

Toutes les matrices envisagées dans ce problème sont des matrices de $\mathcal{M}_n(\mathbb{R})$ avec $n \geq 2$.

Si $A \in \mathcal{M}_n(\mathbb{R})$, une « racine carrée de A » est une matrice $R \in \mathcal{M}_n(\mathbb{R})$ telle que $R^2 = A$; on note alors $\text{Rac}(A) = \{R \in \mathcal{M}_n(\mathbb{R}) / R^2 = A\}$ l'ensemble de ses racines carrées.

I. Généralités sur $\text{Rac}(A)$.

1. Soit $A \in \mathcal{M}_n(\mathbb{R})$.

a. Prouver que pour que $\text{Rac}(A)$ soit non vide, il faut que $\det(A)$ soit positif.

$$\text{Si } A = R^2, \det A = (\det R)^2 \geq 0.$$

b. Prouver que si $R \in \text{Rac}(A)$, A et R commutent.

$$\text{Par associativité du produit matriciel, } AR = R^2R = (RR)R = R(RR) = RA.$$

c. Soit B une matrice semblable à A , $B = P^{-1}AP$. Quel lien existe-t-il entre $\text{Rac}(A)$ et $\text{Rac}(B)$?

$$R \in \text{Rac}(B) \Leftrightarrow R^2 = B \Leftrightarrow R^2 = P^{-1}AP \Leftrightarrow (PRP^{-1})^2 = A \Leftrightarrow PRP^{-1} \in \text{Rac}(A).$$

2. Pour tout réel α , on envisage la matrice de $\mathcal{M}_2(\mathbb{R})$ suivante : $A_\alpha = \begin{pmatrix} 1 & 0 \\ \alpha & -1 \end{pmatrix}$.

a. Calculer A_α^2 .

$$A_\alpha^2 = I_2.$$

b. Étant donnée une matrice A de $\mathcal{M}_2(\mathbb{R})$, l'ensemble $\text{Rac}(A)$ est-il toujours une partie finie de $\mathcal{M}_2(\mathbb{R})$?

Il y a une infinité de matrices de la forme A_α et toutes sont dans $\text{Rac}(I_2)$.

c. Expliciter une autre catégorie de matrices M de $\mathcal{M}_2(\mathbb{R})$, en nombre infini, telles que $M^2 = I_2$ (c'est du cours).

Les matrices de la forme $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ avec $a^2 + b^2 = 1$ sont les matrices des symétries orthogonales du plan euclidien. Elles vérifient, comme toutes les matrices de symétrie d'ailleurs, $M^2 = I_2$.

3. Soit u un endomorphisme non nul de \mathbb{R}^n , que l'on suppose nilpotent. On note p « l'indice de nilpotence de u », c'est-à-dire le plus petit des entiers k tels que $u^k = 0$.

a. Prouver l'existence d'un vecteur a de E tel que $u^{p-1}(a) \neq 0$, et prouver que la famille $(a, u(a), \dots, u^{p-1}(a))$ est libre.

Par définition même de p , on sait que $u^{p-1} \neq 0$. Il existe donc a tel que $u^{p-1}(a) \neq 0$.

Si $\alpha_0 a + \alpha_1 u(a) + \dots + \alpha_{p-1} u^{p-1}(a) = 0$, on prend u^{p-1} de tout cela et on obtient $\alpha_0 u^{p-1}(a) = 0$ donc

$\alpha_0 = 0$. En prenant maintenant le u^{p-2} , on trouve $\alpha_1 = 0$ et ainsi de suite.

b. En déduire que $p \leq n$ puis que $u^n = 0$.

On a trouvé une famille libre de p éléments, on est donc certain que $p \leq n$. Mais puisque $u^p = 0$, a fortiori $u^n = 0$.

c. Soit N une matrice nilpotente de $\mathcal{M}_n(\mathbb{R})$ d'indice de nilpotence p . Prouver que si $p > \frac{n+1}{2}$, alors $\text{Rac}(N) = \emptyset$.

Supposons $N = R^2$. Alors $R^{2p} = N^p = 0$: R est nilpotente. En revanche, $R^{2p-2} = N^{p-1} \neq 0$, donc $2p-2 < n$ d'après la question précédente. Bref, $2p-2 \leq n-1$, ou encore $p \leq \frac{n+1}{2}$. On obtient le résultat à prouver par contraposition.

5. Soit $A \in \mathcal{M}_n(\mathbb{R})$ de rang $n-1$, R une racine carrée de A .

a. Prouver que le noyau de R est inclus dans le noyau de A , et que R ne saurait être inversible.

Soit $X \in \mathcal{M}_{n,1}(\mathbb{R})$: $RX = 0 \Rightarrow RRX = 0 \Leftrightarrow AX = 0$. Par ailleurs, $\det A = (\det R)^2 = 0 \Rightarrow \det R = 0$.

b. En déduire que A et R ont même noyau.

Ainsi, le noyau de R qui n'est pas réduit à $\{0\}$ est inclus dans le noyau de A qui est une droite. Ils sont donc égaux pour d'évidentes raisons de dimensions.

c. Prouver que A et R ont même image.

Puisque $A = R^2$, $\text{Im } A \subset \text{Im } R$. Le théorème du rang prouve que ces ensembles ont même dimension, ils sont égaux.

II. Cas des matrices 2-2 non inversibles.

6. Rappeler le théorème de Cayley-Hamilton. À quelle formule se réduit-il pour $n = 2$?

Si $A \in \mathcal{M}_n(\mathbb{K})$ et si P_A désigne son polynôme caractéristique, alors $P_A(A) = 0$. En particulier, en dimension 2, $A^2 - \text{tr}(A)A + \det(A)I_2 = 0$.

7. Soit A une matrice de $\mathcal{M}_2(\mathbb{R})$ supposée non inversible, et R une racine carrée éventuelle de A .

a. Calculer $\det(R)$.

$$\det A = (\det R)^2 = 0 \Rightarrow \det R = 0$$

b. En déduire une condition nécessaire portant sur $\text{tr}(A)$ pour que R existe.

On applique le théorème de Cayley-Hamilton à R en supposant qu'il existe : $R^2 - \text{tr}(R)R = 0$, soit encore $A = \text{tr}(R)R$. En prenant les traces, il vient $\text{tr}(A) = \text{tr}(R)^2$. Il est donc nécessaire, pour que R existe, que la trace de A soit positive.

c. On suppose en outre que $\text{tr}(A) \neq 0$. Prouver que R est proportionnelle à A .

$$\text{Si } \text{tr}(A) \neq 0, \text{ alors } \text{tr}(R) \neq 0 \text{ d'où } R = \frac{1}{\text{tr}(R)} A : R \text{ est proportionnelle à } A.$$

8. On envisage $A = \begin{bmatrix} 3 & 2 \\ 9 & 6 \end{bmatrix}$. Déterminer $\text{Rac}(A)$.

Cette matrice est bien de rang 1 et comme sa trace est positive, cela rend plausible l'existence de R (mais pas certaine !). D'après ce qui précède, si R existe, elle est proportionnelle à A : $R = \lambda A$.

Alors $R^2 = A \Leftrightarrow \lambda^2 A^2 = A \Leftrightarrow \lambda^2 \begin{pmatrix} 27 & 18 \\ 81 & 54 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 9 & 6 \end{pmatrix} \Leftrightarrow \lambda^2 = \frac{1}{9}$. Finalement, A possède exactement deux racines carrées que sont $\frac{1}{3}A$ et $-\frac{1}{3}A$.

III. Cas où $A = I_n$.

9. Prouver que $\text{Rac}(I_n)$ est exactement constitué des matrices de $\mathcal{M}_n(\mathbb{R})$ qui sont diagonalisables et à spectre inclus dans $\{-1, 1\}$.

$A^2 = I_n$ si et seulement si A est la matrice d'une symétrie dans la base canonique de \mathbb{R}^n . Or l'étude des symétries montre que ce sont exactement les endomorphismes diagonalisables à spectre inclus dans $\{-1, 1\}$.

On peut aussi résoudre cette question en disant que le polynôme scindé-simple qu'est $X^2 - 1$ est annulateur de A ; A est donc diagonalisable et ses valeurs propres sont des racines de $X^2 - 1$. La réciproque est évidente.

IV. Un exemple explicite.

On considère ici la matrice A suivante :

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 4 \\ 1 & -2 & 3 \end{pmatrix}.$$

10. a. Calculer le polynôme caractéristique P_A de A .

On trouve facilement $P_A = (X - 1)(X^2 + 1)$.

b. A est-elle diagonalisable dans $\mathcal{M}_3(\mathbb{R})$? dans $\mathcal{M}_3(\mathbb{C})$?

P_A n'a pas toutes ses racines réelles, donc A n'est pas diagonalisable dans $\mathcal{M}_3(\mathbb{R})$. En revanche, P_A a toutes ses racines simples dans \mathbb{C} et l'on sait qu'il s'agit d'une condition **suffisante** pour que A soit diagonalisable dans $\mathcal{M}_3(\mathbb{C})$.

c. Expliciter un vecteur propre $X_1 \in \mathcal{M}_{3,1}(\mathbb{R})$ de A associé à sa valeur propre réelle.

On résout $AX = X$ et l'on trouve facilement que $X_1 = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$ convient.

d. Calculer $A^2 + I_3$, et donner un exemple de vecteur non nul $X_2 \in \mathcal{M}_{3,1}(\mathbb{R})$ tel que $(A^2 + I_3)X_2 = 0$.

$A^2 + I_3 = \begin{pmatrix} 2 & -2 & 4 \\ 2 & -2 & 4 \\ 1 & -1 & 2 \end{pmatrix}$: les deux premières colonnes de cette matrice étant opposées, on en déduit que le

vecteur $X_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ vérifie $(A^2 + I_3)X_2 = 0$ (pour ceux qui le voient mal, raisonnez en termes d'applications linéaires :

$C_1 = -C_2 \Rightarrow u(i) = -u(j) \Leftrightarrow u(i + j) = 0$).

e. Prouver que la famille (X_1, X_2, AX_2) est une base de $\mathcal{M}_{3,1}(\mathbb{R})$.

Deux méthodes pour cette question. La première « à la main » : on calcule AX_2 puis le déterminant (sur la base canonique) de la famille (X_1, X_2, AX_2) pour vérifier qu'il est non nul. Je vous laisse faire le calcul. La seconde plus savante : d'après le lemme des noyaux, on sait que $\mathcal{M}_{3,1}(\mathbb{R}) = \ker(A - I_3) \oplus \ker(A^2 + I_3)$. Or $X_1 \in \ker(A - I_3)$, $X_2 \in \ker(A^2 + I_3)$ et $AX_2 \in \ker(A^2 + I_3)$ car $(A^2 + I_3)AX_2 = A(A^2 + I_3)X_2 = A0 = 0$. Enfin X_2 et AX_2 sont indépendants car sinon X_2 serait vecteur propre de A associé à une valeur propre réelle, ce qui n'est pas. On en déduit le résultat annoncé puisque X_1 est une base de $\ker(A - I_3)$ et (X_2, AX_2) une base de $\ker(A^2 + I_3)$.

11. a. Prouver que A est semblable à la matrice R suivante :

$$R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

b. Prouver que R puis A possèdent des racines carrées réelles et en expliciter au moins une pour chacune.

On a établi le lien, dans la question 1.b., entre les racines carrées de deux matrices semblables. Trouver des racines pour R permet donc d'en trouver pour A . Or le bloc inférieur droit de R ressemble à s'y méprendre à la matrice d'une rotation d'angle $\frac{\pi}{2}$... et comment, en faisant deux fois la même opération, parvient-on à un quart

de tour ? En effectuant un huitième de tour, ou encore une rotation d'angle $\frac{\pi}{4}$! Finalement, la matrice S suivante

vérifie $S^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ avec $S = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. On trouve alors 4 racines carrées à R (on peut d'ailleurs prouver que ce sont les seules) qui sont :

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon' S \end{pmatrix} \text{ avec } \varepsilon, \varepsilon' \in \{-1, 1\}$$

V. Le cas diagonalisable.

12. a. Expliciter une infinité de racines carrées de la matrice nulle.

N'importe quelle matrice N_a ne possédant que des termes nuls sauf son terme supérieur droit qui est égal à a est de carré nul.

b. Soit A une matrice diagonalisable à spectre positif possédant 0 comme valeur propre multiple. Prouver que A possède une infinité de racines carrées.

$$\text{On écrit } A = PBP^{-1} \text{ avec } B = \begin{pmatrix} 0_p & & (0) \\ & \lambda_1 & \\ & \ddots & \\ (0) & & \lambda_k \end{pmatrix} \text{ et } R_a = P \begin{pmatrix} N_a & & (0) \\ & \sqrt{\lambda_1} & \\ & \ddots & \\ (0) & & \sqrt{\lambda_k} \end{pmatrix} P^{-1} \text{ vérifie } R_a^2 = A.$$

13. On note D la matrice de $\mathcal{M}_3(\mathbb{R})$ suivante :

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 9 \end{pmatrix}.$$

a. Donner (en raisonnant « à la main » !) une condition nécessaire et suffisante pour qu'une matrice M de $\mathcal{M}_3(\mathbb{R})$ commute avec D .

On voit aisément que M commute avec D si et seulement si M est diagonale (l'argument majeur étant que 1, 4 et 9 sont deux à deux distincts).

b. Quelle est la forme nécessaire d'une racine carrée de D ?

Déterminer toutes les racines carrées de D . Combien y en a-t-il ?

Une racine carrée de D se devant de commuter avec D , elle doit être diagonale. Alors :

$$\text{diag}(a, b, c)^2 = \text{diag}(1, 4, 9) \Leftrightarrow a^2 = 1, b^2 = 4 \text{ et } c^2 = 9.$$

Cela nous donne exactement 8 racines carrées pour D .

14. En adaptant la démarche suivie dans la question 13., prouver que la matrice Δ suivante ne possède pas de racines carrées dans $\mathcal{M}_3(\mathbb{R})$:

$$\Delta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -9 \end{pmatrix}.$$

Pour les mêmes raisons que dans la question précédente, les éventuelles racines carrées de Δ , se devant de commuter avec Δ , doivent d'être diagonales. Mais

$$\text{diag}(a, b, c)^2 = \text{diag}(1, -4, -9) \Leftrightarrow a^2 = 1, b^2 = -4 \text{ et } c^2 = -9,$$

ce qui exclut toute solution dans \mathbb{R} .

15. Soit A une matrice carrée diagonalisable à spectre positif et dont les valeurs propres sont deux à deux distinctes. En adaptant ce qui précède, prouver que A possède un nombre fini de racines carrées et les expliciter toutes. Combien y en a-t-il ?

On écrit $A = P \text{diag}(a_1, \dots, a_n) P^{-1} = P \Delta P^{-1}$. On sait que les racines carrées de A sont les PRP^{-1} où R est une racine carrée de Δ . On prouve que les matrices qui commutent avec Δ sont les matrices diagonales, et donc que les racines de Δ sont les matrices diagonales de la forme $\text{diag}(r_1, \dots, r_n)$ avec $r_k^2 = a_k$. On dispose donc de deux choix pour r_k , sauf si $a_k = 0$. Finalement, Δ possède exactement 2^{n-1} ou 2^n racines carrées, selon que 0 est valeur propre de A ou non.

VI. Cas où $A = -I_n$.

16. a. Prouver que pour $n = 2$, la matrice $-I_2$ possède effectivement des racines carrées (on pourra raisonner géométriquement, en cherchant une transformation plane dont le carré est $-Id$).

Il suffit d'envisager une rotation d'angle $\frac{\pi}{2}$ qui, quand on l'effectue deux fois, permet de réaliser un demi-tour. Ainsi, la matrice $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ vérifie $J^2 = -I_2$.

b. En déduire que pour n pair, $-I_n$ possède des racines carrées (on pourra exhiber une telle racine carrée sous forme d'une matrice diagonale par blocs, en utilisant la question précédente).

En supposant $n = 2p$, la matrice Δ diagonale par blocs comportant p matrices J sur sa diagonale vérifie $M^2 = -I_{2p}$.

c. Prouver que $\text{Rac}(-I_n) = \emptyset$ pour n impair.

Si n est impair, $\det I_n = -1 < 0$ et donc I_n n'est pas un carré (question 1.a.).

17. Soit n un entier pair non nul ($n = 2p$), et u un endomorphisme de \mathbb{R}^n tel que $u^2 = -Id$.

On construit par récurrence une famille de vecteurs de \mathbb{R}^n de la façon suivante : on choisit un vecteur non nul e_1 , et on pose $\varepsilon_1 = u(e_1)$. Supposons alors construits, pour $k < p$, les vecteurs $e_1, \varepsilon_1, \dots, e_k, \varepsilon_k$. Cette famille ayant un cardinal strictement plus petit que n , il est possible de choisir un vecteur e_{k+1} qui ne soit pas dans $\text{vect}\{e_1, \varepsilon_1, \dots, e_k, \varepsilon_k\}$. On pose alors $\varepsilon_{k+1} = u(e_{k+1})$. On répète alors ce processus jusqu'à construire ainsi une famille $(e_1, \varepsilon_1, \dots, e_p, \varepsilon_p)$ de vecteurs de \mathbb{R}^n .

a. Prouver que la famille $(e_1, \varepsilon_1, \dots, e_p, \varepsilon_p)$ est une base de \mathbb{R}^n .

Comme elle possède le bon cardinal, il y a juste à prouver que cette famille est libre. Mais :

$$\alpha_1 e_1 + \beta_1 \varepsilon_1 + \dots + \alpha_p e_p + \beta_p \varepsilon_p = 0 \Rightarrow u(\alpha_1 e_1 + \beta_1 \varepsilon_1 + \dots + \alpha_p e_p + \beta_p \varepsilon_p) = \alpha_1 \varepsilon_1 - \beta_1 e_1 + \dots + \alpha_p \varepsilon_p - \beta_p e_p = 0,$$

En multipliant la première équation par α_p , la seconde par β_p et en faisant la différence, on fait apparaître $(\alpha_p^2 + \beta_p^2)e_p$ comme combinaison linéaire de $e_1, \varepsilon_1, \dots, e_{p-1}, \varepsilon_{p-1}$. Mais tel qu'a été construit e_p , cela entraîne que $\alpha_p^2 + \beta_p^2 = 0$, c'est-à-dire $\alpha_p = \beta_p = 0$. On raisonne de même pour les autres coefficients.

b. Écrire la matrice de u dans cette base, et en déduire la forme générale des matrices carrées R telles que $R^2 = -I_n$.

On voit aisément que la matrice de u dans cette base est la matrice diagonale par blocs Δ de la question 16.b. Les racines carrées de $-I_n$ sont donc les matrices semblables à Δ .