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 $\operatorname{pgcd}(x, y, z) = 1$. 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 $\frac{1}{2}(P + P^{-1})$ et, en diagonalisant P dans $\mathbb{C}$, on voit que ses valeurs propres sont les $\cos \frac{2k\pi}{n}$ pour $0 \leqslant k \leqslant n-1$. Elle répond à la question.

6. On a $Q(X) = X^d \left(\left(\frac{1}{X}\right)^d + a_{d-1}\left(\frac{1}{X}\right)^{d-1} + \cdots + a_1\left(\frac{1}{X}\right) + a_0 \right) = 1 + a_{d-1}X + \cdots + a_1 X^{d-1} + a_0 X^d$. 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

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

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 $x_1, \ldots, x_d$. 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 $X = \sum_{i=1}^{d} x_i \varepsilon_i \neq 0$, $X^T SX = \sum_{i=1}^{d} \lambda_i x_i^2 > 0$. 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 $(\varepsilon_1, \ldots, \varepsilon_d)$ 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 $(e_1, \ldots, e_d)$ est une base B-orthogonale de $\mathbb{R}^d$ qui convient (on a aisément $\mathrm{Vect}(e_1, \ldots, e_k) = \mathrm{Vect}(\varepsilon_1, \ldots, \varepsilon_k)$ pour tout k).

(b) Notons $P \in GL_d(\mathbb{Q})$ la matrice de passage de la base canonique à la base $(e_1, \ldots, e_d)$ 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 $(e_1, \ldots, e_d)$. 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 $\sum_{k=1}^{d} q_k x'_k y'_k = X'^T DY'$ avec $D = \mathrm{Diag}(q_1, \ldots, q_d)$ pour tous X' et Y', en prenant les vecteurs de la base canonique, on en déduit que $P^T SP = D = \mathrm{Diag}(q_1, \ldots, q_d)$. 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

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

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

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

Or $\mathrm{P}^{\mathrm{T}}\mathrm{DP} = \mathrm{P}^{\mathrm{T}}\Delta^2\mathrm{P} = (\Delta\mathrm{P})^{\mathrm{T}}(\Delta\mathrm{P}) = \mathrm{R}^{\mathrm{T}}\mathrm{R}$. Il vient donc $\mathrm{R}^{\mathrm{T}}\mathrm{RM} = \mathrm{M}^{\mathrm{T}}\mathrm{R}^{\mathrm{T}}\mathrm{R}$ ou encore en multipliant par les inverses, $\mathrm{RMR}^{-1} = (\mathrm{R}^{\mathrm{T}})^{-1}\mathrm{M}^{\mathrm{T}}\mathrm{R}^{\mathrm{T}} = (\mathrm{RMR}^{-1})^{\mathrm{T}}$ si bien que 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 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 $\mathrm{Q}^{-1}\widetilde{\mathrm{D}}\mathrm{Q} = \mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d) = \mathrm{Q}^{\mathrm{T}}\widetilde{\mathrm{D}}\mathrm{Q}$ 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 $\mathrm{Q}^{\mathrm{T}}\mathrm{BQ} = \mathrm{Q}^{\mathrm{T}}\widetilde{\mathrm{D}}\mathrm{QQ}^{\mathrm{T}}\mathrm{M}'\mathrm{Q} = \mathrm{Diag}(q_1\mathrm{I}_n, \ldots, q_d\mathrm{I}_d)\mathrm{Q}^{\mathrm{T}}\mathrm{M}'\mathrm{Q}$ 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 : $\mathrm{N}^{-1}\mathrm{Q}^{\mathrm{T}}\mathrm{BQN}^{-1}$ est donc symétrique, elle est à coefficients rationnels car N, Q et B le sont. Mais par ailleurs, $\mathrm{N}^{-1}\mathrm{Q}^{\mathrm{T}}\mathrm{BQN}^{-1} = \mathrm{NQ}^{\mathrm{T}}\mathrm{M}'\mathrm{QN}^{-1}$ 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 $\mathrm{N}^{-1}\mathrm{Q}^{\mathrm{T}}\mathrm{BQN}^{-1}$ est une matrice symétrique à coefficients rationnels admettant z comme valeur propre. Cqfd.