Autour de l'équation $X^2 = A$ dans $\mathcal{M}_n(\mathbb{R})$

Adrien REISNER[1]

Abstract. We studies in this article some algebraic and topological properties of the set of matrices $Rac(A) = \left\{X \in \mathcal{M}_n(\mathbb{R}); X^2 = A\right\}$, where A is an element of $\mathcal{M}_n(\mathbb{R})$.

Keywords: symmetrical matrix, characteristic polinomial, eigenvector, eigenvalue, closed set.

MSC 2010: 15B99, 81U20.

1. Notations et définitions. Etant donné $A \in \mathcal{M}_n(\mathbb{R})$, on note $Rac(A)$ l'ensemble $\left\{X \in \mathcal{M}_n(\mathbb{R}); X^2 = A\right\}$ et on appelle *racine carrée* de A tout élément de $Rac(A)$. On se propose l'étude de quelques propriétés élémentaires – *algébriques* et *topologiques* – de cet ensemble. $\mathcal{S}_n^+(\mathbb{R})$ désignera l'ensemble des matrices réelles symétriques positives (i.e. $A \in \mathcal{S}_n^+(\mathbb{R})$ si et seulement si $A = {}^tA \in \mathcal{M}_n(\mathbb{R})$ et $\forall X$, ${}^tXAX \geq 0$).

2. Etude algébrique: cas particuliers, exemples.

Théorème 1. *Si $A \in M_n(\mathbb{R})$ admet n valeurs propres réelles distinctes $\lambda_1 < \lambda_2 < \ ... \ < \lambda_n$, alors $Rac(A) = \emptyset$ si $\lambda_1 < 0$, $CardRac(A) = 2^{n-1}$ si $\lambda_1 = 0$, $CardRac(A) = 2^n$ si $\lambda_1 > 0$.*

Démonstration. La matrice A ayant n valeurs propres distinctes, cette matrice est diagonalisable. Il existe donc $P \in GL_n(\mathbb{R})$ telle que $A = PDP^{-1}$, où $D = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$. Soit alors $R \in \mathcal{M}_n(\mathbb{R})$ et $S = P^{-1}RP$. On a $R^2 = A$ si et seulement si $P^{-1}R^2P = D$, i.e. $S^2 = D$. Par suite $Rac(A) = P\ Rac(D)\ P^{-1}$. Soit S une racine carrée de D. Il vient: $SD = S^3 = DS$. Le produit matriciel $SD = DS$ montre alors – les λ_i étant distincts – que la matrice S est elle-même diagonalisable: $S = diag(s_1, s_2, \ldots, s_n)$ et que $s_i^2 = \lambda_i$, $i = 1, 2, \ldots, n$. On en déduit que si $\lambda_1 < 0$, alors $Rac(A) = \emptyset$. Si tous les λ_i sont positifs, on a: $Rac(D) \subset \{diag(\varepsilon_i\sqrt{\lambda_i})_{i:1,\ldots,n}; \varepsilon_i = \pm 1\}$. Réciproquement, si $S = diag(\varepsilon_i\sqrt{\lambda_i})_{i:1,\ldots,n}$ où $\varepsilon_i = \pm 1$, alors $S^2 = D$, et l'inclusion ci-dessus est une égalité. L'application $M \to P^{-1}MP$ est une bijection de $Rac(A)$ dans $Rac(D)$, d'où: si $\lambda_1 < 0$, $Rac(A) = \emptyset$; si $\lambda_1 \geq 0$, $Rac(A) = \{P\ diag(\varepsilon_i\sqrt{\lambda_i})_{i:1,\ldots,n}\ P^{-1}; \varepsilon_i = \pm 1\}$. Finalement, le théorème est démontré, en distinguant respectivement les cas où $\lambda_1 = 0$ et $\lambda_1 > 0$.

Exemple. Soit à déterminer $Rac(A)$ où $A = \begin{pmatrix} 11 & -5 & 5 \\ -5 & 3 & -3 \\ 5 & -3 & 3 \end{pmatrix}$. Le polynôme caractéristique de la matrice A étant $\chi_A(X) = X(X^2 - 17X + 16) = X(X-1)(X-16)$, son spectre est $Sp(A) = \{0, 1, 16\}$. Déterminons les sous-espaces propres de la matrice A. Le noyau de A, sous-espace associé à la valeur propre $\lambda_1 = 0$, est la droite $\mathbb{R}v_1$ où ${}^tv_1 = (0, 1, 1)$. Le sous-espace propre associé à la valeur propre $\lambda_2 = 1$ est le sous espace $\mathbb{R}v_2$ où ${}^tv_2 = (1, 1, -1)$. Enfin $\mathbb{R}v_3$ où ${}^tv_3 = (2, -1, 1)$ est le sous-espace propre de la matrice A associé à la valeur propre $\lambda_3 = 16$. On a donc: $P^{-1}AP = diag(0, 1, 16)$, où P est la matrice $P = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$. La matrice A admet quatre

[1]TELECOM ParisTech; e-mail: *Adrien.Reisner@telecom-paristech.fr*

racines carrées qui sont: $Pdiag(0,1,4)P^{-1}$, $Pdiag(0,-1,4)P^{-1}$, $Pdiag(0,1,-4)P^{-1}$ et $Pdiag(0,-1,-4)P^{-1}$, soit explicitement:
$R_1 = \begin{pmatrix} 3 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$, $R_2 = \frac{1}{3}\begin{pmatrix} 7 & -5 & 5 \\ -5 & 1 & -1 \\ 5 & -1 & 1 \end{pmatrix}$, $R_3 = -R_2$ et $R_4 = -R_1$.

Remarque. La matrice A étant symétrique, A est diagonalisable, les sous-espaces propres $\mathbb{R}v_i$, $i : 1,2,3$, de cette matrice sont orthogonaux deux à deux ce qu'on vérifie immédiatement (ainsi la matrice de passage P peut être choisie orthogonale, i.e. vérifiant $P^{-1} = {}^tP$, en remplaçant les trois vecteurs v_i par les vecteurs $\frac{v_i}{\|v_i\|}$, $i : 1,2,3$.

Théorème 2. *On a:*
$Rac(O) = \{PM_rP^{-1}; P \in GL_n(\mathbb{R}),\ M_r = \begin{pmatrix} O & I_r \\ O & O \end{pmatrix}$, *avec* $r \in \mathbb{N} \cap [1, n/2]\} \cup \{O\}$.

Démonstration. Soit $R \in \mathcal{M}_n(\mathbb{R})$ une racine carrée de la matrice nulle et désignons par f l'endomorphisme de $\mathbb{R}^n$ dont R est la matrice dans la base canonique de $\mathbb{R}^n$. Ayant $f \circ f = 0$, il vient $Imf \subset Kerf$ et par suite – à partir de l'égalité $rgf + dimKerf = n$ –: $rgf = r \leq \frac{1}{2}n$. Soit $(e_1, \ldots, e_r)$ une base de Imf que l'on complète avec $(e_{r+1}, \ldots, e_{n-r})$ pour former une base de $Kerf$. Si u_i, $i : 1, \ldots, r$ est un vecteur tel que $f(u_i) = e_i$, soit $\mathcal{B} = (e_1, \ldots, e_{n-r}, u_1, \ldots, u_r)$. Montrons que les n éléments de $\mathcal{B}$ forment une famille libre, i.e. que $\mathcal{B}$ est une base de $\mathbb{R}^n$. Supposant que $\sum_{i=1}^{n-r} \alpha_i e_i + \sum_{i=1}^{r} \beta_i u_i = 0$, il vient, avec les notations précédentes: $\sum_{i=1}^{r} \alpha_i f(u_i) + \sum_{i=r+1}^{n-r} \alpha_i e_i + \sum_{i=1}^{r} \beta_i u_i = 0$. Ayant $f^2 = 0$ et $f(e_i) = 0$ pour $i : r+1, \ldots, n-r$, on obtient alors: $\sum_{i=1}^{r} \beta_i f(u_i) = \sum_{i=1}^{r} \beta_i e_i = 0$. La famille $\{e_i\}_{i=1,\ldots,r}$ étant libre, $\beta_i = 0, i : 1, \ldots, r$, et finalement $\mathcal{B}$ est libre – puisque les $(e_1, \ldots, e_{n-r})$ sont libres – . Dans cette base $\mathcal{B}$, la matrice de l'endomorphisme f est: $Mat(f, \mathcal{B}) = \mathcal{M}_r = \begin{pmatrix} O & I_r \\ O & O \end{pmatrix}$. Si $R \in Rac(O)$, alors soit $R = O$, soit R est semblable à une matrice de type $\mathcal{M}_r$ avec $r \leq \frac{1}{2}n$. Réciproquement, si $r \leq \frac{1}{2}n$, un calcul élémentaire prouve que $\mathcal{M}_r^2$=O (car $r \leq \frac{1}{2}n$), donc que toute matrice semblable à $\mathcal{M}_r$ est de carré nul.

Exemple. Les matrices carrées d'ordre 4 de carré nul sont la matrice nulle et les matrices semblables à $\mathcal{M}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ ou à $\mathcal{M}_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Théorème 3. $Rac(I_n) = \{Pdiag(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n); P \in GL_n(\mathbb{R}), \varepsilon_i \in \{-1, +1\}, \forall i\}$.

Démonstration. Soit R telle que $R^2 = I$; alors $detR = \pm 1$ et R est inversible (d'ailleurs d'inverse elle-même). Le polynôme $X^2 - 1$ est un polynôme annulateur de la matrice R. C'est un polynôme scindé à racines simples sur $\mathbb{R}$ et par suite R est $\mathbb{R}$-diagonalisable et les valeurs propres appartiennent à l'ensemble $\{-1, 1\}$. Donc $RacI \subset \{Pdiag(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)P^{-1}; P \in GL_n(\mathbb{R}), \varepsilon_i = \pm 1,\ i : 1, \ldots, n\}$.

Réciproquement, $D = diag(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ vérifie $D^2 = I$ et il en est de même pour toute matrice semblable à la matrice D. L'inclusion précédente est donc une égalité.

Théorème 4. *Toute matrice A réelle symétrique positive admet au moins une racine carrée qui est elle même symétrique et positive: $Rac(A) \cap S_n^+(\mathbb{R}) \neq \emptyset$.*

Démonstration. Soit A une matrice réelle symétrique *positive*. Cette matrice est donc ortho-diagonalisable: $A = PDP^{-1} = PD\ {}^tP$, avec $D = diag(\lambda_1, \lambda_2, ..., \lambda_n)$ où $\lambda_i \geq 0, i : 1, \ldots, n$ – la matrice A étant positive – et P une matrice orthogonale. Si $\Delta = diag(\sqrt{\lambda_1}, ..., \sqrt{\lambda_n})$, la matrice $R = P\Delta\ {}^tP$ est symétrique positive, car elle est semblable à la matrice positive Δ ($Sp(R) = Sp(\Delta) \subset \mathbb{R}^+$). Enfin $R^2 = P\Delta^2\ {}^tP = A$. Ainsi A admet au moins une racine carrée R, également symétrique positive.

Remarques. 1)Toute matrice symétrique n'admet pas forcément de racine carrée dans $\mathcal{M}_n(\mathbb{R})$, comme le prouve la matrice $(-1) \in \mathcal{M}_1(\mathbb{R})$.

2) La matrice A de l'exemple du Théorème 1 vérifie bien les hypothèses du théorème précédent. On vérifie qu'effectivement les quatre racines carrées de A sont elles mêmes symétriques. R_1 est de plus positive.

3. Etude topologique: Rac(A) ensemble fermé. On munit $\mathcal{M}_n(\mathbb{R})$ de la norme: $N(A) = \max\limits_{1 \leq i,j \leq n} |a_{ij}|$, si $A = (a_{ij})$.

Remarque. $\mathcal{M}_n(\mathbb{R})$ étant de dimension finie, toutes les normes y sont équivalentes. Pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$, les propriétés topologiques de $Rac(A)$ restent inchangées lorsqu'on remplace la norme N par toute autre norme de $\mathcal{M}_n(\mathbb{R})$.

Théorème 5. *a) Pour toute $A \in \mathcal{M}_n(\mathbb{R})$, $Rac(A)$ est une partie fermée de $\mathcal{M}_n(\mathbb{R})$.*
b) $Rac(I_n)$ n'est pas une partie bornée de $\mathcal{M}_n(\mathbb{R})$.

Démonstration. a) Soit $A \in \mathcal{M}_n(\mathbb{R})$. L'application $R \to R^2$ est continue sur $\mathcal{M}_n(\mathbb{R})$ (chaque fonction coordonnée est continue comme fonction polynomiale des coefficients de R). Si (R_k) est une suite convergentes de matrices de $\mathcal{M}_n(\mathbb{R})$ de limite R, alors $R_k^2 \to R^2$. Donc (R_k) étant une suite convergente d'éléments de $Rac(A)$, la limite appartient elle-même à $Rac(A)$. Ainsi $Rac(A)$ est un ensemble fermé de $\mathcal{M}_n(\mathbb{R})$.

b) Considérons pour $q \in \mathbb{N}^*$ la matrice $S_q = \begin{pmatrix} 1 & 0 \\ q & -1 \end{pmatrix}$. On a: $N(S_q) = \max(|q|, 1)$ $\to \infty$ lorsque $q \to \infty$ et $S_q^2 = I_2$. On en déduit que $Rac(I_2)$ n'est pas bornée. Définissons alors lorsque $n \geq 3$ la matrice par blocs $M_q = \begin{pmatrix} S_q & O \\ O & I_{n-q} \end{pmatrix}$. Cette matrice vérifie: $M_q^2 = I_n$, $N(M_q) \to \infty$ lorsque $q \to \infty$ et par suite $Rac(I_n)$ n'est pas bornée dans $\mathcal{M}_n(\mathbb{R})$ pour la norme N, donc aussi pour toute autre norme de $\mathcal{M}_n(\mathbb{R})$.

On appelle norme sur-multiplicative sur $GL_n(\mathbb{R})$ une norme $\mathcal{N}$ vérifiant, pour tout $A, B \in GL_n(\mathbb{R})$ l'inégalité: $\mathcal{N}(AB) \geq \mathcal{N}(A)\mathcal{N}(B)$.

Corollaire 6. *Pour $n \geq 2$ il n'existe pas de norme sur-multiplicative sur $GL_n(\mathbb{R})$.*

Démonstration. Compte tenu du théorème précédent il existe dans $Rac(I_n)$ une suite (R_k) non bornée. Supposons alors par l'absurde qu'il existe sur $GL_n(\mathbb{R})$ une norme $\mathcal{N}$ sur-multiplicative. On aurait alors: $\mathcal{N}(I_n) = \mathcal{N}(R_k^2) \geq [\mathcal{N}(R_k)]^2$. Le membre de gauche est constant alors que celui de droite est de limite infinie, les deux normes N et $\mathcal{N}$ étant équivalentes – voir remarque précédente – , d'où contradiction.