MPI** - Lycée Colbert

Concours Blanc 2025
Mathématiques 2

Jeudi 18 décembre 2025
8h00-12h00

Sujet X-ENS (maths A)

Durée : 4 heures

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve

Le but de ce problème est d'étudier certains aspects de la diagonalisabilité des matrices symétriques à coefficients rationnels. Ces matrices sont diagonalisables dans $\mathbb{R}$, mais il se trouve que leurs valeurs propres ne peuvent pas prendre n'importe quelle valeur réelle. Le principal objectif de ce problème est de caractériser les nombres réels qui apparaissent comme valeurs propres de matrices symétriques à coefficients rationnels.

Notations

Dans tout le problème, si n et m sont des entiers naturels non nuls et K est un corps,
- on note $M_{m,n}(K)$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans K ainsi que $M_n(K) = M_{n,n}(K)$ l'ensemble des matrices carrées de taille n à coefficients dans K ;
- on identifie l'espace vectoriel K^n à l'espace vectoriel des vecteurs colonnes $M_{n,1}(K)$;
- on note $S_n(K)$ l'ensemble des matrices symétriques carrées de taille n à coefficients dans K ;
- si $A \in M_{m,n}(K)$, on note A^T la matrice transposée de A et, si $m = n$,

$$\chi_A(X) = \det(XI_n - A)$$

son polynôme caractéristique, qui est donc un polynôme unitaire ;
- si $q_1, \dots, q_n$ sont des éléments de K, on note $\mathrm{Diag}(q_1, \dots, q_n)$ la matrice diagonale de taille n de coefficients diagonaux $q_1, \dots, q_n$.

Première partie

1. Exhiber une matrice $M \in S_2(\mathbb{Q})$ dont $\sqrt{2}$ est valeur propre.

2. Le but de cette question est de montrer que $\sqrt{3}$ n'est pas valeur propre d'une matrice de $S_2(\mathbb{Q})$. On suppose qu'il existe $M \in S_2(\mathbb{Q})$ telle que $\sqrt{3}$ est valeur propre de M.

2a. En utilisant l'irrationnalité de $\sqrt{3}$, montrer que le polynôme caractéristique de M est $X^2 - 3$.

2b. Montrer que si $n \in \mathbb{Z}$, alors n^2 est congru à 0 ou 1 modulo 3.

2c. Montrer qu'il n'existe pas de triplet d'entiers (x, y, z) premiers entre eux dans leur ensemble tel que $x^2 + y^2 = 3z^2$.

2d. Conclure.

3a. On se donne $q \in \mathbb{Q}$, $n \in \mathbb{N}^\star$ et une matrice $A \in S_n(\mathbb{Q})$ telle que $A^2 = qI_n$. Construire une matrice $B \in S_{2n}(\mathbb{Q})$ commutant à la matrice $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ et telle que $B^2 = (q+1)I_{2n}$.

3b. Montrer que pour tout $d \geqslant 1$, il existe $n \in \mathbb{N}^\star$ et des matrices $M_1, \dots, M_d \in S_n(\mathbb{Q})$ qui commutent deux à deux et telles que $M_k^2 = kI_n$ pour tout entier $1 \leqslant k \leqslant d$.

3c. Soit $d \geqslant 1$ un entier. En déduire que si $q_1, \dots, q_d \in \mathbb{Q}$, $q_i > 0$, alors il existe $n \in \mathbb{N}^\star$ et des matrices $M_1, \dots, M_d \in S_n(\mathbb{Q})$ qui commutent deux à deux et telles que $M_i^2 = q_i I_n$ pour tout $1 \leqslant i \leqslant d$.

4. Le but de cette question est de montrer que $\sqrt[3]{2}$ n'est pas valeur propre d'une matrice symétrique à coefficients dans $\mathbb{Q}$. On raisonne par l'absurde, supposant l'existence d'une matrice $M \in S_n(\mathbb{Q})$ (pour un certain entier n) dont $\sqrt[3]{2}$ est valeur propre.

4a. Montrer que $X^3 - 2$ divise le polynôme caractéristique de M. (On pourra commencer par prouver que $\sqrt[3]{2} \notin \mathbb{Q}$.)

4b. Conclure.

5. Pour $n \in \mathbb{N}^\star$, construire une matrice $M \in S_n(\mathbb{Q})$ dont $\cos(\frac{2\pi}{n})$ est valeur propre. (On pourra commencer par construire une matrice orthogonale à coefficients dans $\mathbb{Q}$ qui admet $e^{2i\pi/n}$ pour valeur propre.)

Deuxième partie

Soit $P(X)$ un polynôme unitaire de degré $d \geqslant 1$ à coefficients complexes que l'on écrit sous la forme :

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_{d-1} X^{d-1} + X^d.$$

On suppose que $a_0 \neq 0$. On note $\lambda_1, \ldots, \lambda_d \in \mathbb{C}$ les racines de $P(X)$ (avec multiplicité). Pour tout entier $n \geqslant 1$, on définit :

$$N_n = \lambda_1^n + \lambda_2^n + \cdots + \lambda_d^n.$$

6. Soit $Q(X)$ le polynôme réciproque de $P(X)$ défini par $Q(X) = X^d P(\frac{1}{X})$. Montrer que :

$$\begin{aligned} Q(X) &= 1 + a_{d-1} X + \cdots + a_1 X^{d-1} + a_0 X^d \\ &= (1 - \lambda_1 X)(1 - \lambda_2 X) \cdots (1 - \lambda_d X). \end{aligned}$$

7. On définit la fonction $f : \mathbb{R} \backslash (\mathbb{R} \cap \{\frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_d}\}) \to \mathbb{C}$ par $f(x) = \frac{Q'(x)}{Q(x)}$.
Montrer qu'il existe $r > 0$ tel que f est développable en série entière sur $]-r, r[$, et que le développement en série entière de f en 0 s'écrit :

$$\forall x \in \,]-r, r[\,, \quad f(x) = -\sum_{n=0}^{\infty} N_{n+1} x^n.$$

8a. Montrer que si $a_0, \ldots, a_{d-1}$ sont des éléments de $\mathbb{Q}$, alors $N_n \in \mathbb{Q}$ pour tout $n \geqslant 1$.

8b. Réciproquement montrer que si $N_n \in \mathbb{Q}$ pour tout $n \geqslant 1$, alors $a_0, \ldots, a_{d-1}$ sont des éléments de $\mathbb{Q}$.

8c. En déduire que si $\mu_1, \ldots, \mu_d$ sont des nombres complexes et si $P(X) = \prod_{i=1}^d (X - \mu_i)$, alors $P(X) \in \mathbb{Q}[X]$ si et seulement si

$$\forall n \geqslant 1, \quad \sum_{i=1}^d \mu_i^n \in \mathbb{Q}.$$

9. Soient $n \geqslant 1$ et $m \geqslant 1$ deux entiers et $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ des nombres complexes. On définit :

$$\begin{aligned} A(X) &= (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \\ B(X) &= (X-\beta_1)(X-\beta_2)\cdots(X-\beta_m). \end{aligned}$$

Montrer que si $A(X)$ et $B(X)$ sont à coefficients rationnels, alors les polynômes

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(X-\alpha_i\beta_j) \quad \text{et} \quad \prod_{i=1}^{n}\prod_{j=1}^{m}(X-\alpha_i-\beta_j)$$

sont aussi à coefficients rationnels.

Troisième partie

On dit qu'un nombre complexe z est *totalement réel* (resp. *totalement positif*) s'il existe un polynôme $P(X)$ non nul à coefficients rationnels tel que :

(i) z est une racine de P, et

(ii) toutes les racines de P sont dans $\mathbb{R}$ (resp. dans $\mathbb{R}_+$).

10. Soit M une matrice symétrique à coefficients dans $\mathbb{Q}$. Montrer que les valeurs propres de M sont totalement réelles.

11a. Montrer que l'ensemble des nombres totalement réels est un sous-corps de $\mathbb{R}$. (On pourra utiliser le résultat de la question **9**.)

11b. Montrer que l'ensemble des nombres totalement positifs est inclus dans $\mathbb{R}_+$, est stable par addition, multiplication et que l'inverse d'un nombre totalement positif non nul est totalement positif.

12. Soit x un nombre complexe. Montrer que x est totalement réel si et seulement si x^2 est totalement positif.

Quatrième partie

Le but de cette partie est de montrer que, réciproquement, tout nombre totalement réel est valeur propre d'une matrice symétrique à coefficients dans $\mathbb{Q}$.
On note $\mathscr{R}$ l'ensemble des nombres totalement réels et on **admet** qu'il existe une fonction $t : \mathscr{R} \to \mathbb{Q}$ vérifiant les deux propriétés suivantes :

(i) pour $x, y \in \mathscr{R}$ et $\lambda, \mu \in \mathbb{Q}$, on a $t(\lambda x + \mu y) = \lambda t(x) + \mu t(y)$

(ii) pour x totalement positif, on a $t(x) \geqslant 0$ et l'égalité est stricte si $x \neq 0$.

On considère un nombre z totalement réel non nul. Par définition, il existe un polynôme unitaire $Z(X) \in \mathbb{Q}[X]$ qui annule z. On écrit $Z(X)$ sous la forme :

$$Z(X) = X^d - \big(a_{d-1}X^{d-1} + \cdots + a_1 X + a_0\big)$$

avec $d \in \mathbb{N}^\star$ et $a_i \in \mathbb{Q}$ pour tout $i \in \{0, \ldots, d-1\}$. On suppose en outre que $Z(X)$ est choisi de façon à ce que d soit minimal parmi les degrés des polynômes unitaires $P(X) \in \mathbb{Q}[X]$ tels que $P(z) = 0$.

On considère la matrice S de taille $d \times d$ dont le coefficient (i, j), $1 \leqslant i, j \leqslant d$, vaut $t(z^{i+j})$. Pour $X, Y \in \mathbb{R}^d$, on pose $B(X, Y) = X^T S Y$.

13a. Montrer que $B(X, X) > 0$ pour $X \in \mathbb{Q}^d$, $X \neq 0$.

13b. En déduire que la matrice S est inversible.

14. Montrer que B est un produit scalaire sur $\mathbb{R}^d$.

15a. Montrer qu'il existe une base $(e_1, \ldots, e_d)$ de $\mathbb{R}^d$ avec $e_i \in \mathbb{Q}^d$ pour tout i et $B(e_i, e_j) = 0$ pour $i \neq j$.

15b. En déduire qu'il existe $P \in \mathrm{GL}_d(\mathbb{Q})$ et $q_1, \ldots, q_d \in \mathbb{Q}$, $q_i > 0$, tels que :

$$S = P^T \cdot \mathrm{Diag}(q_1, \ldots, q_d) \cdot P.$$

On pose :

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \ddots & 0 & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{d-2} \\ 0 & \cdots & 0 & 1 & a_{d-1} \end{pmatrix}.$$

16. Calculer le polynôme caractéristique de M.

17a. Vérifier que la matrice SM est symétrique.

17b. En déduire que la matrice RMR^{-1} est symétrique où $R = \mathrm{Diag}(\sqrt{q_1}, \ldots, \sqrt{q_d}) \cdot P$.

18. Construire une matrice symétrique à coefficients rationnels dont z est valeur propre.

X-ENS 2020 – Épreuve A

Serge Francinou & Hervé Gianella

1. La matrice $M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est symétrique à coefficients rationnels et a pour polynôme caractéristique le polynôme $X^2 - (\operatorname{Tr} M)X + \det M = X^2 - 2$. Donc $\sqrt{2}$ est valeur propre de M.

2. **(a)** On a $\chi_M(\sqrt{3}) = 0$ ce qui donne $3 - (\operatorname{Tr} M)\sqrt{3} + \det M = 0$. Or $\sqrt{3}$ est irrationnel et $\operatorname{Tr} M, \det M$ sont des rationnels. On a donc nécessairement $\operatorname{Tr} M = 0$ et $\det M = -3$ soit $\chi_M = X^2 - 3$.

(b) Si $n \equiv 0\ [3]$ alors $n^2 \equiv 0\ [3]$ et si $n \equiv 1$ ou $2\ [3]$ alors $n^2 \equiv 1\ [3]$ (car $2^2 \equiv 1\ [3]$).

(c) Supposons qu'il existe un triplet (x, y, z) d'entiers premiers entre eux tel que $x^2 + y^2 = 3z^2$. En passant modulo 3 on a $x^2 + y^2 \equiv 0\ [3]$. D'après la question précédente cela impose que x et y sont tous les deux divisibles par 3. Mais dans ce cas 9 divise $3z^2$ et z est aussi divisible par 3. C'est contradictoire.

(d) La matrice M s'écrit $M = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ et on a $\det M = -a^2 - b^2 = -3$ soit $a^2 + b^2 = 3$. On peut écrire $a = \dfrac{x}{z}$ et $b = \dfrac{y}{z}$ avec x, y, z entiers tels que pgcd $(x, y, z) = 1$. Mais on a alors une contradiction avec la question précédente.

3. **(a)** La matrice $B = \begin{pmatrix} A & I_n \\ I_n & -A \end{pmatrix}$ convient. On peut la trouver en étudiant d'abord le cas $n = 1$.

(b) On procède par récurrence sur d. Pour $d = 1$ on peut prendre $n = 1$ et $M_1 = (1)$. Supposons le résultat vrai au rang d avec des matrices $M_1, \dots, M_d$. On considère alors les matrices de taille $2n$ suivantes :

$$M'_1 = \begin{pmatrix} M_1 & 0 \\ 0 & M_1 \end{pmatrix}, \dots, M'_d = \begin{pmatrix} M_d & 0 \\ 0 & M_d \end{pmatrix}, M'_{d+1} = \begin{pmatrix} M_d & I_n \\ I_n & -M_d \end{pmatrix}$$

Elles sont symétriques, à coefficients dans $\mathbb{Q}$, commutent deux à deux et satisfont la propriété au rang $d + 1$ par des calculs par blocs et d'après la question précédente.

(c) Si $M \in \mathcal{S}_n(\mathbb{Q})$ vérifie $M^2 = kI_n$ avec $k \in \mathbb{N}^*$ alors M est inversible et la matrice M^{-1} est encore symétrique à coefficients dans $\mathbb{Q}$ et vérifie $(M^{-1})^2 = \dfrac{1}{k}I_n$. De plus, si M, N sont deux matrices de $\mathcal{S}_n(\mathbb{Q})$ qui commutent avec $M^2 = kI_n$ et $N^2 = k'I_n$ on a $MM' \in \mathcal{S}_n(\mathbb{Q})$ et $(MM')^2 = kk'I_n$.

Soit alors $d \geqslant 1$ et $q_1, \dots, q_d$ des rationnels strictement positifs. On pose $q_i = \dfrac{a_i}{b_i}$ pour tout i avec a_i, b_i dans $\mathbb{N}^*$. D'après la question (b), appliquée avec un entier plus grand que tous les a_i et tous les b_i, on peut trouver $n \in \mathbb{N}^*$ et des matrices $A_1, \dots A_d, B_1, \dots, B_d$ de $\mathcal{S}_n(\mathbb{Q})$ qui commutent toutes et dont les carrés sont respectivement les matrices scalaires a_iI_n et b_iI_n. Compte tenu des remarques qui précèdent les matrices $M_i = A_iB_i^{-1}$ sont dans $\mathcal{S}_n(\mathbb{Q})$, commutent deux à deux et vérifient $M_i^2 = q_iI_n$.

4. **(a)** Il est clair que $\sqrt[3]{2} \notin \mathbb{Q}$ car si $\sqrt[3]{2} = \dfrac{a}{b}$ avec deux entiers a et b premiers entre eux, alors $a^3 = 2b^3$ et a est pair. En posant $a = 2a'$ on constate que b est aussi pair ce qui est absurde. L'ensemble I des polynômes $P \in \mathbb{Q}[X]$ tels que $P(\sqrt[3]{2}) = 0$ est un idéal de $\mathbb{Q}[X]$, non nul car il contient $X^3 - 2$, et est donc engendré par un unique polynôme unitaire μ (le polynôme minimal de $\sqrt[3]{2}$). Celui-ci divise $X^3 - 2$ et n'est pas de degré 1 car $\sqrt[3]{2} \notin \mathbb{Q}$. Il ne peut pas non plus être de degré 2 car le quotient $\dfrac{X^3 - 2}{\mu}$ serait de degré 1 et aurait une racine rationnelle. Mais c'est impossible car les racines de $X^3 - 2$ sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. On a donc $\mu = X^3 - 2$.

Comme $\sqrt[3]{2}$ est valeur propre de M, le polynôme caractéristique de M s'annule en $\sqrt[3]{2}$ et est donc dans I puisqu'il est à coefficients dans $\mathbb{Q}$. On en déduit que $X^3 - 2$ divise χ_M.

(b) On obtient notre contradiction car les valeurs propres de M sont toutes réelles et ce n'est pas le cas de $j\sqrt[3]{2}$.

5. Considérons la matrice de permutation P correspondant au n-cycle $(1, 2, \dots, n)$. C'est une matrice orthogonale, à coefficients dans $\mathbb{Q}$ et son polynôme caractéristique est $X^n - 1$. En particulier $e^{2i\pi/n}$ est valeur propre de P. On note que ${}^t P = P^{n-1} = P^{-1}$. Donc la partie symétrique de P est égale à $\dfrac{1}{2}(P + P^{-1})$ et, en diagonalisant P dans $\mathbb{C}$, on voit que ses valeurs propres sont les $\cos \dfrac{2k\pi}{n}$ pour $0 \leqslant k \leqslant n-1$. Elle répond à la question.

6. On a $Q(X) = X^d \left(\left(\dfrac{1}{X}\right)^d + a_{d-1}\left(\dfrac{1}{X}\right)^{d-1} + \cdots + a_1\left(\dfrac{1}{X}\right) + a_0 \right) = 1 + a_{d-1}X + \cdots + a_1 X^{d-1} + a_0 X^d$. Par ailleurs, $Q(X) = X^d(1/X - \lambda_1)\cdots(1/X - \lambda_d) = (1 - \lambda_1 X)\cdots(1 - \lambda_d X)$ en distribuant un facteur X sur chacun des facteurs $(1/X - \lambda_i)$.

7. Pour x dans le domaine de définition de f, on a

$$f(x) = \frac{\sum_{i=1}^d (-\lambda_i) \prod_{k \neq i}(1 - \lambda_k x)}{Q(x)} = -\sum_{i=1}^n \frac{\lambda_i}{1 - \lambda_i x}.$$

Si pour tout i, $|\lambda_i x| < 1$, on a

$$f(x) = -\sum_{i=1}^d \lambda_i \sum_{n=0}^{+\infty} (\lambda_i x)^n = -\sum_{n=0}^{+\infty} \sum_{i=1}^d \lambda_i^{n+1} x^n = -\sum_{n=0}^{+\infty} N_{n+1} x^n,$$

l'interversion étant possible puisque la somme sur l'indice i est finie. Si on note r la valeur minimale des $1/|\lambda_i|$, $r > 0$ et pour $x \in]-r, r[$, on a $f(x) = -\sum_{n=0}^{+\infty} N_{n+1} x^n$ et f est bien développable en série entière.

8. **(a) (b)** On a pour $|x| < r$, $f(x)Q(x) = Q'(x)$. Comme f et Q sont de rayons strictement positifs, la règle du produit de Cauchy s'applique : le produit $f(x)Q(x)$ est développable en série entière et ses coefficients s'obtiennent par les formules de convolution : le coefficient de x^k dans f est $-N_{k+1}$, celui de x^l dans Q est a_{d-l} si $l \leqslant d$ (avec $a_d = 1$) et 0 sinon. Le coefficient de x^n dans le produit $f(x)Q(x)$ est donc

$$-\sum_{\substack{k+l=n \\ l \leqslant d}} N_{k+1} a_{d-l}.$$

Comme le produit $f(x)Q(x)$ est égal à $Q'(x)$ avec $Q'(x) = \sum_{n=1}^d n a_{d-n} X^{n-1}$, par unicité des coefficients d'une série entière de rayon strictement positif, on obtient

• pour $n < d$, $-(n+1)a_{d-n-1} = N_{n+1}a_d + N_n a_{d-1} + \cdots + a_{d-n}N_1 = N_{n+1} + N_n a_{d-1} + \cdots + a_{d-n}N_1$;

• pour $n \geqslant d$, $N_{n+1}a_d + N_n a_{d-1} + \cdots + N_{n+2-d}a_1 + N_{n+1-d}a_0 = N_{n+1} + N_n a_{d-1} + \cdots + N_{n+2-d}a_1 + N_{n+1-d}a_0 = 0$.

Si les coefficients a_i sont dans $\mathbb{Q}$, il apparaît que si $N_1, \dots, N_n \in \mathbb{Q}$, alors N_{n+1} est aussi rationnel. Pour $n = 0$, on a $N_1 = -a_{d-1} \in \mathbb{Q}$ et par récurrence sur n, tous les sommes de Newton N_n sont rationnelles : on a (a).

Supposons réciproquement que tous les N_n sont rationnels. On a $-a_{d-1} = N_1$ et $a_{d-1} \in \mathbb{Q}$. Si on suppose $a_{d-1}, \dots, a_{d-n}$ rationnels, on a par la formule pour $n < d$, $a_{d-n-1} \in \mathbb{Q}$. On obtient donc par récurrence que tous les coefficients a_i sont rationnels.

(c) Les deux sous-questions précédentes donnent le résultat lorsque les μ_i sont non nuls. Quitte à renuméroter les racines, on peut supposer les $\mu_i \neq 0$ si $i \leqslant d'$ et $\mu_i = 0$ pour $d' < i \leqslant d$. On a donc $P = X^{d-d'} \prod_{i=1}^{d'} (X - \mu_i) = X^{d-d'}Q(X)$. On a

$$P \in \mathbb{Q}[X] \iff Q \in \mathbb{Q}[X] \iff \forall n \geqslant 1,\ \sum_{i=1}^{d'} \mu_i^n \in \mathbb{Q} \iff \forall n \geqslant 1,\ \sum_{i=1}^{d} \mu_i^n \in \mathbb{Q}$$

9. Notons $N_k = \sum_{i=1}^{n} \alpha_i^k$, $N'_k = \sum_{i=1}^{m} \beta_i^k$, $N''_k = \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} (\alpha_i\beta_j)^k$ et enfin, $N'''_k = \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} (\alpha_i + \beta_j)^k$ pour $k \geqslant 1$. Comme $A, B \in Q[X]$, les sommes N_k et N'_k sont rationnelles. Pour montrer que les polynômes demandés sont aussi à coefficients rationnels, il suffit de démontrer que les sommes de Newton associées N''_k et N'''_k sont toutes rationnelles. On a bien

$$N''_k = \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} \alpha_i^k\beta_j^k = N_k N'_k \in \mathbb{Q},$$

$$N'''_k = \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} \sum_{l=0}^{n} k\binom{k}{l}\alpha_i^l\beta_j^{k-l} = \sum_{l=0}^{k}\binom{k}{l} \sum_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}} \alpha_i^l\beta_j^{k-l} = \sum_{l=0}^{k}\binom{k}{l} N_l N'_{k-l} \in \mathbb{Q}.$$

10. Une valeur propre de $M \in \mathcal{S}_n(\mathbb{Q})$ est une racine de $\chi_M \in \mathbb{Q}[X]$. Or M est aussi une matrice symétrique réelle donc diagonalisable (en base orthonomée) d'après le théorème spectral. En particulier, χ_M est scindé sur $\mathbb{R}$ et la valeur propre est donc totalement réelle.

11. **(a)** 1 est totalement réel puisque $X - 1 \in \mathbb{Q}[X]$. Soit α_1 et β_1 des nombres totalement réels. Il s'agit de montrer que $-\alpha_1$, $\alpha_1 + \beta_1$, $\alpha_1\beta_1$ et $1/\alpha_1$ (quand α_1 non nul) sont tous des nombres totalement réels. Il existe $A, B \in \mathbb{Q}[X]$ scindés sur $\mathbb{R}$ s'écrivant

$$A(X) = (X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n), \quad B(X) = (X - \beta_1)(X - \beta_2)\cdots(X - \beta_m).$$

Avec la question 9, on a directement que $\alpha_1\beta_1$ et $\alpha_1 + \beta_1$ sont des racines de polynômes de $\mathbb{Q}[X]$ scindés sur $\mathbb{R}$: ils sont totalement réels. Par ailleurs, $-\alpha_1$ est racine de $A(-X) \in \mathbb{Q}[X]$ qui est encore scindé sur $\mathbb{R}$ donc $-\alpha_1$ est totalement réel. Si α_1 est non nul, le polynôme réciproque de A, $C(X) = X^n A\left(\frac{1}{X}\right)$ est à coefficients rationnels et admet comme racines les inverses des racines non nulles de A. Les racines de C sont donc réelles et $1/\alpha_1$ est totalement réel.

(b) Il suffit de reprendre ce qui précède mais avec l'hypothèse que α_1 et β_1 sont totalement positifs et on peut alors supposer les α_i et les β_j dans $\mathbb{R}_+$. En considérant chacun des polynômes trouvés à la question précédente pour la somme, le produit et l'inverse, on constate que les racines de tous ces polynômes sont positives.

12. On suppose x^2 totalement positif. Il existe $A(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \in \mathbb{Q}[X]$ avec $\alpha_1 = x^2$ et les α_i tous positifs. On pose $B(X) = A(X^2) \in \mathbb{Q}[X]$, on a $B(x) = 0$ et B est scindé sur $\mathbb{R}$ car $B(X) = \prod_{i=1}^{n}(X - \sqrt{\alpha_i})(X + \sqrt{\alpha_i})$: x est donc totalement réel.

On suppose réciproquement $x = \alpha_1$ totalement réel et on considère $A(X) = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \in \mathbb{Q}[X]$ avec les α_i réels. On pose $C(X) = (X - \alpha_1^2)(X - \alpha_2^2)\cdots(X - \alpha_n^2)$. Les racines de C sont positives et x^2 est l'une d'elle. Reste à voir si $C \in \mathbb{Q}[X]$. Comme les sommes de Newton de C sont des sommes de Newton de $A \in \mathbb{Q}[X]$ (puisque $\sum_{i=1}^{n}(\alpha_i^2)^k = \sum_{i=1}^{n}\alpha_i^{2k}$) et comme ces dernières sont rationnelles puisque $A \in \mathbb{Q}[X]$ (question 8), on en déduit que $C \in \mathbb{Q}[X]$ (toujours question 8).

13. **(a)** Soit $X \in \mathbb{Q}^d$ non nul de coordonnées $x_1, \dots, x_d$. On a, par $\mathbb{Q}$-linéarité de t,

$$B(X, X) = \sum_{1\leqslant i,j\leqslant d} t(z^{i+j})x_i x_j = t\left(\sum_{1\leqslant i,j\leqslant d} x_i x_j z^{i+z}\right) = t\left(\left(\sum_{k=1}^{d} x_k z^k\right)^2\right)$$

Le corps des nombres totalement réels contient $\mathbb{Q}$ donc $\sum_{k=1}^{d} x_k z^k$ est totalement réel. Son carré est donc totalement positif d'après la question 12. Il n'est pas nul, car z étant non nul, on aurait $\sum_{i=1}^{d} x_i z^{i-1} = 0$ et cela nous donnerait un polynôme non nul de $\mathbb{Q}[X]$ de degré $< d$ qui s'annule en z ce qui contredirait la minimalité de d (il est facile de rendre le polynôme unitaire). La propriété (*ii*) de la fonction t permet de conclure que $B(X, X) > 0$.

(b) Si la matrice B n'était pas inversible on pourrait trouver un vecteur non nul X de $\mathbb{Q}^d$ dans son noyau et un tel vecteur contredirait le résultat précédent.

14. Par densité de $\mathbb{Q}^d$ dans $\mathbb{R}^d$ on a $B(X, X) \geqslant 0$ pour tout vecteur $X \in \mathbb{R}^d$ donc la forme bilinéaire symétrique B est positive (notons que la symétrie de B découle de la symétrie de la matrice S). Les valeurs propres de S sont toutes positives : en effet, si X est un vecteur propre de S associée à λ, $X^T SX = \lambda X^T X$ et $\lambda \geqslant 0$ car $X^T X > 0$. Comme S est inversible, ces valeurs propres sont mêmes strictement positives. Par application du théorème spectral, on prend ensuite une base orthonormée de $\mathbb{R}^d$, $(\varepsilon_i)_{1\leqslant i\leqslant d}$, ε_i associée à la valeur propre λ_i de S et si $X = \displaystyle\sum_{i=1}^{d} x_i\varepsilon_i \neq 0$, $X^T SX = \displaystyle\sum_{i=1}^{d} \lambda_i x_i^2 > 0$. La forme bilinéaire symétrique canoniquement associée à S est donc définie positive : c'est un produit scalaire.

15. **(a)** On cherche une base orthogonale de $\mathbb{R}^d$ pour le produit scalaire B qui soit formée de vecteurs à coefficients rationnels. On part de la base canonique $(\varepsilon_1, \dots, \varepsilon_d)$ et on lui applique le processus de Gram-Schmidt mais sans normaliser les vecteurs. On pose donc $e_1 = \varepsilon_1$ puis $e_2 = \varepsilon_2 - \dfrac{B(\varepsilon_2, e_1)}{B(e_1, e_1)} e_1$ et de manière générale,

$$e_{p+1} = \varepsilon_{p+1} - \sum_{i=1}^{p} \frac{B(\varepsilon_{p+1}, e_i)}{B(e_i, e_i)} e_i$$

Les produits scalaires sont tous dans $\mathbb{Q}$ et la famille $(e_1, \dots, e_d)$ est une base B-orthogonale de $\mathbb{R}^d$ qui convient (on a aisément $\mathrm{Vect}(e_1, \dots, e_k) = \mathrm{Vect}(\varepsilon_1, \dots, \varepsilon_k)$ pour tout k).

(b) Notons $P \in GL_d(\mathbb{Q})$ la matrice de passage de la base canonique à la base $(e_1, \dots, e_d)$ que l'on vient de construire. Soit X, Y dans $\mathbb{R}^d$ et X', Y' les coordonnées de ces deux vecteurs dans la base $(e_1, \dots, e_d)$. On a $X = PX'$, $Y = PY'$ et

$$\sum_{k=1}^{d} q_k x'_k y'_k = B(X, Y) = X^T SY = X'^T P^T SPY'$$

où l'on a posé $q_k = B(e_k, e_k) > 0$ pour tout k (la première égalité provient de ce que la base des e_i est orthogonale). Comme $\displaystyle\sum_{k=1}^{d} q_k x'_k y'_k = X'^T DY'$ avec $D = \mathrm{Diag}(q_1, \dots, q_d)$ pour tous X' et Y', en prenant les vecteurs de la base canonique, on en déduit que $P^T SP = D = \mathrm{Diag}(q_1, \dots, q_d)$. La matrice P^{-1} répond à la question posée.

16. La matrice M est la matrice compagnon du polynôme Z et il est classique de montrer que $\chi_M = Z$ (on peut par exemple dans le déterminant du polynôme caractéristique ajouter à la ligne L_i la ligne XL_{i+1} de $i = n - 1$ à $i = 1$, ou bien établir le résultat par récurrence sur d).

17. **(a)** La matrice SM a dans ses $d - 1$ premières colonnes les colonnes 2 à d de S. Elle s'écrit donc

$$\begin{pmatrix} t(z^3) & t(z^4) & \dots & t(z^{d+1}) & s_1 \\ t(z^4) & t(z^5) & & t(z^{d+2}) & s_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ t(z^{d+2}) & t(z^{d+3}) & & t(z^{2d}) & s_d \end{pmatrix}$$

avec, pour tout i,

$$s_i = \sum_{j=1}^{d} a_{j-1} t(z^{i+j}) = t\left(z^{i+1} \sum_{j=1}^{d} a_{j-1} z^{j-1}\right) = t(z^{i+d+1})$$

ce qui prouve la symétrie de la matrice SM.

(b) Posons $\mathrm{D} = \mathrm{Diag}(q_1, \ldots, q_d)$ et $\Delta = \mathrm{Diag}(\sqrt{q_1}, \ldots, \sqrt{q_d})$. On a bien entendu $\Delta^2 = \mathrm{D}$. La matrice SM étant symétrique on a donc

$$\mathrm{P^T DPM} = \mathrm{SM} = (\mathrm{SM})^\mathrm{T} = \mathrm{M^T S^T} = \mathrm{M^T P^T DP}$$

Or $\mathrm{P^T DP} = \mathrm{P^T}\Delta^2\mathrm{P} = (\Delta\mathrm{P})^\mathrm{T}(\Delta\mathrm{P}) = \mathrm{R^T R}$. Il vient donc $\mathrm{R^T RM} = \mathrm{M^T R^T R}$ ou encore en multipliant par les inverses, $\mathrm{RMR^{-1}} = (\mathrm{R^T})^{-1}\mathrm{M^T R^T} = (\mathrm{RMR^{-1}})^\mathrm{T}$ si bien que $\mathrm{RMR^{-1}}$ est symétrique.

18. Considérons $\mathrm{A} = \Delta\mathrm{RMR^{-1}}\Delta = \Delta^2\mathrm{PMP^{-1}}$ qui est symétrique à coefficients rationnels. Considérons l'entier n et les matrices M_i de la question 3c. On considère $\widetilde{\mathrm{D}}$ la diagonale par blocs de taille nd avec des blocs $\mathrm{D} = \Delta^2 = \mathrm{Diag}(q_1, \ldots, q_d)$ et M' la diagonale par blocs de blocs $\mathrm{PMP^{-1}}$. On a $\chi_{\mathrm{M}'} = \chi_\mathrm{M}^n = \mathrm{Z}^n \in \mathbb{Q}[\mathrm{X}]$ et z en est encore racine. En faisant une permutation des vecteurs de la base canonique de $\mathbb{Q}^{nd}$, on trouve que $\widetilde{\mathrm{D}}$ est semblable à la matrice diagonale par blocs de blocs $q_i\mathrm{I}_n$. Plus précisément, il existe une matrice de permutation Q de taille nd telle que $\mathrm{Q}^{-1}\widetilde{\mathrm{D}}\mathrm{Q} = \mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d) = \mathrm{Q^T}\widetilde{\mathrm{D}}\mathrm{Q}$ puisque Q est orthogonale. On note $\mathrm{D}' = \mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d)$ et on considère $\mathrm{B} = \widetilde{\mathrm{D}}\mathrm{M}'$ qui est diagonale par blocs avec des blocs symétriques A. On a $\mathrm{Q^T BQ} = \mathrm{Q^T}\widetilde{\mathrm{D}}\mathrm{QQ^T M'Q} = \mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d)\mathrm{Q^T M'Q}$ qui est encore une matrice symétrique et $\mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d) = \mathrm{Diag}(\mathrm{M}_1^2, \ldots, \mathrm{M}_d^2) = \mathrm{Diag}(\mathrm{M}_1, \ldots, \mathrm{M}_d)^2$. Notons $\mathrm{N} = \mathrm{Diag}(\mathrm{M}_1, \ldots, \mathrm{M}_d)$ qui est une matrice symétrique inversible : $\mathrm{N^{-1}Q^T BQN^{-1}}$ est donc symétrique, elle est à coefficients rationnels car N, Q et B le sont. Mais par ailleurs, $\mathrm{N^{-1}Q^T BQN^{-1}} = \mathrm{NQ^T M'QN^{-1}}$ et cette matrice est semblable à M' qui possède z comme valeur propre, puisque z est racine de son polynôme caractéristique. Il s'ensuit que $\mathrm{N^{-1}Q^T BQN^{-1}}$ est une matrice symétrique à coefficients rationnels admettant z comme valeur propre. Cqfd.