Composition A
X-ENS 2020 – MP

Le but de ce problème est d'étudier certains aspects de la diagonalisabilité des matrices symétriques à coefficients rationnels. Ces matrices sont diagonalisables dans $\mathbf{R}$, 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 $\mathbf{K}$ est un corps,

- on note $\mathscr{M}_{n,m}(\mathbf{K})$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans $\mathbf{K}$ ainsi que $\mathscr{M}_n(\mathbf{K}) = \mathscr{M}_{n,n}(\mathbf{K})$ l'ensemble des matrices carrées de taille n à coefficients dans $\mathbf{K}$;
- on identifie l'espace vectoriel $\mathbf{K}^n$ à l'espace vectoriel des vecteurs colonnes $\mathscr{M}_{n,1}(\mathbf{K})$;
- on note $\mathscr{S}_n(\mathbf{K})$ l'ensemble des matrices symétriques carrées de taille n à coefficients dans $\mathbf{K}$;
- si $A \in \mathscr{M}_{m,n}(\mathbf{K})$, on note A^{T} la matrice transposée de A et, si $m = n$ et avec un abus de notation,

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

son polynôme caractéristique, qui est donc un polynôme unitaire ;

- si $q_1, \ldots, q_n$ sont des éléments de $\mathbf{K}$, on note $\mathrm{diag}(q_1, \ldots, q_n)$ la matrice diagonale de taille n de coefficients diagonaux $q_1, \ldots, q_n$.

PARTIE I

1. Exhiber une matrice M dans $\mathscr{S}_2(\mathbf{Q})$ dont $\sqrt{2}$ est valeur propre.
2. Le but de cette question est de démontrer que $\sqrt{3}$ n'est pas valeur propre d'une matrice de $S_2(\mathbf{Q})$. On suppose qu'il existe M dans $\mathscr{S}_2(\mathbf{Q})$ telle que $\sqrt{3}$ est valeur propre de M.
   (a) En utilisant l'irrationnalité de $\sqrt{3}$, montrer que le polynôme caractéristique de M est $X^2 - 3$.
   (b) Démontrer que pour tout entier relatif n, n^2 est congru à 0 ou 1 modulo 3.
   (c) Démontrer qu'il n'existe pas de triplet d'entiers (x, y, z) premiers entre eux dans leur ensemble tel que $x^2 + y^2 = 3z^2$.
   (d) Conclure.
3. (a) On se donne q dans $\mathbf{Q}$, n dans $\mathbf{N}^*$ et une matrice A dans $\mathscr{S}_n(\mathbf{Q})$ telle que $A^2 = qI_n$. Construire une matrice B dans $\mathscr{S}_{2n}(\mathbf{Q})$ commutant à la matrice $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$ et telle que $B^2 = (q+1)I_{2n}$.
   (b) Démontrer que pour tout entier d vérifiant $d \geq 1$, il existe n dans $\mathbf{N}^*$ et des matrices $M_1, \ldots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $M_k^2 = kI_n$ pour tout entier $1 \leq k \leq d$.
   (c) Soit $d \geq 1$ un entier. En déduire, pour $q_1, \ldots, q_d$ dans $\mathbf{Q}$, avec $q_i > 0$, qu'il existe n dans $\mathbf{N}^*$ et des matrices $M_1, \ldots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $M_i^2 = q_i I_n$ pour tout $1 \leq i \leq d$.
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 $\mathbf{Q}$. On raisonne par l'absurde, supposant l'existence d'une matrice M dans $\mathscr{S}_n(\mathbf{Q})$ (pour un certain n) dont $\sqrt[3]{2}$ est valeur propre.
   (a) Démontrer que $X^3 - 2$ divise le polynôme caractéristique de M. (On pourra commencer par démontrer que $\sqrt[3]{2}$ n'est pas rationnel).
   (b) Conclure.
5. Pour n dans $\mathbf{N}^*$, construire une matrice M de $\mathscr{S}_n(\mathbf{Q})$ dont $\cos(\frac{2\pi}{n})$ est valeur propre. (On pourra commencer par construire une matrice orthogonale à coefficients dans $\mathbf{Q}$ qui admet $e^{2i\pi/n}$ pour valeur propre).

PARTIE II

Soit P un polynôme unitaire de degré $d \geq 1$ à coefficients complexes que l'on écrit sous la forme

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

On suppose $a_0 \neq 0$. On note $\lambda_1, \ldots, \lambda_d$ les racines de P dans $\mathbf{C}$ (avec multiplicité). On définit

$$\forall n \in \mathbf{N}^* \quad N_n = \lambda_1^n + \lambda_2^n + \cdots + \lambda_d^n \, .$$

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

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

7. On définit la fonction f de $\mathbf{R} \setminus \left\{ \frac{1}{\lambda_1}, \ldots, \frac{1}{\lambda_d} \right\}$ dans $\mathbf{C}$ par $f(x) = \frac{Q'(x)}{Q(x)}$.
   Démontrer 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

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

8.(a) Démontrer que si $a_0, \ldots, a_{d-1}$ appartiennent à $\mathbf{Q}$, alors il en va de même pour N_n pour tout $n \geq 1$.

(b) Réciproquement, démontrer que si $\forall n \in \mathbf{N}^* \; N_n \in \mathbf{Q}$, alors $a_0, \ldots, a_{d-1}$ sont rationnels.

(c) En déduire que si $\mu_1, \ldots, \mu_d$ sont des nombres complexes et si $P = \prod_{i=1}^{d} (X - \mu_i)$, alors

$$P \in \mathbf{Q}[X] \Longleftrightarrow \forall n \geq 1 \; \sum_{i=1}^{d} \mu_i^n \in \mathbf{Q} \, .$$

9. Soit n et m deux entiers supérieurs à 1 et $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ des nombres complexes. On définit

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

   Démontrer que si A et B sont à coefficients rationnels, alors

$$\prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i \beta_j) \in \mathbf{Q}[X] \quad \text{et} \quad \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i - \beta_j) \in \mathbf{Q}[X] \, .$$

PARTIE III

On dit qu'un nombre complexe z est *totalement réel* (resp. *totalement positif*) s'il existe un polynôme unitaire à coefficients rationnels tel que

(i) z est une racine de P, et

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

10. Soit M dans $\mathscr{S}_n(\mathbf{Q})$. Démontrer que les valeurs propres de M sont totalement réelles.

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

(b) Démontrer que l'ensemble des nombres totalement positifs est inclus dans $\mathbf{R}^+$, est stable par addition, multiplication, et que l'inverse d'un nombre totalement positif non nul est totalement positif.

12. Soit x dans $\mathbf{C}$. Démontrer que x est totalement réel si et seulement si x^2 est totalement positif.

PARTIE IV

Le but de cette partie est de démontrer que, réciproquement, tout nombre totalement réel est valeur propre d'une matrice symétrique à coefficients dans $\mathbf{Q}$.

On note $\mathcal{R}$ l'ensemble des nombres totalement réels et on **admet** qu'il existe une fonction $t : \mathcal{R} \to \mathbf{Q}$ vérifiant les deux propriétés suivantes :

(i) pour x et y dans $\mathcal{R}$ et λ et μ dans $\mathbf{Q}$, on a $t(\lambda x + \mu y) = \lambda t(x) + \mu t(y)$

(ii) pour x totalement positif, on a $t(x) \geq 0$ 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 dans $\mathbf{Q}[X]$ dont z est racine. On écrit Z sous la forme

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

avec d dans $\mathbf{N}^*$ et a_i dans $\mathbf{Q}$ pour tout $i \in [\![0; d-1]\!]$. On suppose que Z est choisi de façon à ce que d soit minimal parmi les degrés des polynômes unitaires P de $\mathbf{Q}[X]$ tels que $P(z) = 0$.
On considère la matrice S de taille $d \times d$ dont le coefficient (i, j) vaut $t(z^{i+j})$ pour $1 \leq i, j \leq d$.
Pour X et Y dans $\mathbf{R}^d$, on pose $B(X, Y) = X^{\mathrm{T}} S Y$.

13.(a) Démontrer $B(X, X) > 0$ pour X dans $\mathbf{Q}^d$ vérifiant $X \neq 0$.

(b) En déduire que la matrice S est inversible.

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

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

(b) En déduire qu'il existe P dans $\mathrm{GL}_d(\mathbf{Q})$ et $q_1, \ldots, q_d$ dans $\mathbf{Q}$, avec $q_i > 0$, tels que

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

On pose

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

16. Calculer le polynôme caractéristique de M.

17.(a) Vérifier que la matrice SM est symétrique.

(b) 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.

Composition A
X-ENS 2020 – MP

PARTIE I

1. Soit $M = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Alors $M \in \mathscr{S}_2(\mathbf{Q})$ et $\chi_M = X^2 - 2$, donc $\boxed{M \in \mathscr{S}_2(\mathbf{Q}) \text{ et } \sqrt{2} \text{ est valeur propre.}}$

2.(a) Puisque $\sqrt{3}$ n'est pas rationnel, χ_M n'est pas scindé sur $\mathbf{Q}$. Soit alors R le reste de la division euclidienne de χ_M par $X^2 - 3$. Puisque $\mathbf{Q}$ est un corps, R appartient à $\mathbf{Q}[X]$. On a de plus $0 = \chi_M(\sqrt{3}) = R(\sqrt{3})$ puisque $\sqrt{3}$ est racine de X^2-3. Si R est de degré 1, alors, par relation coefficients-racines, $\sqrt{3}$ est rationnel, ce qui n'est pas vrai. Donc R est un polynôme constant, et est donc nul. Ainsi $X^2 - 3$ divise χ_M. Comme ce dernier est unitaire de degré 2, on a $\boxed{\chi_M = X^2 - 3.}$

(b) Soit n un entier relatif. Si $3 \mid n$, alors $3 \mid n^2$. Sinon $n \equiv \pm 1 \pmod 3$ et donc $n^2 \equiv 1 \pmod 3$. Ainsi $\boxed{n^2 \text{ est congru à 0 ou 1 modulo 3.}}$

(c) Soit (x, y, z) un triplet d'entiers vérfiant $x^2 + y^2 = 3z^2$. D'après ce qui précède $x^2 + y^2$ est congru à 0, 1 ou 2 modulo 3, selon qu'aucun, un seul ou les deux parmi x et y sont divisibles par 3. Puisque $3z^2$ est divisble par 3, on en déduit que x et y le sont aussi et donc $x^2 + y^2$ est divisible par 9. Par conséquent $3z^2$ est divisible par 9, donc z^2 est divisble par 3 et, en appliquant à nouveau la question précédente, z est divisble par 3. Il en résulte que 3 divise x, y et z. Par conséquent $\boxed{\text{il n'existe aucun triplet d'entiers premiers entre eux dans leur ensemble tel que } x^2 + y^2 = 3z^2.}$

(d) Soit M dans $\mathscr{S}_2(\mathbf{Q})$ ayant X^2-3 comme polynôme caractéristique. Alors $\mathrm{tr}(M) = 0$ et $\det(M) = -3$. On en déduit qu'on dispose de a et b dans $\mathbf{Q}$ tels que $M = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ et $a^2 + b^2 = 3$. On écrit $a = \dfrac{u}{v}$ et $b = \dfrac{r}{s}$ avec r, s, u et v entiers, et $vs \neq 0$. Il vient $a^2 + b^2 = \dfrac{(us)^2 + (rv)^2}{(vs)^2} = 3$ et donc $(us)^2 + (rv)^2 = 3(vs)^2$. On pose alors $d = pgcd(us, rv, vs)$, $x = us/d$, $y = rv/d$ et $z = vs/d$. Ainsi x, y et z sont entiers, premiers dans leur ensemble et vérifient $x^2 + y^2 = 3z^2$. Par contradiction avec la question précédente : $\boxed{\text{aucune matrice dans } \mathscr{S}_2(\mathbf{Q}) \text{ n'admet } \sqrt{3} \text{ comme valeur propre.}}$

3.(a) Soit $B = \begin{pmatrix} A & I_n \\ I_n & -A \end{pmatrix}$. Alors $B \in \mathscr{S}_{2n}(\mathbf{Q})$ par symétrie de A, $B\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} B = \begin{pmatrix} qI_n & A \\ A & -qI_n \end{pmatrix}$ et $B^2 = (q+1)I_{2n}$: $\boxed{B \in \mathscr{S}_{2n}(\mathbf{Q}), \text{ commute à } \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \text{ et vérifie } B^2 = (q+1)I_{2n}.}$

(b) On raisonne par récurrence. Pour d dans $\mathbf{N}^*$, on note $(\mathbf{H}_d)$ le prédicat : il existe n dans $\mathbf{N}^*$ et des matrices $M_1, \ldots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $M_k^2 = kI_n$ pour tout entier $1 \leq k \leq d$.

Pour $d = 1$, en prenant $n = 1$ et $M_1 = I_1$, on déduit que $(\mathbf{H}_1)$ est vrai. Soit d dans $\mathbf{N}^*$ tel que $(\mathbf{H}_d)$ est vrai. On dispose donc de n dans $\mathbf{N}^*$ et de matrices $M_1, \ldots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $M_k^2 = kI_n$ pour tout entier $1 \leq k \leq d$. On pose alors $m = 2n$, $M'_k = \begin{pmatrix} M_k & 0 \\ 0 & M_k \end{pmatrix}$ pour k dans $[\![1; d]\!]$ et $M'_{d+1} = \begin{pmatrix} M_d & I_n \\ I_n & -M_d \end{pmatrix}$. Alors par construction toutes ces matrices sont dans $\mathscr{S}_m(\mathbf{Q})$. Les matrices M'_k commutent entre elles pour $k \leq d$ car c'est le cas pour les matrices M_k, et on a $M'_k M'_{d+1} = M'_{d+1} M'_k = \begin{pmatrix} M_k M_d & M_k \\ M_k & -M_k M_d \end{pmatrix}$. Enfin pour $k \leq d+1$, $(M'_k)^2 = k^2 I_m$. On en déduit que $(\mathbf{H}_{d+1})$ est vrai. Le principe de récurrence permet donc de conclure

Pour tout d dans $\mathbf{N}^*$, il existe n dans $\mathbf{N}^*$ et des matrices $M_1, \dots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $M_k^2 = kI_n$ pour tout entier $1 \leq k \leq d$.

(c) Soit $q_1, \dots, q_d$ dans $\mathbf{Q}$, avec $q_i > 0$. On dispose de $a_1, \dots, a_d$ et $b_1, \dots, b_d$ dans $\mathbf{N}^*$ vérifiant, pour tout i dans $[\![1; d]\!]$, $q_i = \dfrac{a_i}{b_i}$. On note alors $m = \max(a_1, \dots, a_d, b_1, \dots, b_d)$. D'après la question précédente on dispose de n dans $\mathbf{N}^*$ et de matrices $N_1, \dots, N_m$ dans $\mathscr{S}_n(\mathbf{Q})$ qui commutent deux à deux et telles que $N_k^2 = kI_n$ pour tout $1 \leq k \leq m$. En particulier toutes ces matrices sont inversibles et on peut poser $M_i = N_{a_i} N_{b_i}^{-1}$ pour $1 \leq i \leq d$. Toutes ces matrices commutent entre elles, car les N_k commutent entre elles, et sont symétriques car les N_k le sont et commutent entre elles, et donc les M_i appartiennent à $\mathscr{S}_n(\mathbf{Q})$. Enfin on a, toujours par commutativité, $M_i^2 = N_{a_i}^2 N_{b_i}^{-2} = q_i I_n$. Ainsi

$M_1, \dots, M_d$ appartiennent à $\mathscr{S}_n(\mathbf{Q})$, commutent deux à deux et vérifient $M_i^2 = q_i I_n$ pour $1 \leq i \leq d$.

4.(a) Soit R le reste de la division euclidienne de χ_M par $X^3 - 2$. Alors R appartient à $\mathbf{Q}[X]$ et $R(\sqrt[3]{2}) = \chi_M(\sqrt[3]{2}) = 0$ puisque $\sqrt[3]{2}$ est racine de $X^3 - 2$. Si R n'est pas nul, on dispose de (a, b, c) rationnels tels que $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$. Quitte à diviser par leur pgcd, on peut supposer a, b et c premiers entre eux dans leur ensemble. Si a est pair, on peut diviser cette relation par $\sqrt[3]{2}$ et obtenir $b + c\sqrt[3]{2} + \dfrac{a}{2}\sqrt[3]{4} = 0$.

Si b est également pair, on a également $c + \dfrac{a}{2}\sqrt[3]{2} + \dfrac{b}{2}\sqrt[3]{2}$. Comme a, b et c ne sauraient être tous trois pairs, on en déduit que, quitte à modifier a, b et c, on peut supposer que a est impair. On remarque alors qu'on a, en multipliant la première équation par $\sqrt[3]{2}$ puis par $\sqrt[3]{4}$

$$\begin{pmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt[3]{2} \\ \sqrt[3]{4} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

et donc que la matrice $\left(\begin{smallmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{smallmatrix}\right)$ ne saurait être inversible. Mais son déterminant est impair puisque somme de a^3 et de termes pairs. Cette contradiction assure $R = 0$ et donc $X^3 - 2$ divise χ_M.

(b) On en conclut que si une telle matrice M existe, alors $j\sqrt[3]{2}$ est valeur propre de M. Comme cette matrice est symétrique réelle, le théorème spectral assure que c'est impossible et donc

aucune matrice symétrique à coefficients rationnels n'admet $\sqrt[3]{2}$ comme valeur propre.

5. Soit n dans $\mathbf{N}^*$. La matrice de permutation, qui est aussi la matrice compagnon du polynôme $X^n - 1$, $\begin{pmatrix} 0 & & & 1 \\ 1 & 0 & & \\ & \ddots & \ddots & \\ (0) & & 1 & 0 \end{pmatrix}$, admet $X^n - 1$ comme polynôme caractéristique (et polynôme minimal). Comme ses vecteurs colonnes forment une base orthonormée, c'est aussi une matrice orthogonale. On note A cette matrice et son spectre est l'ensemble des racines n^{e} de l'unité, chacune avec multiplicité 1. On pose $M = \frac{1}{2}(A + A^{\mathrm{T}})$. Alors $M \in \mathscr{S}_n(\mathbf{Q})$ par construction. On a aussi $M = \frac{1}{2}(A + A^{-1})$ puisque A est orthogonal. Si X est un vecteur propre pour A associé à $e^{2i\pi/n}$, on a $A^{-1}X = e^{-2i\pi/n}X$ et donc $MX = \cos(\frac{2\pi}{n})$. Ainsi M appartient à $\mathscr{S}_n(\mathbf{Q})$ et admet $\cos(\frac{2\pi}{n})$ comme valeur propre.

PARTIE II

6. Par définition, on a $Q = \displaystyle\sum_{k=0}^{d} a_k X^{n-k} = a_0 X^d + \cdots + a_{d-1}X + 1$ et $Q = X^d \displaystyle\prod_{i=1}^{d}(\frac{1}{X} - \lambda_i) = \prod_{i=1}^{d}(1 - \lambda_i X)$, i.e. $Q = 1 + a_{d-1}X + \cdots + a_1 X^{d-1} + a_0 X^d = (1 - \lambda_1 X)(1 - \lambda_2 X) \cdots (1 - \lambda_d X)$.

7. Si μ est une racine de Q de multiplicité m, on a $Q = a_0(X - \mu)^m R$ avec $R(\mu) \neq 0$. On a donc $Q' = a_0(X - \mu)^{m-1}(mR + (X - \mu)R')$. On a donc $\frac{(X-\mu)Q'}{Q} = \frac{mR + (X-\mu)R'}{R}$ et cette faction admet m

comme évaluation en μ. On en déduit $f(x) = \sum_{k=1}^{r} \frac{m_k}{x - \mu_k}$, où les (μ_k) sont les racines de Q comptées sans multiplicités et m_k leurs multiplicités. Chacun des termes de la somme est développable en série entière avec un rayon de convergence égal à μ_k. En posant $r = \min \frac{1}{|\lambda_i|}$, ce qui est licite par finitude et non nullité des racines de P, et puisque les racines de Q sont les inverses de celles de P, on en déduit que $\boxed{f \text{ est développable en série entière sur }]-r;r[.}$

Il vient, sur $]-r;r[$,

$$f(x) = -\sum_{k=1}^{r} \frac{m_k}{\mu_k} \sum_{n=0}^{+\infty} \mu_k^{-n} x^n \quad \text{ou encore} \quad f(x) = -\sum_{n=0}^{+\infty} \left(\sum_{k=1}^{r} m_k \mu_k^{-n+1} \right) x^n$$

ce qui peut s'écrire, puisque les μ_k sont les inverses des λ_i et en tenant compte des multiplicités $\boxed{f(x) = -\sum_{n=0}^{\infty} N_{n+1} x^n.}$

8.(a) Si $a_0, \ldots, a_{d-1}$ appartiennent à $\mathbf{Q}$, alors f est une fraction rationnelle à coefficients rationnels. Il en va donc de même pour toutes ses dérivées et donc l'évaluation en 0 de ces dérivées est rationnelle. Or pour tout entier n supérieur à 1, on a $N_n = -\frac{f^{(n-1)}(0)}{(n-1)!}$ et donc $\boxed{N_n \in \mathbf{Q}.}$

(b) Si, pour tout entier n dans $\mathbf{N}^*$, N_n est rationnel, alors f et toutes ses dérivées prennent des valeurs rationnelles en 0. On va démontrer par récurrence forte sur k dans $[\![0;d]\!]$ le prédicat $(\mathbf{H}_k) : Q^{(k)}(0)$, et donc a_{d-k}, sont rationnels.

Pour $k = 0$, on a $Q(0) = a_d = 1$, donc $(\mathbf{H}_0)$ est vrai. Supposons $(\mathbf{H}_i)$ vrai pour $0 \leq i \leq k$ avec k dans $[\![0;d-1]\!]$. On a, par formule de Leibniz et en tenant compte de $Qf = Q'$,

$$(k+1)!\, a_{d-k-1} = Q^{(k+1)}(0) = \sum_{i=0}^{k} \binom{k}{i} Q^{(i)}(0) f^{k-i}(0) \in \mathbf{Q}$$

et donc $(\mathbf{H}_{i+1})$ est vrai. Par principe de récurrence finie, $\boxed{a_0, \ldots, a_{d-1} \text{ sont rationnels.}}$

(c) Les deux questions précédentes, jointes au fait qu'un polynôme est à coefficients rationnels si et seulement si son polynôme réciproque l'est, donnent directement le résultat dans le cas où P n'admet pas 0 comme racine. Or, pour tout k dans $\mathbf{N}$, $P \in \mathbf{Q}[X] \iff X^k P \in \mathbf{Q}[X]$ et la somme $\sum_{i=1}^{d} \mu_i^n$ est indépendante de la multiplicité, éventuellement nulle, de la racine 0. Il en résulte $\boxed{P \in \mathbf{Q}[X] \iff \forall n \geq 1 \sum_{i=1}^{d} \mu_i^n \in \mathbf{Q}.}$

9. On note $N_n(A)$, $N_n(B)$, $N_n(P)$ et $N_n(Q)$ les quantités N_n définies à la question précédente relatives respectivement aux polynômes A, B et $\prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i\beta_j)$ et $\prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i - \beta_j)$. Pour n dans $\mathbf{N}^*$, on a donc $N_n(P) = N_n(A)N_n(B)$ et $N_n(Q) = \sum_{k=0}^{n} \binom{n}{k} N_k(A) N_{n-k}(B)$. Si A et B sont à coefficients rationnels, il résulte de la question précédente que les quantités $N_n(A)$ et $N_n(B)$ sont rationnelles pour tout entier n dans $\mathbf{N}^*$, et les formules précédentes montrent qu'il en va de même pour les quantités $N_n(P)$ et $N_n(Q)$. La question précédente permet donc de conclure que

$\boxed{\text{les polynômes } \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i\beta_j) \text{ et } \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i - \beta_j) \text{ sont aussi à coefficients rationnels.}}$

PARTIE III

10. Une valeur propre de M est racine de χ_M. De plus $\chi_M \neq 0$ et $\chi_M \in \mathbf{Q}[X]$. Il résulte du théorème spectral que toutes ses racines sont réelles et donc

toutes les valeurs propres de M sont totalement réelles.

11.(a) Puisque 1 est racine de $X-1$, il est totalement réel. Soit α et β totalement réels. On dispose de A et B deux polynômes unitaires de $\mathbf{Q}[X]$ n'ayant que des racines réelles et admettant respectivement α et β comme racines. Si β est non nul, B n'est pas un monôme, et donc le polynôme réciproque de B appartient à $\mathbf{Q}[X]$ et n'est pas constant. On note $\tilde{B}$ le polynôme unitaire associé à ce dernier. Ses racines sont les inverses des racines non nulles de B, donc toutes réelles, et $\frac{1}{\beta}$ en est racine. Le polynôme $(-1)^{\deg(A)}A(-X)$ est également unitaire, dans $\mathbf{Q}[X]$, à racines toutes réelles car opposées à celles de A, et $-\alpha$ en est racine. On introduit les polynômes P et Q définis à la question 9. D'après cette question ils sont unitaires et dans $\mathbf{Q}[X]$. De plus toutes leurs racines sont réelles puisque $\mathbf{R}$ est un corps, et parmi celles-ci il y a respectivement $\alpha\beta$ et $\alpha+\beta$. Il en résulte que

l'ensemble des nombres totalement réels est un sous-corps de $\mathbf{R}$.

(b) Avec les notations de la question précédente, $\tilde{B}$, P et Q sont à racines dans $\mathbf{R}_+$ puisque $\mathbf{R}_+^*$ est stable par inverse et $\mathbf{R}_+$ est stable par addition et multiplication. En particulier α est inclus dans $\mathbf{R}_+$ puisque c'est une racine de A. Il en résulte que

l'ensemble des nombres totalement positifs est inclus dans $\mathbf{R}^+$, est stable par addition, multiplication, et l'inverse d'un nombre totalement positif non nul est totalement positif.

12. Si x^2 est totalement positif, on dispose de P dans $\mathbf{Q}[X]$, unitaire, à racines toutes réelles positives, dont x^2. On note $Q = P(X^2)$, alors Q est dans $\mathbf{Q}[X]$, unitaire et admet x comme racine. Ses racines sont les racines carrées dans $\mathbf{C}$ de celles de P et sont donc toutes réelles. Réciproquement si x est totalement réel, on dispose de P dans $\mathbf{Q}[X]$, unitaire, à racines toutes réelles, dont x. On note $\mu_1, \ldots, \mu_d$ les racines de P comptées sans multiplicité. D'après la question 8c, pour tout n dans $\mathbf{N}^*$, $\sum_{k=1}^{d} \mu_k^n \in \mathbf{Q}$. Soit Q le polynôme $\prod_{k=1}^{d}(X-\mu_k^2)$. Pour tout n dans $\mathbf{N}^*$, on a $\sum_{k=1}^{d}(\mu_k^2)^n \in \mathbf{Q}$ et donc, d'après la question 8c, $Q \in \mathbf{Q}[X]$. Comme il est unitaire, admet x^2 comme racine et que toutes ses racines sont des carrés de nombres réels, donc positifs, on peut conclure que x est totalement réel si et seulement si x^2 est totalement positif.

PARTIE IV

13.(a) Soit X dans $\mathbf{Q}^d$ avec $X \neq 0$. On note $X = (x_1, \ldots, x_d)^{\mathrm{T}}$ de sorte qu'on a

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

et donc, en posant $u = \sum_{i=1}^{d} x_i z^{i-1}$, on a $B(X,X) = t(z^2u^2)$. D'après la question 11, u est totalement réel puisque z l'est. D'après la question 12, u^2 et z^2 sont totalement positifs, et donc leur produit aussi d'après la question 11. Comme u est un polynôme en z de degré strictement inférieur à d, il est non nul. Comme z non plus, u^2z^2 n'est pas nul et totalement positif. Par hypothèse sur t, $B(X,X) > 0$.

(b) Il résulte de la question précédente que, pour tout X dans $\mathbf{Q}^d$ non nul, SX est non-nul. Autrement dit l'application $X \mapsto SX$ de $\mathbf{Q}^d$ dans lui-même est injective, entre deux $\mathbf{Q}$-espaces vectoriels de même dimension finie. Elle est donc surjective. On dispose donc d'une famille libre de $\mathbf{Q}^d$ dans l'image

de S. Cette famille admet donc un déterminant non nul et est donc une famille libre de $\mathbf{R}^d$. Par conséquent S est surjective de $\mathbf{R}^d$ dans lui-même. Par dimension on en conclut que $\boxed{S \text{ est inversible.}}$

14. Par bilinéarité du produit matriciel, B est une forme bilinéaire. Elle est symétrique car S l'est et qu'une matrice de taille 1 est invariante par transposition. Par densité de $\mathbf{Q}$ dans $\mathbf{R}$, $\mathbf{Q}^d$ est dense dans $\mathbf{R}^d$ et donc la question précédente permet d'obtenir que $B(X,X)$ est positif pour tout X dans $\mathbf{R}^d$. Par conséquent S est une matrice symétrique réelle positive. Puisqu'elle est inversible d'après la question précédente, elle est définie positive et ainsi $\boxed{B \text{ est un produit scalaire sur } \mathbf{R}^d.}$

15.(a) Soit $(b_1, \dots, b_d)$ la base canonique de $\mathbf{R}^d$. Elle est en particulier à coefficients rationnels. On lui applique l'algorithme d'orthogonalisation de Gram-Schmidt en définissant une base $(e_1, \dots, e_d)$ de $\mathbf{R}^d$ par récurrence : $e_1 = b_1$ et, pour i dans $[\![2; d]\!]$, $e_i = b_i - \sum_{j<i} B(b_i, e_j)e_j$. Puisque la matrice S est à coefficients rationnels, $B(X,Y)$ est un rationnel dès que X et Y sont à coefficients rationnels. Une récurrence immédiate permet donc de conclure que

$\boxed{(e_1, \dots, e_d) \text{ est une base de } \mathbf{R}^d, \text{ avec } e_i \in \mathbf{Q}^d \text{ pour tout } i \text{ et } B(e_i, e_j) = 0 \text{ pour } i \neq j.}$

(b) On note Q la matrice dont les colonnes sont les vecteurs $(e_1, \dots, e_d)$ et $q_i = B(e_i, e_i)$. Alors Q est à coefficients rationnels et inversible puisque les e_i sont dans $\mathbf{Q}^d$ et forment une base. Si X et Y sont dans $\mathbf{R}^d$, on les décompose dans la base $(e_1, \dots, e_d)$: $X = \sum_{i=1}^{d} x_i e_i$ et $Y = \sum_{i=1}^{d} y_i e_i$. Autrement dit on a $X = Q \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$ et $Y = Q \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix}$. Par bilinéarité de B et la question précédent, on a $B(X,Y) = \sum_{i=1} q_i x_i y_i$. Par définition on a également

$$B(X,Y) = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}^{\mathrm{T}} Q^{\mathrm{T}} S Q \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix}$$

et donc en notant $Q^{\mathrm{T}}SQ = (a_i, j)$, il vient $B(X,Y) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i y_j$. En identifiant les deux formules pour $(x_1, \dots, x_d)$ et $(y_1, \dots, y_d)$ deux vecteurs quelconques de la base canonique de $\mathbf{R}^d$, on en déduit $Q^{\mathrm{T}}SQ = \mathrm{diag}(q_1, \dots, q_d)$. On pose alors $P = Q^{-1}$. Puisque Q est inversible, P l'est aussi. Son inverse peut se calculer à partir de son déterminant et sa comatrice, donc à partir de déterminant de sous-matrices de Q. Puisque Q est à coefficients rationnels, ces déterminants le sont aussi et donc P est à coefficients rationnels. De plus puisque les (e_i) et S sont à coefficients rationnels, les (q_i) sont rationnels, et ils sont strictement positifs car S est définie positive, i.e.

$\boxed{P \in \mathrm{GL}_d(\mathbf{Q}),\ (q_1, \dots, q_d) \in (\mathbf{Q}_+^*)^d \text{ et } S = P^{\mathrm{T}} \cdot \mathrm{diag}(q_1, \dots, q_d) \cdot P.}$

16. Il s'agit d'une matrice compagnon et donc, par exemple en faisant l'opération élémentaire $L_1 \leftarrow L_1 + \lambda L_2 + \cdots + \lambda^{d-1} L_{d-1}$ sur la matrice $\lambda I_d - M$, avec λ dans $\mathbf{R}$, puis en développant par rapport à la première ligne, $\boxed{\chi_M = Z.}$

17.(a) Soit i et j dans $[\![1; d]\!]$. Le coefficient d'indice (i,j) de SM est donné par $t(z^{i+j+1})$ si $j < d$ et par $\sum_{k=1}^{d} t a_{k-1} t(z^{i+k})$ si $j = d$. Puisque $Z(z) = 0$ et par hypothèse sur t, le second cas peut se récrire $t\left(z^{i+1} \sum_{k=1}^{d} a_{k-1} z^{k-1}\right)$, soit $t(z^{i+1+d})$. Le coefficient est donc $t(z^{i+j+1})$ dans tous les cas et ainsi

$\boxed{SM \text{ est symétrique.}}$

(b) D'après la question 15b, on a $S = R^{\mathrm{T}}R$, donc $SM = R^{\mathrm{T}}RM$ et $RMR^{-1} = (R)^{-\mathrm{T}}(SM)R^{-1}$. Puisque SM est symétrique $\boxed{RMR^{-1} \text{ est symétrique.}}$

18. D'après la question 3c on dispose de n dans $\mathbf{N}^*$ et de $M_1, \ldots, M_d$ dans $\mathscr{S}_n(\mathbf{Q})$, inversibles et telles que $M_i^2 = q_i I_n$ pour tout $1 \leq i \leq d$. Les matrices diagonales de taille nd données par

$$D = \mathrm{diag}(q_1, \ldots, q_1, \ldots, q_d, \ldots, q_d) \quad \text{et} \quad \Delta = \mathrm{diag}(q_1, \ldots, q_d, \ldots, q_1, \ldots, q_d)$$

expriment le même endomorphisme dans deux bases obtenues par permutation des vecteurs de l'une. Elles sont donc orthosemblables via une matrice Q dans $\mathrm{GL}_{nd}(\mathbf{Q})$ vérifiant $Q^{\mathrm{T}}Q = I_{nd}$ et $D = Q^{\mathrm{T}}\Delta Q$. On note $\tilde{Q}$ la matrice diagonale par blocs, dont les blocs diagonaux sont égaux à $M_1, \ldots, M_d$. On a donc $\tilde{Q}^2 = D$ et donc aussi $Q\tilde{Q}^{-2}Q^{\mathrm{T}} = \Delta^{-1}$. On note $\tilde{M}$ la matrice diagonale par blocs, dont les blocs diagonaux tous sont égaux à $\mathrm{diag}(q_1, \ldots, q_d)PMP^{-1}$. Remarquons que cette dernière matrice est à coefficients rationnels et est égale à $\mathrm{diag}(\sqrt{q_1}, \ldots, \sqrt{q_d})RMR^{-1}\mathrm{diag}(\sqrt{q_1}, \ldots, \sqrt{q_d})$, et donc $\tilde{M}$ est symétrique, d'après la question précédente. Enfin on pose

$$A = \tilde{Q}^{-1}\left(Q^{\mathrm{T}}\tilde{M}Q\right)\tilde{Q}^{-1}\,.$$

Sous cette forme on constate que A est symétrique puisque $\tilde{M}$ et les blocs diagonaux de de $\tilde{Q}$ le sont. Puisque toutes les matrices en jeu sont à coefficients rationnels, A l'est aussi. Enfin, en conjuguant par $Q\tilde{Q}^{-1}$, A est semblable à $Q\tilde{Q}^{-2}Q^{\mathrm{T}}\tilde{M}$ i.e. $\Delta^{-1}\tilde{M}$. Cette matrice est diagonale par blocs avec des blocs diagonaux tous égaux à PMP^{-1}, donc est semblable celle dont tous les blocs diagonaux sont égaux à M. Elle a donc même spectre que M, et particulier admet z comme valeur propre : $\boxed{A \in \mathscr{S}_n(\mathbf{Q}) \text{ et } z \in \mathrm{Sp}(A).}$