$.

1) Existence d'une racine de -1 modulo p .

- a) Montrer que $x^2 \equiv 1[p]$ si et seulement si $x \equiv \pm 1[p]$. **Indication :** Si p premier divise ab , alors $p \mid a$ ou $p \mid b$.
- b) En appliquant le théorème de Bézout, justifier que pour tout élément $a \in \llbracket 1, p-1 \rrbracket$, il existe un unique élément $b \in \llbracket 1, p-1 \rrbracket$ tel que $ab \equiv 1[p]$, appelé inverse de a modulo p .
- c) En regroupant chaque facteur avec son inverse dans le produit $(p-1)!$, montrer le théorème de Wilson : $(p-1)! \equiv -1[p]$.
- d) En déduire l'existence de $a \in \mathbb{Z}$ tel que $a^2 + 1 \equiv 0[p]$.

2) On considère le réseau $\mathcal{R} = \mathbb{Z} \begin{pmatrix} p \\ 0 \end{pmatrix} + \mathbb{Z} \begin{pmatrix} a \\ 1 \end{pmatrix}$ et $A = D(O, \sqrt{2p})$, le disque ouvert (sans le bord) de rayon $\sqrt{2p}$ centré en l'origine. En appliquant un théorème de Minkowski, montrer que $p \in \mathcal{N}_2$.

V. On considère un nombre premier p impair.

1) Montrer que pour tout $a \in \llbracket 1, p-1 \rrbracket$, l'équation $x^2 \equiv a[p]$ a ou bien 2, ou bien aucune solution dans $\llbracket 1, p-1 \rrbracket$. En déduire le nombre de $a \in \llbracket 1, p-1 \rrbracket$ qui sont des carrés modulo p .

2) Montrer qu'il existe $x, y \in \llbracket 0, p-1 \rrbracket$ tel que $p \mid x^2 + y^2 + 1$.

Indication : Utiliser la question précédente : est-il possible que $\{x^2[p]\}$ et $\{-y^2 - 1[p]\}$ soient disjoints ?

3) En considérant le réseau de \mathbb{R}^4 engendré par $(p, 0, 0, 0)$, $(0, p, 0, 0)$, $(x, y, 1, 0)$ et $(y, -x, 0, 1)$, dont le volume du parallélépipède fondamental vaut p^2 (le déterminant de la matrice triangulaire supérieure formée des quatre vecteurs), montrer que $p \in \mathcal{N}_4$. On pourra admettre que le volume d'une boule de rayon r dans \mathbb{R}^4 est $\frac{\pi^2 r^4}{2}$.

VI. Conclusion.

1) Montrer le théorème des quatre carrés de Lagrange : $\mathcal{N}_4 = \mathbb{N}$.

2) Soit p premier, avec $p \equiv 3[4]$. En utilisant le théorème de Fermat, montrer que -1 n'est pas un carré modulo p . En déduire que si $p \mid x^2 + y^2$, alors $p \mid x$ et $p \mid y$.

3) En déduire quels sont les p premiers appartenant à \mathcal{N}_2 , puis une description des éléments de \mathcal{N}_2 , en termes de leur décomposition en facteurs premiers.