DM 06 : matrices [corrigé]

Exercice 1

Soit $\rho = 3 + \sqrt{5}$.

Le but de cet exercice est de déterminer les trois derniers chiffres avant la virgule de ρ^N, pour un nombre N quelconque (mais gigantesque).

Introduisons quelques notations :

- Pour tout $x \in \mathbb{R}$, on note $\lfloor x \rfloor$ la *partie entière (inférieure)* de x, c'est-à-dire le plus grand entier $\leqslant x$. Par exemple, on a $5 \leqslant \rho < 6$, donc $\lfloor \rho \rfloor = 5$.
- On note $m : \mathbb{Z} \to [\![0, 999]\!]$ l'application telle que, pour tout $n \in \mathbb{Z}$, $m(n)$ soit le reste de n dans la division euclidienne par 1000.

Le but de l'exercice est ainsi de déterminer, pour tout $N \in \mathbb{N}$, l'entier $r_N = m\big(\lfloor \rho^N \rfloor\big)$.

1. En utilisant le cours, montrer que la suite $(u_n)_{n\in\mathbb{N}} = \Big((3+\sqrt{5})^n + (3-\sqrt{5})^n\Big)_{n\in\mathbb{N}}$ vérifie une relation de récurrence $\forall n \in \mathbb{N}, u_{n+2} + \alpha u_{n+1} + \beta u_n = 0$, où α et β sont deux réels que l'on déterminera.

   On voit que $(u_n)_{n\in\mathbb{N}}$ a la forme des suites récurrentes linéaires d'ordre 2 vérifiant une relation de récurrence dont le polynôme caractéristique aurait $3 \pm \sqrt{5}$ comme racines.
   D'après les relations de Viète, ce polynôme devrait être $X^2 - 6X + 4$.
   On vérifie alors que $(u_n)_{n\in\mathbb{N}}$ est bien la suite récurrente linéaire vérifiant

   $$u_0 = 2, \qquad u_1 = 6 \qquad \textit{et} \qquad \forall n \in \mathbb{N}, u_{n+2} - 6u_{n+1} + 4u_n = 0.$$

2. En déduire que la suite $(u_n)_{n\in\mathbb{N}}$ est à valeurs entières.

   C'est une récurrence (double) immédiate.

3. Montrer $\forall n \in \mathbb{N}^*, \lfloor \rho^n \rfloor = u_n - 1$.

   On a $4 < 5 < 9$, donc $2 < \sqrt{5} < 3$ par stricte croissance de $\sqrt{\cdot}$, puis $0 < 3 - \sqrt{5} < 1$.
   Soit $n \in \mathbb{N}^*$. On a donc $(3-\sqrt{5})^n - 1 < 0$, donc

   $$(3+\sqrt{5})^n + (3-\sqrt{5})^n - 1 < (3+\sqrt{5})^n < (3+\sqrt{5})^n + (3-\sqrt{5})^n,$$

   c'est-à-dire $u_n - 1 < \rho^n < u_n$.
   La question précédente montrant que $u_n - 1$ est un entier, on en déduit $u_n - 1 = \lfloor \rho^n \rfloor$.

4. En utilisant ce qui précède, montrer qu'il existe deux entiers $n_0 \in \mathbb{N}$ et $T \in [\![1, 10^6]\!]$ tels que la suite $(r_n)_{n\in\mathbb{N}}$ soit T-périodique à partir du rang n_0, c'est-à-dire que $\forall n \geqslant n_0, r_{n+T} = r_n$.

   On va en fait montrer que la suite $\big(m(u_n)\big)_{n\in\mathbb{N}}$ possède la propriété demandée par l'énoncé. Cela conclura immédiatement car la question précédente montre que, pour tout $n \in \mathbb{N}^*$, on a $\lfloor \rho^n \rfloor = u_n - 1$, donc

   $$r_n = m\left(\lfloor \rho^n \rfloor\right) = \begin{cases} m(u_n) - 1 & \textit{si } m(u_n) > 0 \\ 999 & \textit{si } m(u_n) = 0. \end{cases}$$

Quand on aura trouvé $n_0 \in \mathbb{N}$ et $T \in [\![1, 10^6]\!]$ tels que que $(m(u_n))_{n\in\mathbb{N}}$ est T-périodique à partir du rang n_0, on en déduira donc que $(r_n)_{n\in\mathbb{N}}$ est T-périodique à partir du rang $\max(n_0, 1)$.
Or, puisque la suite $(u_n)_{n\in\mathbb{N}}$ vérifie $u_0 = 2$, $u_1 = 6$ et $\forall n \in \mathbb{N}, u_{n+2} = 6u_{n+1} - 4u_n$, la suite $(v_n)_{n\in\mathbb{N}} = (m(u_n))_{n\in\mathbb{N}}$ est à valeurs dans $[\![0, 999]\!]$ vérifie

$$v_0 = 2, \qquad v_1 = 6 \qquad \text{et} \qquad \forall n \in \mathbb{N}, v_{n+2} = m\left(6v_{n+1} - 4v_n\right). \tag{$\star$}$$

L'application

$$\varphi : \begin{cases} \mathbb{N} \to & [\![0, 999]\!]^2 \\ n \mapsto (v_n, v_{n+1}) \end{cases}$$

possède un domaine infini et un codomaine fini. D'après le principe des tiroirs, elle ne peut pas être injective. Mieux : sa restriction à $[\![0, 10^6]\!]$ (qui possède $10^6 + 1$ éléments, soit un de plus que $[\![0, 999]\!]^2$) ne peut pas non plus être injective.
On peut donc trouver $0 \leqslant n_0 < n_1 \leqslant 10^6$ tels que $\varphi(n_0) = \varphi(n_1)$. En posant $T = n_1 - n_0 \in [\![1, 10^6]\!]$, on a donc $\varphi(n_0 + T) = \varphi(n_0)$, c'est-à-dire $(v_{n_0}, v_{n_0+1}) = (v_{n_0+T}, v_{n_0+1+T})$.
Pour tout $n \geqslant n_0$, on note alors $P(n)$ l'assertion $v_{n+T} = v_n$. Montrons $\forall n \geqslant n_0, P(n)$ par récurrence double.
Initialisation. *Ce qui précède montre $v_{n_0+T} = v_{n_0}$ et $v_{n_0+1+T} = v_{n_0}$, c'est-à-dire $P(n_0)$ et $P(n_0 + 1)$.*
Hérédité. *Soit $n \geqslant n_0$ tel que $P(n)$ et $P(n + 1)$. On a donc*

$$\begin{aligned} v_{n+2+T} &= m\left(6v_{n+1+T} - 4v_{n+T}\right) && \text{(d'après } (\star)\text{)} \\ &= m\left(6v_{n+1} - 4v_n\right) && \text{(d'après } P(n) \text{ et } P(n+1)\text{)} \\ &= v_{n+2}, && \text{(d'après } (\star)\text{)} \end{aligned}$$

ce qui montre $P(n + 2)$ et clôt la récurrence.

5. À l'aide d'un ordinateur, trouver effectivement deux entiers n_0 et T qui conviennent.

Les premières valeurs de $(v_n)_{n\in\mathbb{N}}$ se calculent très efficacement par la relation de récurrence ($\star$), en n'oubliant pas de bel et bien travailler modulo 1000, pour éviter tout un tas de problèmes liés à la manipulation de très grands entiers.
On obtient notamment les premières valeurs suivantes pour $(v_n)_{n\in\mathbb{N}}$.

	0	1	2	3	4	5	6	7	8	9
	2	6	28	**144**	**752**	936	608	904	992	336
1_	48	944	472	56	448	464	992	96	608	264
2_	152	856	528	744	352	136	408	904	792	136
3_	648	344	472	456	848	264	192	96	808	464
4_	552	456	528	344	952	336	208	904	592	936
5_	248	744	472	856	248	64	392	96	8	664
6_	952	56	528	944	552	536	8	904	392	736
7_	848	144	472	256	648	864	592	96	208	864
8_	352	656	528	544	152	736	808	904	192	536
9_	448	544	472	656	48	664	792	96	408	64
10_	752	256	528	**144**	**752**	936	608	904	992	$\cdots$

Cela montre que $n_0 = 3$ et $T = 100$ conviennent, pour $(v_n)_{n\in\mathbb{N}}$ et donc pour $(r_n)_{n\in\mathbb{N}}$ comme expliqué plus haut.

6. Calculer r_N, pour $N = 10^{10^{10}}$.

Puisque N est un multiple de 100, on a $r_N = r_{100} = v_{100} - 1$ (attention à ne pas prendre v_0, qui tombe avant que la suite ne soit devenue périodique).

Ainsi, les trois derniers chiffres avant la virgule de $(3 + \sqrt{5})^{10^{10^{10}}}$ sont 751.

Exercice 2

Soit $n \geqslant 2$ un entier et $M \in M_n(\mathbb{R})$ une matrice telle que $\forall P \in GL_n(\mathbb{R}), PM \in S_n(\mathbb{R})$.

Montrer que M est la matrice nulle.

- *On montre d'abord que* M *est symétrique.*
  Soit $i \neq j$ *deux éléments de* $M_n(\mathbb{R})$. *On a alors*
  - $I_n \in GL_n(\mathbb{R})$, *donc* $I_n M = M \in S_n(\mathbb{R})$, *donc* $[M]_{i,j} = [M]_{j,i}$ *;*
  - $D_i(2) \in GL_n(\mathbb{R})$, *donc* $D_i(2)M \in S_n(\mathbb{R})$, *donc* $2[M]_{i,j} = [D_i(2)M]_{i,j} = [M]_{j,i}$.

  En comparant ces deux calculs, il vient $2[M]_{i,j} = [M]_{j,i}$, *d'où* $[M]_{i,j} = 0$, *ce qui conclut.*
- *Montrons maintenant* M *nulle.*
  Soit $i \in [\![1, n]\!]$. *Fixons un entier* $k \in [\![1, n]\!] \setminus \{i\}$ *et notons* $T = T_{k,i}(1)$ *la matrice de transvection de l'opération* $L_k \leftarrow L_k + L_i$.
  Pour tout $P \in GL_n(\mathbb{R})$, *la matrice* PT *est inversible. On a donc* $\forall P \in GL_n(\mathbb{R}), PTM \in S_n(\mathbb{R})$ *et le premier point de la démonstration (appliqué à* TM*) montre que* TM *est diagonale.*
  En particulier, $0 = [TM]_{k,i} = [M]_{k,i} + [M]_{i,i} = [M]_{i,i}$, *ce qui conclut.*

Exercice 3

Soit $A \in M_2(\mathbb{R})$ tel que $\det(A^2 - A + I_2) = 0$.

1. Montrer que $A^2 - A + I_2 = 0_2$.

   Notons $\zeta = \zeta_6 = \exp\left(i\dfrac{2\pi}{6}\right)$. *Les racines du polynôme complexe* $X^2 - X + 1$ *sont* ζ *et* $\overline{\zeta}$.

   - *On va commencer par montrer que* $\mathrm{Sp}_{\mathbb{C}}(A) = \{\zeta, \overline{\zeta}\}$.
     - *Montrons l'inclusion directe. Soit* $\lambda \in \mathrm{Sp}_{\mathbb{C}}(A)$. *On peut donc trouver* $X \in \mathbb{C}^2$ *non nul tel que* $AX = \lambda X$.
       On en déduit $A^2X = \lambda^2 X$, *puis* $0_{\mathbb{C}^2} = (A^2 - A + I_2)X = (\lambda^2 - \lambda + 1)X$.
       Comme $X \neq 0_{\mathbb{C}^2}$, *on en déduit* $\lambda^2 - \lambda + 1 = 0$, *et donc* $\lambda \in \{\zeta, \overline{\zeta}\}$.
     - *L'inclusion précédente montre notamment que le polynôme* $\chi_A = X^2 - \mathrm{tr}(A)X + \det(A)$ *(réel, du second degré) ne possède pas de racine réelle. Il possède donc deux racines complexes, qui doivent ainsi être* ζ *et* $\overline{\zeta}$.

     On a ainsi $\mathrm{Sp}_{\mathbb{C}}(A) = \{\zeta, \overline{\zeta}\}$.
   - *D'après les formules de Viète, on en déduit* $\mathrm{tr}(A) = \det(A) = 1$. *Le théorème de Cayley-Hamilton entraîne alors que* $A^2 - A + I_2 = 0_2$.

2. Soit $\alpha, \beta \in \mathbb{R}$. Calculer $\det(A^2 + \alpha A + \beta I_2)$.

   On a montré à la question précédente que $\chi_A = X^2 - X + 1$, *donc* A *est semblable (sur* $\mathbb{C}$*) à* $\mathrm{diag}(\zeta, \overline{\zeta})$.
   On peut donc trouver $P \in GL_2(\mathbb{C})$ *tel que* $A = P\,\mathrm{diag}(\zeta, \overline{\zeta})P^{-1}$. *On en déduit que*

   $$\begin{aligned} A^2 + \alpha A + \beta I_2 &= P\,\mathrm{diag}(\zeta^2, \overline{\zeta}^2)P^{-1} + P\alpha\ \mathrm{diag}(\zeta, \overline{\zeta})P^{-1} + \beta I_2 \\ &= P\,\mathrm{diag}(\zeta^2 + \alpha\zeta + \beta, \overline{\zeta}^2 + \alpha\overline{\zeta} + \beta)P^{-1}. \end{aligned}$$

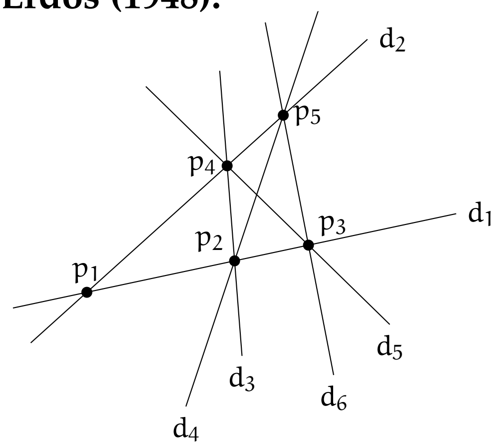
   Par invariance du déterminant par similitude, on en déduit

   $$\begin{aligned} \det\left(A^2 + \alpha A + \beta I_2\right) &= \det\left(\mathrm{diag}(\zeta^2 + \alpha\zeta + \beta, \overline{\zeta}^2 + \alpha\overline{\zeta} + \beta)\right) \\ &= (\zeta^2 + \alpha\zeta + \beta)(\overline{\zeta}^2 + \alpha\overline{\zeta} + \beta) \\ &= 1 + \alpha\zeta + \beta\zeta^2 + \alpha\overline{\zeta} + \alpha^2 + a\beta\zeta + \beta\overline{\zeta}^2 + \alpha\beta\overline{\zeta} + \beta^2 \end{aligned}$$

$$= \alpha^2 + \beta^2 + \alpha\beta(\zeta + \overline{\zeta}) + \alpha(\zeta + \overline{\zeta}) + \beta(j + \overline{j}) + 1$$
$$= \alpha^2 + \beta^2 + \alpha\beta + \alpha - \beta + 1.$$

Problème. Théorème de De Bruijn-Erdős (1948).

Partie I. Présentation du problème.



Dans tout le problème, on fixe un entier $n \geqslant 3$.

On se donne n points distincts $p_1, \ldots, p_n$ dans le plan, qui ne sont pas tous alignés.

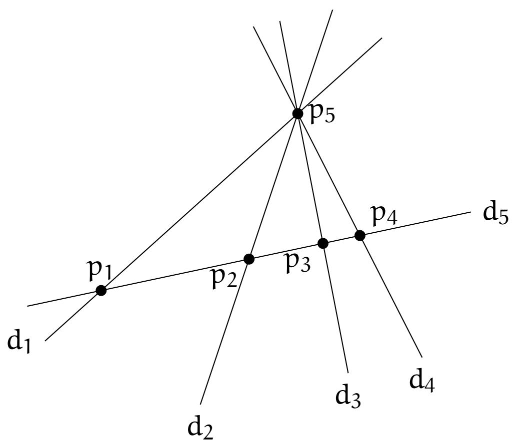
On trace alors toutes les droites reliant au moins deux de ces points, et on les numérote $d_1, \ldots, d_k$, pour un certain entier $k \geqslant 1$.

La figure ci-contre montre un exemple où $n = 5$ et $k = 6$.

> Le but du problème est de montrer que si les n points ne sont pas tous alignés, alors $k \geqslant n$.

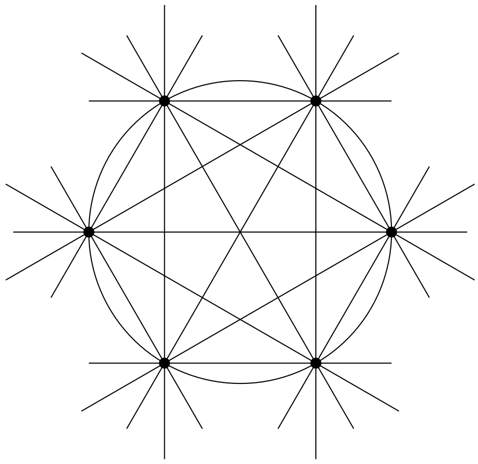
1. Donner un exemple où $k = n$. (Rappel : $n \geqslant 3$ est fixé, vous ne pouvez pas le choisir).

   Il suffit de prendre $n - 1$ points $p_1, \ldots, p_{n-1}$ sur une même droite d_n et un point en dehors de la droite formée par les autres. Il y a ainsi exactement n droites : d_n et, pour tout $i \in [\![1, n-1]\!]$, $d_i = (p_i\ p_n)$.



2. Donner, en fonction de n, la valeur maximale de k.

   - *Toute droite d_j (pour $j \in [\![1, k]\!]$) est de la forme $d_j = (p_{i_0}\ p_{i_1})$, pour un certain choix d'indices $i_0 < i_1$ dans $[\![1, n]\!]$.*
     Ainsi, il y a moins de droites que de paires $\{i_0, i_1\}$ d'entiers différents.
     Ainsi, $k\binom{n}{2}$.
   - *On peut effectivement avoir $k = \binom{n}{2}$ en prenant des points tels que trois d'entre eux ne sont jamais alignés. C'est par exemple le cas si les points sont tous sur un même cercle.*



$n = 6$ *points,* $k = \binom{6}{2} = 15$ *droites.*

3. Pour tout $i \in [\![1, n]\!]$, on note r_i le nombre de droites passant par p_i.
(Dans l'exemple plus haut, par exemple, $r_1 = 2$ et $\forall i \in [\![2, 5]\!], r_i = 3$.)
Traduire sur les nombres $r_1, \ldots, r_n$ l'hypothèse selon laquelle les points ne sont pas tous alignés.

   Dire que les points ne sont pas tous alignés signifie que par chaque point, passent plusieurs droites, c'est-à-dire que $\forall i \in [\![1, n]\!], r_i \geqslant 2$.

Partie II. Deux lemmes matriciels.

Le but de cette partie est de montrer les deux résultats suivants.

Lemme A. Soit $M \in \mathcal{M}_n(\mathbb{R})$ tel que $\forall X \in \mathbb{R}^n, X^T M X = 0 \Rightarrow X = 0_{\mathbb{R}^n}$. Alors $M \in GL_n(\mathbb{R})$.

Lemme B. Soit $k \geqslant 1$ et $(A, B) \in \mathcal{M}_{n,k}(\mathbb{R}) \times \mathcal{M}_{k,n}(\mathbb{R})$ tels que $AB \in GL_n(\mathbb{R})$. Alors $k \geqslant n$.

4. Démontrer le lemme A.

   Soit $X \in \ker(M)$. *On a donc* $MX = 0_{\mathbb{R}^n}$, *donc* $X^T M X = 0_{\mathbb{R}^n}$. *Par hypothèse,* $X = 0_{\mathbb{R}^n}$.
   On a ainsi montré $\ker(M) = \{0_{\mathbb{R}^n}\}$, *donc* $M \in GL_n(\mathbb{R})$ *en vertu du critère nucléaire d'inversibilité.*

5. (a) Soit $k \geqslant 1$ et $M \in \mathcal{M}_{k,n}(\mathbb{R})$. On suppose que l'une des colonnes de M est combinaison linéaire des colonnes précédentes, *i.e.* qu'il existe $j_0 \in [\![1, n]\!]$ et $\lambda_1, \ldots, \lambda_{j_0 - 1} \in \mathbb{R}$ tels que

$$C_{j_0}(M) = \sum_{j=1}^{j_0 - 1} \lambda_j \, C_j(M).$$

   Montrer qu'il existe alors $X \in \mathbb{R}^n$ non nul tel que $MX = 0_{\mathbb{R}^k}$.

   Soit $j_0 \in [\![1, n]\!]$ *et* $\lambda_1, \ldots, \lambda_{j_0-1} \in \mathbb{R}$ *tels que* $C_{j_0}(M) = \sum_{j=1}^{j_0-1} \lambda_j \, C_j(M)$.
   On peut réécrire cette égalité sous la forme

$$M\, e_{j_0} = \sum_{j=1}^{j_0-1} \lambda_j \, M\, e_j \qquad \textit{c'est-à-dire} \qquad M \left(e_{j_0} - \sum_{j=1}^{j_0-1} \lambda_j \, e_j \right) = 0_{\mathbb{R}^k},$$

   et le vecteur $X = e_{j_0} - \sum_{j=1}^{j_0-1} \lambda_j \, e_j$ *est bien un élément non nul (sa* j_0*-ième coordonnée vaut* 1*) du noyau de* M.

(b) Soit $1 \leqslant k < n$ et $M \in \mathrm{M}_{k,n}(\mathbb{R})$ une matrice échelonnée réduite.
Montrer qu'il existe $X \in \mathbb{R}^n$ non nul tel que $MX = 0_{\mathbb{R}^k}$.

La matrice M *a au plus* $k < n$ *pivots, donc il existe une colonne sans pivot.*
Soit $j_0 \in [\![1, n]\!]$ *le plus petit indice de colonne tel que* $C_{j_0}(M)$ *n'ait pas de pivot.*
En particulier, $C_1(M), \dots, C_{j_0-1}(M)$ *ont un pivot, donc* $C_1(M) = f_1, \dots, C_{j_0-1}(M) = f_{j_0-1}$*, où l'on a noté* $f_1, \dots, f_k$ *les éléments de la base canonique de* $\mathbb{R}^k$*.*
Comme $C_{j_0}(M)$ *n'a pas de pivot, elle est nécessairement de la forme*

$$C_{j_0}(M) = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_{j_0-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \sum_{j=1}^{j_0-1} \lambda_j f_k = \sum_{j=1}^{j_0-1} \lambda_j C_j(M).$$

Autrement dit, $C_{j_0}(M)$ *est combinaison linéaire des colonnes précédentes, et la question précédente conclut.*

(c) Démontrer le lemme B.

Supposons par l'absurde $k < n$*.*
On peut trouver une suite d'opérations élémentaires transformant B *en une matrice échelonnée réduite. En faisant le produit des matrices d'opérations élémentaires correspondantes, on trouve* $P \in \mathrm{GL}_n(\mathbb{R})$ *tel que* $PB \in \mathrm{M}_{n,k}(\mathbb{R})$ *soit échelonnée réduite.*
D'après la question précédente, on peut trouver $X \in \mathbb{R}^n$ *non nul tel que* $(PB)X = 0_{\mathbb{R}^k}$*.*
En multipliant à gauche par P^{-1}*, on obtient* $BX = 0_{\mathbb{R}^k}$*, puis* $X = I_n X = 0_{\mathbb{R}^n}$ *en multipliant à gauche par* $A \in \mathrm{M}_{n,k}(\mathbb{R})$*.*
Cela fournit une contradiction, donc on avait bien $n \geqslant k$*.*

Partie III. Conclusion.

6. Soit $a, r_1, r_2, \dots, r_n$ des nombres réels tels que $a \geqslant 0$ et $\forall i \in [\![1, n]\!], r_i > a$.

Montrer que $M = \begin{pmatrix} r_1 & & & (a) \\ & r_2 & & \\ & & \ddots & \\ (a) & & & r_n \end{pmatrix}$ est inversible. (Tous les coefficients hors diagonale valent a).

Soit $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *tel que* $X^T M X = 0$*.*
La matrice $X^T M X$ *est de taille* 1×1*, et son unique élément est*

$$\begin{aligned} [X^T M X]_{1,1} &= \sum_{1 \leqslant k, \ell \leqslant n} [X^T]_{1,k} [M]_{k,\ell} [X]_{\ell,1} \\ &= \sum_{1 \leqslant k, \ell \leqslant n} [M]_{k,\ell}\, x_k\, x_\ell. \end{aligned}$$

En notant $J \in \mathrm{M}_n(\mathbb{R})$ *la* all-ones matrix*, on a* $M = a\,J + \mathrm{diag}(r_1 - a, \dots, r_n - a)$*, ce qui permet de continuer le calcul de façon rapide :*

$$[X^T M X]_{1,1} = \sum_{1 \leqslant k, \ell \leqslant n} [M]_{k,\ell}\, x_k\, x_\ell$$

$$
\begin{aligned}
&= \sum_{1\leqslant k,\ell\leqslant n} a\, x_k\, x_\ell + \sum_{i=1}^{n} (r_i - a) x_i^2 \\
&= a\left(\sum_{k=1}^{n} x_k\right)^2 + \sum_{i=1}^{n} (r_i - a) x_i^2.
\end{aligned}
$$

En particulier, comme $a \geqslant 0$, on a

$$
[X^T M X]_{1,1} \geqslant \sum_{i=1}^{n} \underbrace{(r_i - a)}_{>0} x_i^2.
$$

Puisque cette somme est nulle et que ses termes sont positifs, chacun d'entre eux doit être nul, ce qui donne $x_1 = \cdots = x_n = 0$, c'est-à-dire $X = 0_{\mathbb{R}^n}$.
Le lemme A montre alors que la matrice M est inversible.

7. Soit $A \in M_{n,k}(\mathbb{R})$ la matrice telle que, pour tout $i \in [\![1, n]\!]$ et tout $j \in [\![1, k]\!]$, le coefficient $[A]_{i,j}$ vaut 1 si le point p_i est sur la droite d_j, et 0 sinon. Calculer $A\,A^T$.

   Soit $i, j \in [\![1, n]\!]$. On a

$$
\begin{aligned}
[A\,A^T]_{i,j} &= \sum_{k=1}^{n} [A]_{i,k}\, [A^T]_{k,j} \\
&= \sum_{k=1}^{n} [A]_{i,k}\, [A^T]_{j,k} \\
&= \sum_{k=1}^{n} \mathbb{1}_{(p_i \in d_k)}\, \mathbb{1}_{(p_j \in d_k)} \\
&= \sum_{k=1}^{n} \mathbb{1}_{(p_i \in d_k \textit{ et } p_j \in d_k)}.
\end{aligned}
$$

   Autrement dit, $[A\,A^T]_{i,j}$ est le nombre de droites d_k passant à la fois par p_i et p_j.
   - *Si $i \neq j$, il y a une unique telle droite, à savoir la droite $(p_i\, p_j)$.*
   - *Si $i = j$, on compte les droites passant par p_i, et la réponse est le nombre entier d_i, par définition de celui-ci.*

   In fine, $A\,A^T = \begin{pmatrix} r_1 & & (a) \\ & r_2 & \\ & & \ddots & \\ (a) & & & r_n \end{pmatrix} \in M_n(\mathbb{R})$.

8. Conclure.

   D'après les deux dernières questions, $A\,A^T$ est inversible.
   D'après le lemme B, on en déduit $k \geqslant n$, et donc le théorème de De Bruijn-Erdős.