MATRICES DE HADAMARD

Deux niveaux de difficulté/longueur :

— Piste bleue : partie **1**.

— Piste noire : tout le devoir, mais il faut attendre la fin du chapitre « Groupes, anneaux, corps » pour traiter la partie **2**.

Dans ce devoir, les lettres m et n désignent un entier supérieur à 2. On appelle *matrice de Hadamard d'ordre n*, en mémoire du mathématicien français Jacques Hadamard (1865-1963), toute matrice carrée H de taille n à coefficients dans $\{-1,1\}$ pour laquelle $H^\top H = nI_n$. L'ensemble de ces matrices sera noté $\mathscr{H}_n$.

1 PREMIERS EXEMPLES ET CONJECTURE DE HADAMARD

1) Pour toutes colonnes $X, Y \in \mathscr{M}_{n,1}(\mathbb{R})$, on appelle *produit scalaire de X et Y* le réel $\langle X,Y\rangle = x_1y_1 + \ldots + x_ny_n$ et on dit que X et Y sont *orthogonales* si $\langle X,Y\rangle = 0$.

Montrer que pour toute matrice carrée M de taille n à coefficients dans $\{-1,1\}$, $M \in \mathscr{H}_n$ si et seulement si ses colonnes sont deux à deux orthogonales.

Avec à ce critère, on vérifie facilement à l'œil nu que $\mathscr{H}_4$ contient les matrices $\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$.

2) a) Montrer que pour tout $A \in \mathscr{M}_n(\mathbb{R})$: $\quad \operatorname{tr}\left(A^\top A\right) = 0 \iff A = 0$.

b) En déduire que pour tout $H \in \mathscr{H}_n$: $\quad HH^\top = nI_n$. On pourra s'intéresser à la matrice $A = HH^\top - nI_n$.

c) En déduire que $\mathscr{H}_n$ est inclus dans $\mathrm{GL}_n(\mathbb{R})$ et *stable par transposition*, i.e. que pour tous $M \in \mathscr{H}_n$: $\quad H^\top \in \mathscr{H}_n$.

3) Pour tout $k \in [\![1,n]\!]$, on note D_k la matrice diagonale de taille n dont les coefficients diagonaux valent 1 à l'exception du $k^{\text{ème}}$ qui vaut -1. Attention, D_k dépend de n en dépit de la notation.

a) Soient $M \in \mathscr{M}_n(\mathbb{R})$ et $k \in [\![1,n]\!]$. Quelle opération réalise-t-on sur M quand on calcule MD_k et D_kM ?

b) Montrer que pour tous $H \in \mathscr{H}_n$ et $k \in [\![1,n]\!]$: $\quad HD_k \in \mathscr{H}_n \quad$ et $\quad D_kH \in \mathscr{H}_n$.

4) On appelle *permutation de $[\![1,n]\!]$* toute bijection de $[\![1,n]\!]$ sur lui-même. L'ensemble des permutations de $[\![1,n]\!]$ est appelé le *groupe symétrique de $[\![1,n]\!]$* et noté S_n.

Pour tout $\sigma \in S_n$, on note P_σ la matrice $\left(\delta_{i\sigma(j)}\right)_{1\leqslant i,j\leqslant n}$ où $\delta_{ab} = \begin{cases} 1 & \text{si } a = b \\ 0 & \text{sinon} \end{cases}$ pour tous $a, b \in \mathbb{R}$.

a) Montrer que P_σ est inversible d'inverse $P_\sigma^\top = P_{\sigma^{-1}}$ pour tout $\sigma \in S_n$.

b) Soient $M \in \mathscr{M}_n(\mathbb{R})$ et $\sigma \in S_n$. Quelle opération sur M réalise-t-on quand on calcule MP_σ et $P_\sigma M$?

c) Montrer que pour tous $H \in \mathscr{H}_n$ et $\sigma \in S_n$: $\quad HP_\sigma \in \mathscr{H}_n \quad$ et $\quad P_\sigma H \in \mathscr{H}_n$.

5) Pour tous $H, H' \in \mathscr{H}_n$, on dit que H' est *Hadamard-équivalente à H*, ce qu'on note $H \sim_{\mathscr{H}_n} H'$, si on peut passer de H à H' par une série de multiplications à gauche et à droite par des matrices D_k et P_σ — éventuellement aucune. On ADMET pour simplifier que $\sim_{\mathscr{H}_n}$ est une relation d'équivalence sur $\mathscr{H}_n$.

a) Montrer que toute matrice $H \in \mathscr{H}_n$ est Hadamard-équivalente à une matrice $H' \in \mathscr{H}_n$ dont les coefficients des première ligne et colonne valent tous 1. Une telle matrice H' est appelée une *forme normalisée de H*.

b) En déduire que toute matrice de Hadamard d'ordre 2 est Hadamard-équivalente à la matrice $W = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

c) Montrer qu'il n'existe pas de matrice de Hadamard d'ordre 3.

6) Pour tous $A \in \mathscr{M}_m(\mathbb{R})$ et $B \in \mathscr{M}_n(\mathbb{R})$, on appelle *produit de Kronecker de A par B* la matrice carrée de taille mn définie par blocs de la façon suivante : $\quad A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix}$.

a) Montrer que pour tous $A, A' \in \mathscr{M}_m(\mathbb{R})$ et $B, B' \in \mathscr{M}_n(\mathbb{R})$:

$$\left(A \otimes B\right)^\top = A^\top \otimes B^\top \qquad \text{et} \qquad \left(A \otimes B\right)\left(A' \otimes B'\right) = (AA') \otimes (BB').$$

b) En déduire que pour tous $H \in \mathscr{H}_m$ et $H' \in \mathscr{H}_n$: $\quad H \otimes H' \in \mathscr{H}_{mn}$.

c) Montrer que toute matrice de Hadamard d'ordre 4 est Hadamard-équivalente à $W \otimes W$.

7) Soit $H \in \mathscr{H}_n$ avec $n \geqslant 4$.

a) Montrer que H est Hadamard-équivalente à une matrice de la forme suivante :

$$\begin{pmatrix} 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & 1 & 1 & \end{pmatrix} \left.\vphantom{\begin{pmatrix} a \\ a \\ a \end{pmatrix}}\right\} a \text{ lignes}$$
$$\begin{pmatrix} 1 & 1 & -1 & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & 1 & -1 & \end{pmatrix} \left.\vphantom{\begin{pmatrix} a \\ a \\ a \end{pmatrix}}\right\} b \text{ lignes}$$
$$\begin{pmatrix} 1 & -1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & -1 & 1 & \end{pmatrix} \left.\vphantom{\begin{pmatrix} a \\ a \\ a \end{pmatrix}}\right\} c \text{ lignes}$$
$$\begin{pmatrix} 1 & -1 & -1 & \cdots \\ \vdots & \vdots & \vdots & \\ 1 & -1 & -1 & \end{pmatrix} \left.\vphantom{\begin{pmatrix} a \\ a \\ a \end{pmatrix}}\right\} d \text{ lignes}$$

b) En déduire que n est divisible par 4.

En résumé, il ne peut exister de matrice de Hadamard d'ordre $n \geqslant 4$ que si n est divisible par 4. Énoncée en 1893, la *conjecture de Hadamard* stipule que la réciproque est vraie, i.e. qu'il existe une matrice de Hadamard d'ordre n pour tout $n \geqslant 4$ divisible par 4. Le plus petit multiple de 4 dont on ignore aujourd'hui s'il est l'ordre d'une matrice de Hadamard est 668.

Si on pose $\mathscr{O} = \left\{n \geqslant 2 \mid \quad \mathscr{H}_n \neq \varnothing\right\}$, on a réussi à montrer que $\mathscr{O} \subset \{2\} \sqcup 4\mathbb{N}^*$, mais aussi que $\mathscr{O}$ est *stable par produit* d'après **6)b)**, i.e. que $mn \in \mathscr{O}$ pour tous $m, n \in \mathscr{O}$.

2 Construction de Paley

Cette partie est consacrée à un procédé de construction de matrices de Hadamard découvert en 1933 par le mathématicien anglais Raymond Paley (1907-1933). On se donne une fois pour toutes un nombre premier impair p. On note $\mathbb{F}_p$ le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, $\mathbb{F}_p^*$ son groupe des inversibles $\mathbb{F}_p \setminus \{\overline{0}\}$, et pour tout $k \in \mathbb{Z}$, $\overline{k}$ la classe de k dans $\mathbb{F}_p$.

On pose ensuite $\mathscr{C} = \left\{x^2 \mid \quad x \in \mathbb{F}_p^*\right\}$ et on définit une application χ de $\mathbb{F}_p$ dans $\mathbb{R}$ en posant pour tout $x \in \mathbb{F}_p$:

$$\chi(x) = \begin{cases} 0 & \text{si } x = \overline{0} \\ 1 & \text{si } x \text{ est un carré non nul dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases}$$

On rappelle enfin que d'après le *théorème de Wilson* : $\quad \overline{(p-1)!} = -\overline{1}$.

8) On note φ l'application $x \longmapsto x^2$ de $\mathbb{F}_p^*$ dans lui-même.

a) Montrer que pour tout $y \in \mathbb{F}_p^*$: $\quad \left|\varphi^{-1}\left(\{y\}\right)\right| \in \{0, 2\}$.

b) En déduire que $|\mathscr{C}| = \left|\mathbb{F}_p^* \setminus \mathscr{C}\right| = \dfrac{p-1}{2}$. Que vaut $\displaystyle\sum_{x \in \mathbb{F}_p} \chi(x)$?

c) Montrer que l'application $x \longmapsto xy$ est bijective de $\mathscr{C}$ sur $\mathbb{F}_p^* \setminus \mathscr{C}$ pour tout $y \in \mathbb{F}_p^* \setminus \mathscr{C}$.

d) En déduire que pour tous $x, y \in \mathbb{F}_p^* \setminus \mathscr{C}$: $\quad xy \in \mathscr{C}$, $\quad$ puis que pour tous $x, y \in \mathbb{F}_p$: $\quad \chi(xy) = \chi(x)\chi(y)$.

e) Montrer que si $-\overline{1} \notin \mathscr{C}$: $\quad \overline{(p-1)!} = \displaystyle\prod_{x \in \mathscr{C}} x \prod_{x \in \mathscr{C}} \left(-x^{-1}\right)$. $\quad$ En déduire qu'en toute généralité : $\quad \chi\left(-\overline{1}\right) = (-1)^{\frac{p-1}{2}}$.

9) **a)** Montrer que pour tous $x, y \in \mathbb{F}_p^*$: $\quad \chi(x)\chi(x+y) = \chi\left(x^{-1}y + \overline{1}\right)$.

b) En déduire que pour tout $y \in \mathbb{F}_p^*$: $\quad \displaystyle\sum_{x \in \mathbb{F}_p} \chi(x)\chi(x+y) = -1$.

10) On note à présent S la matrice $\left(\chi\left(\overline{i-j}\right)\right)_{1 \leqslant i,j \leqslant p}$, J la matrice carrée de taille p dont tous les coefficients valent 1 et U la matrice colonne de taille p dont tous les coefficients valent 1.

a) Montrer que : $\quad S^\top = (-1)^{\frac{p-1}{2}} S$, $\quad SU = U^\top S = 0 \quad$ et $\quad S^\top S = p\, I_p - J$.

b) Montrer que si $p \equiv 3\ [4]$, alors $\begin{pmatrix} 1 & U^\top \\ U & S - I_p \end{pmatrix} \in \mathscr{H}_{p+1}$.

Un calcul analogue montre que si $p \equiv 1[4]$, alors $\begin{pmatrix} T + I_p & T - I_p \\ T - I_p & -T - I_p \end{pmatrix} \in \mathscr{H}_{2(p+1)}$ où $T = \begin{pmatrix} 0 & U^\top \\ U & S \end{pmatrix}$.

11) À l'issue de ce travail, quel est le plus petit multiple de 4 dont on n'a pas montré qu'il appartient à $\mathscr{O}$?