Corrigé de X-ENS MP 2020 Maths A

Alexandre Godard

Première partie

1) *Le polynôme caractéristique d'une matrice M de $\mathscr{M}_2(\mathbb{R})$ est $X^2 - \mathrm{Tr}(M)X + \det(M)$ donc on cherche une matrice vérifiant* $\mathrm{Tr}(M) = 0$ *et* $\det(M) = -2$.

$$\boxed{M = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}}$$

2) a. On a $\chi_M = X^2 - aX + b$ avec a et b dans $\mathbb{Q}$.
On a $\chi_M(\sqrt{3}) = 0$ donc $3 - a\sqrt{3} + b = 0$ donc $a\sqrt{3} = b + 3$.
Comme $\sqrt{3}$ est irrationnel, on a $a = 0$.
On déduit $b = -3$ et

$$\boxed{\chi_M = X^2 - 3}$$

b. Les possibilités pour n modulo 3 sont -1, 0 et 1 donc n^2 est égal à 0 ou 1 modulo 3.
c. Par l'absurde, on suppose qu'il existe un triplet (a, b, c) d'entiers premiers entre eux dans leur ensemble tels que $a^2 + b^2 = 3c^2$.
Les possibilités pour $a^2 + b^2$ modulo 3 sont :

a^2 \ b^2	0	1
0	0	1
1	1	2

Ainsi, comme $a^2 + b^2 \equiv 0$ [3], on a $a^2 \equiv 0$ [3] et $b^2 \equiv 0$ [3].
D'après la question précédente, $a^2 \equiv 0$ [3] entraîne $a \equiv 0$ [3].
On obtient de même $b \equiv 0$ [3].
On a $a = 3a'$ et $b = 3b'$ avec a' et b' dans $\mathbb{N}$.
On a donc $9a'^2 + 9b'^2 = 3c^2$ d'où $3(a'^2 + b'^2) = c^2$.
On a donc $3 \mid c^2$ donc $3 \mid c$ (question précédente ou lemme d'Euclide).
Ainsi 3 est un diviseur commun à a, b et c.
Contradiction.
d. On a $\chi_M = X^2 - 3$ donc $\mathrm{Tr}(M) = 0$.
De plus, M est symétrique donc il existe des rationnels a et b tels que

$$M = \begin{bmatrix} a & b \\ b & -a \end{bmatrix} .$$

On a $\det(M) = -3$ donc $-a^2 - b^2 = -3$ donc $a^2 + b^2 = 3$.
On écrit a et b sous forme de fractions irréductibles : $a = \dfrac{p}{q}$, $b = \dfrac{r}{s}$ et on obtient $(sp)^2 + (qr)^2 = 3(qs)^2$.
En divisant des deux côtés par $((sp) \wedge (qr) \wedge (qs))^2$, on obtient un triplet (u, v, w) d'entiers premiers entre eux tels que $u^2 + v^2 = 3w^2$ ce qui est en contradiction avec la question précédente.

3) a. On pose

$$\boxed{B = \begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix}}$$

Par produit pas blocs, on a

$$\begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix} \times \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} = \begin{bmatrix} A^2 & A \\ A & -A^2 \end{bmatrix}$$

et

$$\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \times \begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix} = \begin{bmatrix} A^2 & A \\ A & -A^2 \end{bmatrix}$$

donc la matrice B commute avec $\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$.

Toujours par produit par blocs,

$$B^2 = \begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix} \times \begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix} = \begin{bmatrix} A^2 + I_n & 0_n \\ 0_n & I_n + A^2 \end{bmatrix} = \begin{bmatrix} (q+1)I_n & 0_n \\ 0_n & (q+1)I_n \end{bmatrix} = (q+1)I_{2n} \ .$$

b. Pour toute matrice carrée, on pose $J(A) = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$ et $K(A) = \begin{bmatrix} A & I_n \\ I_n & -A \end{bmatrix}$.

On définit par récurrence une suite $(\mathscr{B}_n)_{n \in \mathbb{N}^*}$ de familles de matrices de $S_{2^{n-1}}(\mathbb{Q})$ en posant :

- $\mathscr{B}_1 = ([1])$,
- si $\mathscr{B}_n = (A_1, A_2, \ldots, A_m)$, $\mathscr{B}_{n+1} = (J(A_1), J(A_2), \ldots, J(A_m), K(A_m))$.

Par exemple, on a

$$\mathscr{B}_2 = \left(I_2, \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \quad \text{et} \quad \mathscr{B}_3 = \left(I_4, \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & 1 \end{bmatrix} \right) \ .$$

À l'aide des produits par blocs et de la question précédente, on obtient immédiatement par récurrence que pour tout $n \in \mathbb{N}^*$, les matrices M_1, M_2, $\ldots$, M_n de la famille $\mathscr{B}_n$ commutent deux à deux et vérifient $M_k^2 = kI_{2^{n-1}}$ pour tout $k \in [\![1, n]\!]$.

Ainsi, si $d \geqslant 1$, les matrices de la famille $\mathscr{B}_d$ répondent à la question avec $n = 2^{d-1}$.

c. Soient q_1, q_2, $\ldots$, q_d des rationnels strictement positifs.

On écrit pour tout $k \in [\![1, d]\!]$, $q_k = \dfrac{r_k}{s_k}$ avec r_k et s_k dans $\mathbb{N}^*$.

On pose $h = \max(r_1, r_2, \ldots, r_d, s_1, s_2, \ldots, s_d)$ et on applique la question précédente avec $d = h$.

On obtient une famille $(A_1, A_2, \ldots, A_h)$ de matrices de $S_{2^{h-1}}(\mathbb{Q})$ vérifiant $A_k^2 = kI_{2^{h-1}}$ pour tout $k \in [\![1, h]\!]$.

Cette égalité garantit l'inversibilité des matrices de la famille ainsi que l'égalité $\left(A_k^{-1}\right)^2 = \dfrac{1}{k} I_{2^{h-1}}$.

Par ailleurs les matrices A_k^{-1} sont symétriques $\left(\left(A_k^{-1}\right)^T = \left(A_k^T\right)^{-1} = A_k^{-1}\right)$ et à coefficients rationnels (formule d'inversion par transposition de la comatrice).

Si $i \in [\![1, d]\!]$, on pose $M_i = A_{r_i} A_{s_i}^{-1}$.

Le produit de deux matrices symétriques qui commutent est une matrice symétrique $\left((AB)^T = B^T A^T = BA = AB\right)$ donc les matrices M_i appartiennent à $S_{2^{h-1}}(\mathbb{Q})$.

Elles commutent deux à deux (si les matrices commutent, leurs inverses commutent et $A_k A_j^{-1} = A_j^{-1} A_k \iff A_j A_k = A_k A_j$).

Enfin, pour tout $i \in [\![1, d]\!]$, on a

$$M_i^2 = A_{r_i} A_{s_i}^{-1} A_{r_i} A_{s_i}^{-1} = A_{r_i}^2 \left(A_{s_i}^{-1}\right)^2 = \frac{r_i}{s_i} I_{2^{h-1}} \ .$$

4) a. On commence par montrer que $\sqrt[3]{2}$ est irrationnel.

Par l'absurde, on suppose qu'il existe a et b dans $\mathbb{N}^*$ premiers entre eux tels que $\left(\dfrac{a}{b}\right)^3 = 2$.

On obtient alors l'égalité $2b^3 = a^3$.

On a $b \mid a^3$ et b est premier avec a donc d'après le lemme de Gauss, $b \mid a$.

On obtient l'existence d'un entier naturel qui élevé au cube donne 2. Contradiction.

On effectue la division euclidienne de χ_M par X^3-2 : $\chi_M=(X^3-2)Q+R$ avec $Q\in\mathbb{Q}[X]$ et $R\in\mathbb{Q}[X]$ avec $\deg(R)\leqslant 2$.
Le réel $\sqrt[3]{2}$ étant une valeur propre de la matrice M, il annule χ_M.
On déduit qu'il est racine du polynôme R.
Par l'absurde, on suppose que R n'est pas le polynôme nul.
On effectue la division euclidienne de X^3-2 par R : $X^3-2=RQ'+R'$ avec $R'\in\mathbb{Q}[X]$ et $\deg(R')\leqslant 1$.
On déduit que $\sqrt[3]{2}$ est racine de R' qui est un polynôme à coefficients dans $\mathbb{Q}$ de degré inférieur ou égal à 1 : il est donc rationnel ce qui est une contradiction avec ce qui précède.
Ainsi, $R=0$ et $X^3-2\mid\chi_M$.

b. Comme X^3-2 divise χ_M, le nombre complexe $j\sqrt[3]{2}$ annule χ_M et il est donc valeur propre de χ_M.
Or, M est une matrice symétrique réelle donc d'après le théorème spectral ses valeurs propres sont toutes réelles.
Contradiction et résultat :

$$\boxed{\sqrt[3]{2} \text{ n'est pas valeur propre d'une matrice symétrique à coefficients dans } \mathbb{Q}.}$$

5) La matrice de permutation de $\mathscr{M}_n(\mathbb{Q})$

$$\Omega=\begin{bmatrix}0&1&0&\dots&0\\0&0&1&\ddots&\vdots\\\vdots&0&0&\ddots&0\\\vdots&&\ddots&\ddots&1\\1&\dots&\dots&0&0\end{bmatrix}$$

admet $\omega=e^{i\frac{2\pi}{n}}$ comme valeur propre (vecteur propre associé : $(1,\omega,\omega^2,\dots,\omega^{n-1})$).
Il s'agit d'une matrice orthogonale (les vecteurs colonnes forment une base orthonormée de $\mathbb{R}^n$) donc son inverse est égal à sa transposée :

$$\Omega^{-1}=\begin{bmatrix}0&\dots&\dots&0&1\\1&0&&\vdots&0\\0&1&\ddots&\vdots&\vdots\\\vdots&\ddots&\ddots&0&0\\0&\dots&0&1&0\end{bmatrix}$$

Cette matrice admet comme valeur propre $\frac{1}{\omega}=e^{-i\frac{2\pi}{n}}$ avec le même vecteur propre $(1,\omega,\omega^2,\dots,\omega^{n-1})$.
On déduit que la matrice $M=\dfrac{1}{2}(\Omega+{}^t\Omega)$ (qui est une matrice de $S_n(\mathbb{Q})$) admet comme valeur propre $\frac{e^{i\frac{2\pi}{n}}+e^{-i\frac{2\pi}{n}}}{2}=\cos\left(\frac{2\pi}{n}\right)$ (avec toujours le même vecteur propre).

$$M=\begin{bmatrix}0&1/2&0&\dots&1/2\\1/2&0&1/2&\ddots&\vdots\\0&1/2&0&\ddots&0\\\vdots&\ddots&\ddots&\ddots&1/2\\1/2&\dots&0&1/2&0\end{bmatrix}$$

Remarque. La matrice Ω^{-1} est la matrice compagnon du polynôme X^n-1.

Deuxième partie

6) On a

$$\begin{array}{rcl} Q & = & X^d\left(\left(\frac{1}{X}\right)^d + a_{d-1}\left(\frac{1}{X}\right)^{d-1} + \ldots + a_2\left(\frac{1}{X}\right)^2 + a_1\left(\frac{1}{X}\right) + a_0\right) \\ & = & 1 + a_{d-1}X + \ldots + a_2X^{d-2} + a_1X^{d-1} + a_0X^d \end{array}$$

Par ailleurs, on a

$$P = (X-\lambda_1)(X-\lambda_2)\ldots(X-\lambda_d)$$

donc

$$Q = X^d\left(\frac{1}{X}-\lambda_1\right)\left(\frac{1}{X}-\lambda_2\right)\ldots\left(\frac{1}{X}-\lambda_d\right) = (1-\lambda_1X)(1-\lambda_2X)\ldots(1-\lambda_dX)$$

$$\boxed{\begin{array}{rcl} Q & = & 1 + a_{d-1}X + \ldots + a_2X^{d-2} + a_1X^{d-1} + a_0X^d \\ & = & (1-\lambda_1X)(1-\lambda_2X)\ldots(1-\lambda_dX) \end{array}}$$

7) On considère l'application

$$\varphi : \left\{ \begin{array}{rcl} \mathbb{Q}[X]\setminus\{0\} & \to & \mathbb{Q}(X) \\ P & \mapsto & \dfrac{P'}{P} \end{array} \right.$$

(dérivée logarithmique).

Si P et Q sont des polynômes non nuls de $\mathbb{Q}[X]$, on a

$$\varphi(PQ) = \frac{(PQ)'}{PQ} = \frac{P'Q+PQ'}{PQ} = \frac{P'}{P} + \frac{Q'}{Q} = \varphi(P) + \varphi(Q)\ .$$

D'après la question précédente, on a $Q = (1-\lambda_1X)(1-\lambda_2X)\ldots(1-\lambda_dX)$ donc

$$\frac{Q'}{Q} = -\left(\frac{\lambda_1}{1-\lambda_1X} + \frac{\lambda_2}{1-\lambda_2X} + \ldots + \frac{\lambda_d}{1-\lambda_dX}\right)\ .$$

Pour tout $x \in \,]-1,1\,[$, la série $\sum x^n$ converge et on a

$$\frac{1}{1-x} = \sum_{n=0}^{+\infty} x^n\ .$$

On pose $r = \min\left(1, \frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \ldots, \frac{1}{\lambda_d}\right)$.
Si $k \in [\![\,1,d\,]\!]$, pour tout $x \in \,]-r,r\,[$, la série $\sum(\lambda_kx)^n$ converge et on a

$$\frac{1}{1-\lambda_kx} = \sum_{n=0}^{+\infty}(\lambda_kx)^n\ .$$

On déduit que pour tout $x \in \,]-r,r\,[$, la série $\sum(\lambda_1^{n+1}+\lambda_2^{n+1}+\ldots+\lambda_d^{n+1})x^n$ converge et que

$$\begin{array}{rcl} f(x) & = & -\left(\lambda_1\sum_{n=0}^{+\infty}(\lambda_1x)^n + \lambda_2\sum_{n=0}^{+\infty}(\lambda_2x)^n + \ldots + \lambda_d\sum_{n=0}^{+\infty}(\lambda_dx)^n\right) \\ & = & -\left(\sum_{n=0}^{+\infty}\lambda_1^{n+1}x^n + \sum_{n=0}^{+\infty}\lambda_2^{n+1}x^n + \ldots + \sum_{n=0}^{+\infty}\lambda_d^{n+1}x^n\right) \\ & = & -\sum_{n=0}^{+\infty}N_{n+1}x^n \end{array}$$

$$\boxed{f(x) = -\sum_{n=0}^{+\infty}N_{n+1}x^n}$$

8) a. On suppose que a_0, …, a_{d-1} sont des éléments de $\mathbb{Q}$ c'est-à-dire que $P \in \mathbb{Q}[X]$.
On a alors $Q \in \mathbb{Q}[X]$ d'après la question 6.

Par ailleurs $Q \neq 0$, donc $F = \frac{Q'}{Q} \in \mathbb{Q}(X)$.
On déduit que les dérivées successives de la fraction rationnelle F appartiennent à $\mathbb{Q}(X)$.
D'après la question précédente, pour tout $n \geqslant 1$, on a $N_n = -\frac{f^{(n-1)}(0)}{(n-1)!}$ donc $N_n \in \mathbb{Q}$.

b. On suppose que $N_n \in \mathbb{Q}$ pour tout $n \geqslant 1$.
D'après la question 7, pour tout $x \in \left]-r, r\right[$, on a

$$Q'(x) = -Q(x) \sum_{n=0}^{+\infty} N_{n+1} x^n = -\sum_{n=0}^{d} a_{d-n} x^n \times \sum_{n=0}^{+\infty} N_{n+1} x^n$$

(on a posé $a_d = 1$). D'après le théorème du produit de Cauchy, la série entière $\sum c_n x^n$ où $c_n = \sum_{i=0}^{n} a_{d-i} N_{n-i+1}$ a un rayon de convergence supérieur ou égal à r et pour tout $x \in \left]-r, r\right[$, on a

$$\sum_{n=0}^{d-1} (n+1) a_{d-n-1} x^n = \sum_{n=0}^{+\infty} -c_n x^n \ .$$

Par unicité du développement en série entière, on a $(n+1)a_{d-n-1} = -\sum_{i=0}^{n} a_{d-i} N_{n+1-i}$ pour tout $n \in [\![0, d-1]\!]$.
Ces égalités permettent de montrer par récurrence forte finie que $a_{d-k} \in \mathbb{Q}$ pour tout $k \in [\![0, d]\!]$.
<u>Initialisation</u>
On a $a_d = 1$ donc $a_d \in \mathbb{Q}$.
<u>Hérédité</u>
Soit $k \in [\![0, d-1]\!]$.
On suppose qu'on a $a_{d-i} \in \mathbb{Q}$ pour tout $i \in [\![0, k]\!]$.
D'après ce qui précède, on a

$$(k+1) a_{d-(k+1)} = -\sum_{i=0}^{k} a_{d-i} N_{k+1-i} \ .$$

Pour tout $i \in [\![0, k]\!]$, on a $a_{d-i} \in \mathbb{Q}$ (hypothèse de récurrence) et $N_{n+1-i} \in \mathbb{Q}$ (hypothèse de départ) donc $a_{d-(k+1)} \in \mathbb{Q}$.
<u>Conclusion</u>
D'après le principe de récurrence forte, on a $a_{d-k} \in \mathbb{Q}$ pour tout $k \in [\![0, d]\!]$.

Remarque1. Seule l'hypothèse $N_n \in \mathbb{N}$ pour tout $n \in [\![1, d]\!]$ est utilisée.
Remarque2. Dans cette question, on démontre à l'aide d'une technique d'analyse les identités de Newton *qui permettent d'écrire les fonctions symétriques élémentaires des racines (donc les coefficients du polynôme d'après les relations coefficients-racines) en fonction des sommes de* Newton *N_n.*

c. On écrit la forme développée de P : $P = a_0 + a_1 X + a_2 X^2 + \ldots + a_{d-1} X^{d-1} + X^d$ et on applique les questions 8a et 8b.

9) On suppose que les polynômes A et B sont à coefficients rationnels.
Le polynôme $P = \prod_{(i,j) \in [\![1,n]\!] \times [\![1,m]\!]} (X - \alpha_i \beta_j)$ est unitaire et ses racines sont les $\alpha_i \beta_j$ (pour $(i,j) \in [\![1,n]\!] \times [\![1,m]\!]$).
Pour tout $k \in \mathbb{N}$, on note $S_k = \sum_{(i,j) \in [\![1,n]\!] \times [\![1,m]\!]} (\alpha_i \beta_j)^k$ et on a

$$S_k = \left(\sum_{i=1}^{n} \alpha_i^k \right) \times \left(\sum_{j=1}^{n} \beta_j^k \right) \ .$$

Les polynômes A et B sont à coefficients rationnels donc d'après la question 8, on a $\sum_{i=1}^{n} \alpha_i^k \in \mathbb{Q}$ et $\sum_{j=1}^{n} \beta_j^k \in \mathbb{Q}$.

On déduit $S_k \in \mathbb{Q}$.
Pour tout $k \geqslant 1$, on a $S_k \in \mathbb{Q}$ donc d'après la question 8, le polynôme P est à coefficients rationnels.

Le polynôme $Q = \prod_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}(X - (\alpha_i + \beta_j))$ est unitaire et ses racines sont les $\alpha_i + \beta_j$ (pour $(i,j) \in [\![1,n]\!] \times [\![1,m]\!]$).
Pour tout $k \in \mathbb{N}$, on note $\sigma_k = \sum_{(i,j)\in[\![1,n]\!]\times[\![1,m]\!]}(\alpha_i + \beta_j)^k$ et on a d'après la formule du binôme,

$$\begin{aligned}
\sigma_k &= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{q=0}^{k}\binom{k}{q}\alpha_i^{k-q}\beta_j^q \\
&= \sum_{i=1}^{n}\sum_{q=0}^{k}\sum_{j=1}^{n}\binom{k}{q}\alpha_i^{k-q}\beta_j^q \\
&= \sum_{i=1}^{n}\sum_{q=0}^{k}\binom{k}{q}\alpha_i^{k-q}\sum_{j=1}^{n}\beta_j^q \\
&= \sum_{q=0}^{k}\sum_{i=1}^{n}\binom{k}{q}\alpha_i^{k-q}\sum_{j=1}^{n}\beta_j^q \\
&= \sum_{q=0}^{k}\binom{k}{q}\sum_{i=1}^{n}\alpha_i^{k-q}\sum_{j=1}^{n}\beta_j^q
\end{aligned}$$

Les polynômes A et B sont à coefficients rationnels donc d'après la question 8, pour tout $q \in [\![0,n]\!]$ on a $\sum_{i=1}^{n}\alpha_i^{k-q} \in \mathbb{Q}$ et $\sum_{j=1}^{n}\beta_j^q \in \mathbb{Q}$.
Comme $\binom{k}{q} \in \mathbb{N}$ pour tout $q \in [\![0,n]\!]$, on déduit $\sigma_k \in \mathbb{Q}$.
Pour tout $k \geqslant 1$, on a $\sigma_k \in \mathbb{Q}$ donc d'après la question 8, le polynôme P est à coefficients rationnels.

Remarque. Cette question peut être utilisée pour montrer que le produit et la somme de deux nombres algébriques α et β sont algébriques. De façon plus abstraite, on peut aussi utiliser le fait que l'extension de corps $\mathbb{Q}(\alpha,\beta) : \mathbb{Q}$ est de degré fini.

Troisième partie

Remarque. L'hypothèse « non nul » pour le polynôme est inutile, elle découle du fait que le polynôme a toutes ses racines dans $\mathbb{R}$.

10) Soit α une valeur propre de M.
On considère le polynôme caractéristique χ_M de la matrice M.
La matrice M étant à coefficients dans $\mathbb{Q}$, le polynôme χ_M est à coefficients dans $\mathbb{Q}$ (et il est non nul car unitaire).
Le nombre complexe α est une racine de χ_M et d'après le théorème spectral toutes les racines de χ_M sont dans $\mathbb{R}$.
Ainsi, α est totalement réel.

11) a. On note $\mathscr{R}$ l'ensemble de nombres totalement réels.
Il est immédiat que $\mathscr{R} \subset \mathbb{R}$.
$0 \in \mathscr{R}$ grâce au polynôme X.
Soient α et β dans $\mathscr{R}$.
Par hypothèse, il existe un polynôme A (resp. B) non nul à coefficients rationnels tel que α (resp. β) est une racine de A (resp. B) et tel que toutes les racines de A (resp. B) sont dans $\mathbb{R}$.
Quitte à multiplier par un rationnel non nul, on peut supposer que les polynômes A et B sont unitaires.
On note $\alpha_1 = \alpha$, α_2, …, α_n les racines de A et $\beta_1 = \beta$, β_2, …, β_m les racines de B répétées autant de fois

que leur multiplicité (ces nombres sont réels).
D'après le théorème de D'ALEMBERT-GAUSS, les polynômes A et B sont scindés sur $\mathbb{C}$ donc on a

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

D'après la question 9, le polynôme $P = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - (\alpha_i + \beta_j))$ est à coefficients rationnels.
Le nombre complexe $\alpha + \beta$ est une racine de P et toutes les racines de P sont réelles (il s'agit des $\alpha_i + \beta_j$ pour $(i, j) \in [\![1, n]\!] \times [\![1, m]\!]$).
Ainsi $\alpha + \beta \in \mathscr{R}$ et $\mathscr{R}$ est stable par somme.
Soit $\alpha \in \mathscr{R}$.
En notant P un polynôme convenable pour α, on constate immédiatement que le polynôme $P(-X)$ convient pour $-\alpha$.
Ainsi $-\alpha \in \mathscr{R}$.
Ainsi $\mathscr{R}$ est un sous-groupe de $(\mathbb{R}, +)$.

Le complexe 1 appartient à $\mathscr{R}$ (polynôme $X - 1$).
De même que précédemment on montre la stabilité par produit en utilisant la question 9.
Ainsi $\mathscr{R}$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
Soit α est un réel non nul appartenant à $\mathscr{R}$.
On considère P un polynôme qui valide l'appartenance de α à $\mathscr{R}$.
De même qu'à la question 6, on considère le polynôme réciproque de P, $Q = X^n P(\frac{1}{X})$ (avec $n = \deg(P)$: il s'agit de symétriser les coefficients).
Pour tout $z \in \mathbb{C}^*$, on a $P(z) = 0 \iff Q(\frac{1}{z}) = 0$.
On a donc Q est un polynôme non nul à coefficients rationnels, $Q(\frac{1}{\alpha}) = 0$ et toutes les racines de Q sont dans $\mathbb{R}$ (il s'agit des inverses des racines non nulles de P). Ainsi $\frac{1}{\alpha}$ appartient à $\mathscr{R}$.
0 peut être racine de P mais pas de Q car le coefficient constant de Q est égal au coefficient dominant de P.
Le degré de Q est égal au degré de P moins la multiplicité de 0 dans P.
Ainsi,

$$\boxed{\mathscr{R} \text{ est un sous-corps de } (\mathbb{R}, +, \times)}$$

b. On note $\mathscr{R}_+$ l'ensemble de nombres totalement positifs.
Soit α un nombre totalement positif.
Il existe un polynôme P non nul à coefficients dans $\mathbb{Q}$ tel que α est racine de P et toutes les racines de P sont dans $\mathbb{R}_+$.
Le complexe α étant lui-même une racine de P, il appartient à $\mathbb{R}_+$ et on vient de prouver $\mathscr{R}_+ \subset \mathbb{R}_+$.
Soient α et β dans $\mathscr{R}_+$.
Par hypothèse, il existe un polynôme A (resp. B) non nul à coefficients rationnels tel que α (resp. β) est une racine de A (resp. B) et tel que toutes les racines de A (resp. B) sont dans $\mathbb{R}_+$.
On note $\alpha_1 = \alpha$, α_2, …, α_n les racines de A et $\beta_1 = \beta$, β_2, …, β_m les racines de B répétées autant de fois que leur multiplicité (ces nombres sont réels).
D'après le théorème de D'ALEMBERT-GAUSS, les polynômes A et B sont scindés sur $\mathbb{C}$ donc on a

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

D'après la question 9, le polynôme $P = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - (\alpha_i + \beta_j))$ est à coefficients rationnels.
Le nombre complexe $\alpha + \beta$ est une racine de P et toutes les racines de P sont réelles positives (il s'agit des $\alpha_i + \beta_j$ pour $(i, j) \in [\![1, n]\!] \times [\![1, m]\!]$).
Ainsi $\alpha + \beta \in \mathscr{R}_+$ et $\mathscr{R}_+$ est stable par addition.

Soient α et β dans $\mathscr{R}_+$.
Par hypothèse, il existe un polynôme A (resp. B) non nul à coefficients rationnels tel que α (resp. β) est une racine de A (resp. B) et tel que toutes les racines de A (resp. B) sont dans $\mathbb{R}_+$.
Quitte à multiplier par un rationnel non nul, on peut supposer que les polynômes A et B sont unitaires.
On note $\alpha_1 = \alpha$, α_2, $\dots$, α_n les racines de A et $\beta_1 = \beta$, β_2, $\dots$, β_m les racines de B répétées autant de fois que leur multiplicité (ces nombres sont des réels positifs).
D'après le théorème de d'Alembert-Gauss, les polynômes A et B sont scindés sur $\mathbb{C}$ donc on a

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

D'après la question 9, le polynôme $P = \prod_{i=1}^{n}\prod_{j=1}^{m}(X - \alpha_i\beta_j)$ est à coefficients rationnels.
Le nombre complexe $\alpha\beta$ est une racine de P et toutes les racines de P sont réelles positives (il s'agit des $\alpha_i\beta_j$ pour $(i,j) \in [\![1, n]\!] \times [\![1, m]\!]$).
Ainsi $\alpha\beta \in \mathscr{R}_+$ et $\mathscr{R}_+$ est stable par addition.

Soit α est un nombre totalement positif non nul.
On considère P un polynôme qui valide l'appartenance de α à $\mathscr{R}_+$.
De même qu'à la question 6, on considère le polynôme réciproque de P, $Q = X^n P(\frac{1}{X})$ (avec $n = \deg(P)$: il s'agit de symétriser les coefficients).
Pour tout $z \in \mathbb{C}^*$, on a $P(z) = 0 \iff Q(\frac{1}{z}) = 0$.
On a donc Q est un polynôme non nul à coefficients rationnels, $Q(\frac{1}{\alpha}) = 0$ et toutes les racines de Q sont dans $\mathbb{R}_+$ (il s'agit des inverses des racines non nulles de P). Ainsi $\frac{1}{\alpha}$ appartient à $\mathscr{R}_+$.

12) On suppose que x^2 est totalement positif.
Il existe donc P un polynôme non nul à coefficients rationnels qui possède x^2 comme racine et tel que toutes les racines de P sont des réels positifs.
On pose $Q = P(X^2)$.
Le réel x est racine du polynôme Q qui est un polynôme non nul à coefficients rationnels.
Pour tout $z \in \mathbb{C}$, on a z est racine de Q si et seulement si z^2 est racine de P.
Ainsi, si z est une racine de Q, il existe une racine a de P tel que $z^2 = a$.
Par hypothèse, a est un réel positif donc $z = -\sqrt{a}$ ou $z = \sqrt{a}$: z est réel.
On déduit que x est totalement réel.

Réciproquement, on suppose que x est totalement réel.
Il existe donc P un polynôme non nul à coefficients rationnels qui possède x comme racine et tel que toutes les racines de P sont réelles.
Quitte à multiplier par un rationnel non nul, on peut supposer que le polynôme P est unitaire.
On note $\alpha_1 = x$, α_2, $\dots$, α_d les racines de P répétées autant de fois que leur multiplicité (ces racines sont réelles).
D'après le théorème de d'Alembert-Gauss, on a $P = (X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_d)$.
On pose $Q = (X - \alpha_1^2)(X - \alpha_2^2)\dots(X - \alpha_d^2)$.
Le polynôme Q est non nul.
Les sommes de Newton associées à ce polynôme sont les $N'_n = \alpha_1^{2n} + \alpha_2^{2n} + \dots + \alpha_d^{2n}$.
D'après la question 8a appliquée au polynôme P, on a $N'_n \in \mathbb{Q}$ pour tout $n \geqslant 1$.
On applique ensuite la question 8b au polynôme Q pour obtenir que Q est à coefficients rationnels.
Le complexe x^2 est une racine de Q et les racines de Q sont des réels positifs (il s'agit des carrés des racines de P).
On déduit que x^2 est totalement positif.

Ainsi pour tout $x \in \mathbb{C}$, on a

$$\boxed{x \text{ est totalement réel si et seulement si } x^2 \text{ est totalement positif.}}$$

Quatrième partie

13) a. Soit $X = (q_1, q_2, \ldots, q_d) \in \mathbb{Q}^d$, $X \neq 0$.

On a $SX = \left(\sum_{j=1}^{d} t(z^{i+j})q_j\right)_{1 \leqslant i \leqslant d}$ donc

$$X^T SX = \sum_{i=1}^{d} q_i \times \sum_{j=1}^{d} t(z^{i+j})q_j = \sum_{i=1}^{d}\sum_{j=1}^{d} q_i t(z^{i+j})q_j \ .$$

D'après la propriété de $\mathbb{Q}$-linéarité de l'application t, on a

$$B(X,X) = t\left(\sum_{i=1}^{d}\sum_{j=1}^{d} q_i z^{i+j} q_j\right) = t\left(\sum_{i=1}^{d}\sum_{j=1}^{d} q_i z^i q_j z^j\right) = t\left(\left(\sum_{i=1}^{d} q_i z^i\right)\left(\sum_{j=1}^{d} q_j z^j\right)\right) = t\left(\left(\sum_{k=1}^{d} q_k z^k\right)^2\right) \ .$$

Sachant qu'un nombre rationnel q est totalement réel (polynôme $X - q$), on a d'après la question 11a, $\sum_{k=1}^{d} q_k z^k \in \mathscr{R}$.

D'après la question 12, $\left(\sum_{k=1}^{d} q_k z^k\right)^2$ est totalement positif donc d'après l'hypothèse de positivité de l'application t, $B(X,X) \geqslant 0$.

Pour montrer $B(X,X) > 0$, il reste à montrer $\left(\sum_{k=1}^{d} q_k z^k\right)^2 \neq 0$.

Par l'absurde, on suppose $\sum_{k=1}^{d} q_k z^k = 0$.

On a $z \neq 0$ donc $\sum_{k=1}^{d} q_k z^{k-1} = 0$.

On a $X \neq 0$, donc en posant $\ell = \max(\{k \in [\![1,d]\!] \ / \ q_k \neq 0\})$, on obtient en divisant la relation ci-dessus par q_ℓ un polynôme de $\mathbb{Q}[X]$ unitaire de degré $\ell - 1$ qui annule z ce qui contredit la minimalité de d.

On a donc

$$\boxed{B(X,X) > 0}$$

b. Par l'absurde, on suppose que la matrice S n'est pas inversible.

On a donc $\mathrm{Ker}(S) \neq \{0_{\mathbb{Q}^d}\}$ donc il existe $X \in \mathbb{Q}^d$, $X \neq 0$ tel que $SX = 0_{\mathbb{Q}^d}$.

On déduit $B(X,X) = 0$, ce qui est en contradiction avec la sous-question précédente.

$$\boxed{\text{La matrice } S \text{ est inversible.}}$$

14) Pour tous X et Y dans $\mathbb{R}^d$, on a $B(X,Y) \in \mathbb{R}$.

Soient X et Y dans $\mathbb{R}^d$.

On a $B(X,Y)^T = Y^T S^T X = Y^T SX = B(Y,X)$ et $B(X,Y) \in \mathbb{R}$ donc $B(X,Y)^T = B(X,Y)$.

On a donc $B(X,Y) = B(Y,X)$.

L'application B est symétrique.

Soient X, Y et Y' dans $\mathbb{R}^d$.

On a $B(X, Y + Y') = X^T S(Y + Y') = X^T SY + X^T SY' = B(X,Y) + B(X,Y')$.

Soient X et Y dans $\mathbb{R}^d$ et $\lambda \in \mathbb{R}$.

On a $B(X, \lambda Y) = X^T S(\lambda Y) = \lambda X^T SY = \lambda B(X,Y)$.

L'application B est linéaire à droite.

La matrice est une matrice symétrique réelle donc d'après le théorème spectral, elle est diagonalisable sur $\mathbb{R}$ dans une matrice orthogonale.

On note λ_1, λ_2, $\ldots$, λ_d les valeurs propres de S (répétées avec multiplicité) et $D = \mathrm{Diag}(\lambda_1, \lambda_2, \ldots, \lambda_d)$.

D'après la question 13b, la matrice S est inversible donc on a $\lambda_k \neq 0$ pour tout $k \in [\![1,d]\!]$.

Montrons que $\lambda_k > 0$ pour tout $k \in [\![1,d]\!]$.

Par l'absurde, on suppose qu'il existe $i \in [\![1,d]\!]$ tel que $\lambda_i < 0$.

On considère $X_i = (x_1, x_2, \ldots, x_d) \in \mathbb{R}^d$ un vecteur propre de S associé à la valeur propre λ_i.
On a $B(X_i, X_i) = X_i^T S X_i = \lambda_i X_i^T X_i = \lambda_i \sum_{k=1}^{d} x_k^2 < 0$.
L'application

$$\left\{ \begin{array}{ccc} \mathbb{R}^d & \to & \mathbb{R} \\ X & \mapsto & B(X, X) \end{array} \right.$$

est polynomiale donc continue.
On a donc $B(X, X) < 0$ dans un voisinage U de X_i.
La partie $\mathbb{Q}^d$ est dense dans $\mathbb{R}^d$ donc il existe $Y_i \in \mathbb{Q}^d$ dans U.
On a $B(Y_i, Y_i) < 0$ ce qui est en contradiction avec la question 13a.
Ainsi, on a $\lambda_k > 0$ pour tout $k \in [\![1, d]\!]$.
Si $X \in \mathbb{R}^d$, on note $PX = (y_1, y_2, \ldots, y_d)$ et on a

$$B(X, X) = X^T P^T D P X = (PX)^T D (PX) = \sum_{k=1}^{d} \lambda_k y_k^2 \ .$$

Ainsi, pour tout $X \in \mathbb{R}^d$, on a $B(X, X) \geqslant 0$ et $B(X, X) = 0 \iff PX = 0_{\mathbb{R}^d} \iff X = 0_{\mathbb{R}^d}$ (inversibilité de P) : l'application B est définie positive.
L'application B est symétrique, linéaire à droite définie positive donc

$$\boxed{\text{L'application } B \text{ est un produit scalaire sur } \mathbb{R}^d.}$$

15) a. On considère la base canonique de $\mathbb{R}^d$ et on lui applique le procédé d'orthogonalisation de Gram-Schmidt.
Les vecteurs de la base canonique de $\mathbb{R}^d$ appartiennent à $\mathbb{Q}^d$ et $B(X, Y) \in \mathbb{Q}$ pour tous X et Y dans $\mathbb{Q}^d$ donc les vecteurs qui apparaissent dans cet algorithme sont tous des vecteurs de $\mathbb{Q}^d$.
N.B. On ne procède pas à l'étape finale de normalisation des vecteurs.
On obtient donc une base $(e_1, e_2, \ldots, e_d)$ de $\mathbb{R}^d$ orthogonale au sens du produit scalaire B et telle que $e_k \in \mathbb{Q}^d$ pour tout $k \in [\![1, d]\!]$.

b. Soit $X = (x_1, x_2, \ldots, x_d)$ et $Y = (y_1, y_2, \ldots, y_d)$ des vecteurs de $\mathbb{R}^d$.
On considère $X' = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ (resp. $Y' = (\beta_1, \beta_2, \ldots, \beta_d)$) les coordonnées du vecteur X (resp. Y) dans la base $(e_1, e_2, \ldots, e_d)$.
On a donc par bilinéarité de B,

$$B(X, Y) = B\left(\sum_{i=1}^{d} \alpha_i . e_i , \sum_{j=1}^{d} \alpha_j . e_j \right) = \sum_{i=1}^{d} \sum_{j=1}^{d} \alpha_i \beta_j B(e_i, e_j) \ .$$

On a $B(e_i, e_j) = 0$ pour tous $i \neq j$ donc $B(X, Y) = \sum_{k=1}^{d} q_k \alpha_k \beta_k$ où $q_k = B(e_k, e_k)$.
On a $e_k \in \mathbb{Q}^d$ donc $q_k \in \mathbb{Q}$ et d'après la question 13a, $q_k > 0$.
Ainsi, on a $X^T S Y = X'^T D Y'$ où $D = \mathrm{Diag}(q_1, \ldots, q_d)$.
On note Q la matrice de passage de la base canonique de $\mathbb{R}^d$ à la base $(e_1, e_2, \ldots, e_d)$.
Les vecteurs e_1, e_2, $\ldots$, e_d appartiennent à $\mathbb{Q}^d$ donc $Q \in \mathrm{GL}_q(\mathbb{Q})$.
D'après le théorème de changement de coordonnées, on a $X = QX'$ et $Y = QY'$.
On pose $P = Q^{-1}$ et on a $P \in \mathrm{GL}_q(\mathbb{Q})$ et $X' = PX$, $Y' = PY$.
On a donc $X^T S Y = X^T P^T D P Y$.
On pose $A = P^T D P$ et on a $X^T S Y = X^T A Y$ pour tous X et Y dans $\mathbb{R}^d$.
On fixe i et j dans $[\![1, d]\!]^2$ et on évalue cette égalité avec $X = (\delta_k^i)_{1 \leqslant k \leqslant d}$ et $Y = (\delta_k^j)_{1 \leqslant k \leqslant d}$ pour obtenir $S_{ij} = A_{ij}$($\delta_k^q = 1$ si $k = q$, 0 sinon).
On a donc $S = A$ c'est-à-dire

$$\boxed{S = P^T D P}$$

16) Soit $\lambda \in \mathbb{R}$.

$$\chi_M(\lambda) = \begin{vmatrix} \lambda & 0 & \dots & 0 & -a_0 \\ -1 & \lambda & \ddots & \vdots & -a_1 \\ 0 & -1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \lambda & -a_{n-2} \\ 0 & \dots & 0 & -1 & \lambda - a_{d-1} \end{vmatrix} .$$

On ajoute $\lambda L_2 + \lambda^2 L_3 + \dots \lambda^{d-1} L_d$ à L_1 et on obtient

$$\chi_M(\lambda) = \begin{vmatrix} 0 & 0 & \dots & 0 & Z(\lambda) \\ -1 & \lambda & \ddots & \vdots & -a_1 \\ 0 & -1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \lambda & -a_{n-2} \\ 0 & \dots & 0 & -1 & \lambda - a_{d-1} \end{vmatrix} .$$

Par développement par rapport à la première ligne, on obtient

$$\chi_M(\lambda) = (-1)^{d-1} Z(\lambda) \begin{vmatrix} -1 & \lambda & 0 & \dots & 0 \\ 0 & -1 & \lambda & \ddots & \vdots \\ \vdots & \ddots & -1 & \ddots & 0 \\ \vdots & & \ddots & \ddots & \lambda \\ 0 & \dots & \dots & 0 & -1 \end{vmatrix} = (-1)^{d-1} Z(\lambda) \times (-1)^{d-1} = Z(\lambda) .$$

Le polynôme $\chi_M - Z$ admet une infinité de racines donc il s'agit du polynôme nul.
On a donc

$$\boxed{\chi_M = Z}$$

Remarque. La matrice M est appelée matrice compagnon du polynôme Z. En notant $F = \mathrm{Vect}(1, z, z^2, \dots, z^{d-1})$, il s'agit de la matrice représentative de l'endomorphisme de F $\alpha \mapsto z\alpha$ dans la base (au sens des $\mathbb{Q}$-espaces vectoriels) $\mathscr{B} = (1, z, z^2, \dots, z^{d-1})$.

17) a. Soit $(i, j) \in [\![1, d]\!]^2$.
D'après la formule du produit matriciel, on a

$$(SM)_{ij} = \sum_{k=1}^{d} S_{ik} M_{kj} .$$

Si $j \in [\![1, d-1]\!]$, on a $M_{kj} = 1$ si $k = j+1$ et 0 sinon donc $(SM)_{ij} = S_{i,j+1} = t(z^{i+j+1})$.
Si $j = d$, on a $M_{kj} = a_{k-1}$ donc par $\mathbb{Q}$-linéarité de t,

$$(SM)_{ij} = \sum_{k=1}^{d} t\left(z^{i+k}\right) a_{k-1} = \sum_{k=0}^{d-1} a_k t\left(z^{i+k+1}\right) = t\left(\sum_{k=0}^{d-1} a_k z^{i+k+1}\right) = t\left(z^{i+1} \sum_{k=0}^{d-1} a_k z^k\right) .$$

On a $Z(z) = 0$ donc $\sum_{k=0}^{d-1} a_k z^k = z^d$ donc

$$(SM)_{ij} = t\left(z^{i+1} \times z^d\right) = t\left(z^{i+d+1}\right) = t\left(z^{i+j+1}\right) .$$

Ainsi, pour tout $(i, j) \in [\![1, d]\!]^2$, on a $(SM)_{ij} = t\left(z^{i+j+1}\right) = (SM)_{ji}$ donc

$$\boxed{\text{La matrice } SM \text{ est symétrique}}$$

b. D'après la question 15b, on a

$$SM = P^T\text{Diag}(q_1, \dots, q_d)PM = P^T\text{Diag}(\sqrt{q_1}, \dots, \sqrt{q_d})\text{Diag}(\sqrt{q_1}, \dots, \sqrt{q_d})PM = R^TRM$$

donc

$$RMR^{-1} = \left(R^T\right)^{-1}(SM)R^{-1} = \left(R^{-1}\right)^T(SM)R^{-1}$$

et comme la matrice SM est symétrique (sous-question précédente),

$$\left(RMR^{-1}\right)^T = \left(R^{-1}\right)^T(SM)^TR^{-1} = \left(R^{-1}\right)^T(SM)R^{-1} = RMR^{-1}$$

$$\boxed{\text{La matrice } RMR^{-1} \text{ est symétrique.}}$$

18) *La matrice RMR^{-1} est symétrique et a même polynôme caractéristique que M. Cependant, elle n'est pas à coefficients rationnels à cause des racines carrées. Les nombres rationnels q_i n'ont pas de racine carrées dans $\mathbb{Q}$ mais ils en ont dans des anneaux de matrices à coefficients dans $\mathbb{Q}$. De plus ces racines carrées peuvent être choisies symétriques d'après la question 3c. On reprend donc le principe du raisonnement de la question 15b en utilisant des matrices par blocs.*

On a q_1, q_2, …, q_d des rationnels strictement positifs.
D'après la question 3c, il existe $n \in \mathbb{N}^*$ et des matrices M_1, M_2, …, $M_d \in S_n(\mathbb{Q})$ telles que $M_i^2 = q_iI_n$ pour tout $i \in [\![1, d]\!]$.
On note $D = \text{Diag}(q_1, \dots, q_d)$ et pour toute matrice $A \in \mathscr{M}_d(\mathbb{R})$, on note A' la matrice de $\mathscr{M}_{nd}(\mathbb{R})$ obtenue en remplaçant chaque coefficient a_{ij} par un bloc $a_{ij}I_n$. On remarque que :

- pour tous A et B dans $\mathscr{M}_d(\mathbb{R})$, $(AB)' = A'B'$ (théorème du produit par blocs) et en particulier si A est inversible, alors A' est inversible,
- si A est une matrice de $S_d(\mathbb{Q})$, alors A' est une matrice de $S_{nd}(\mathbb{Q})$.

Enfin, on note H la matrice diagonale par blocs

$$H = \begin{bmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_d \end{bmatrix}$$

qui appartient à $S_{nd}(\mathbb{Q})$ et qui est inversible puisque toutes les matrices M_i le sont.
D'après la question 15b et le théorème du produit par blocs, on a

$$S'M' = P'^TD'P'M' = P'^TH^2P'M' = U^TUM'$$

où $U = HP'$ donc

$$UM'U^{-1} = \left(U^T\right)^{-1}(S'M')U^{-1} = \left(U^{-1}\right)^T(SM)'U^{-1}$$

et comme la matrice $(SM)'$ est symétrique (car SM l'est d'après la question 17a),

$$\left(UM'U^{-1}\right)^T = \left(U^{-1}\right)^T(SM)'^TU^{-1} = \left(U^{-1}\right)^T(SM)'U^{-1} = UMU^{-1}$$

donc la matrice $UM'U^{-1}$ appartient à $S_{nd}(\mathbb{Q})$.
Le réel z est une valeur propre de la matrice M : on considère un vecteur propre associé $X = (\alpha_1, \alpha_2, \dots, \alpha_d)$.
Par produit par blocs, le vecteur de $\mathbb{R}^{nd}$ obtenu en répétant n fois chaque coordonnée

$$Y = (\alpha_1, \alpha_1, \dots, \alpha_1, \alpha_2, \alpha_2, \dots, \alpha_2, \dots, \alpha_d, \alpha_d, \dots, \alpha_d)$$

vérifie $M'Y = zY$.
On déduit que z est valeur propre de la matrice M'.

La matrice $UM'U^{-1}$ est semblable à la matrice M' donc elle a même polynôme caractéristique que M' donc z est valeur propre de la matrice $UM'U^{-1}$.
La matrice $UM'U^{-1}$ répond à la question posée.

Remarque. Le fait que les matrices M_i commutent deux à deux n'est pas utilisé.

Décryptage du sujet

Un nombre complexe est dit algébrique s'il existe un polynôme P à coefficient rationnels tel que $P(\alpha) = 0$.
On définit alors le polynôme minimal de α, π_α comme le polynôme unitaire de $\mathbb{Q}[X]$ de degré minimal qui annule α ; π_α est l'unique générateur unitaire de l'idéal de $\mathbb{Q}[X]$ formé par les polynômes qui annulent α.
On appelle conjugués de α les racines complexes de son polynôme minimal.
Par exemple, les conjugués de $\sqrt{2}$ sont $\sqrt{2}$ et $-\sqrt{2}$; les conjugués de $\sqrt[3]{2}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.
Si A est une matrice de $\mathscr{M}_n(\mathbb{Q})$ et que α est une valeur propre complexe de A, alors le polynôme minimal de α divise le polynôme caractéristique de A donc tous les conjugués de α sont également valeurs propres de A.
Si A est une matrice symétrique à coefficients rationnels, on sait d'après le théorème spectral que toutes ses valeurs propres sont réelles. Ainsi, si α est valeur propre d'une telle matrice, il a la propriété que tous ses conjugués sont réels. (Par exemple, $\sqrt[3]{2}$ ne peut être valeur propre d'une matrice symétrique à coefficients rationnels).
Le but du sujet est de démontrer que la réciproque est vraie : si α est un nombre algébrique réel tel que tous ses conjugués sont réels, alors il est effectivement valeur propre d'une matrice symétrique à coefficients rationnels.
Il est démontré dans le sujet que l'ensemble des nombres algébriques dont tous les conjugués sont réels (nombres totalement réels) est un sous-corps de $\mathbb{C}$ (il s'agit d'une extension galoisienne du corps des nombres rationnels).