Matrices réelles inversibles qui sont des carrés

Jean-François Burnol, 29 juin 2018

L'énoncé suivant est un grand classique des développements proposés en agrégation externe comme interne :

Théorème 1. *Une matrice réelle* inversible A *est le carré d'une autre matrice réelle* B *si et seulement si elle est dans l'image de l'exponentielle de matrice.*

Vous trouverez des dizaines de rédactions sur internet (avec quelques variantes dans les preuves). C'est bien joli mais ça laisse complètement ouvert la question de caractériser de manière constructive ces fameuses matrices qui sont des carrés, ou de manière équivalente qui sont dans l'image de l'exponentielle de matrice (réelle). Le théorème suivant apporte la réponse :

Théorème 2. *Une matrice réelle* inversible A *est le carré d'une matrice réelle* B *si et seulement si pour toute valeur propre* λ *réelle* ***négative*** *de* A*, les noyaux* $\operatorname{Ker}(A - \lambda\operatorname{Id})^k$ *sont pour tous les* k *de dimensions paires.* [1]

Preuve. Pour la preuve je vais supposer que le lecteur est déjà familiarisé avec certains faits liés aux démonstrations du théorème 1 (et directement ou indirectement liés à la notion d'espace caractéristique associé à une valeur propre réelle ou complexe), et donc je peux affirmer sans donner de détails [2] qu'il suffit de démontrer l'énoncé dans le cas où la matrice A de taille $n \times n$ a une unique valeur propre λ (dans le spectre complexe) et que celle-ci est réelle et strictement négative. Et il suffit alors de traiter le cas avec $\lambda = -1$ par une réduction triviale.

La matrice $N = A + I_n$ est donc nilpotente. Supposons que $A = B^2$. Alors B commute avec A donc avec N, donc laisse stable chaque $V_k = \operatorname{Ker} N^k \subset \mathbb{R}^n$. On a ici assimilé les matrices aux endomorphismes de $\mathbb{R}^n$ associés. Pour être bien clair je vais plutôt noter ϕ pour l'endomorphisme de matrice A et ψ pour celui de matrice B sur $V = \mathbb{R}^n$ muni de la base canonique.

Soit ϕ_k et ψ_k les restrictions à V_k. Alors $\det \phi_k$ est le carré de $\det \psi_k$ donc positif, et est par ailleurs $(-1)^{\dim V_k}$. En effet l'unique valeur propre (réelle ou complexe) est -1. Donc $\dim V_k$ est pair, pour tout k (lorsque $k = 0$, $V_k = \{0\}$).

Il s'agit maintenant de montrer que cette condition est suffisante pour l'existence d'une matrice B réelle avec $B^2 = A$.

---

1. Vraiment pas clair s'il faut écrire « de dimensions paires » ou « de dimension paire ».
2. Finalement j'ai eu pitié, donc à la fin du texte je donne quelques compléments pour justifier ces affirmations. Ça occupe plus de 60% de ce texte !

Je fais appel à la fiche sur la décomposition de Jordan des endomorphismes nilpotents :

http://jf.burnol.free.fr/agreg180628jordan.pdf

Puisque tous les dim V_k sont pairs les formules de cette fiche impliquent que la (ou plutôt une) décomposition de Jordan pour N comporte un nombre pair c_i de chaque type de bloc de Jordan J_i. Par conséquent il existe une base de $\mathbb{R}^n$ dans laquelle l'endomorphisme η associé à N a une matrice de la forme

$$\begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix}$$

et c'est donc a fortiori aussi le cas pour $\phi = -\mathrm{Id} + \eta$. Mais

$$\begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} = \begin{pmatrix} 0 & I \\ T & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & I \\ T & 0 \end{pmatrix}$$

Donc ϕ est le carré d'un endomorphisme réel, et sa matrice A dans la base canonique est le carré d'une matrice réelle, ce qu'il fallait démontrer. □

On peut aussi reformuler le théorème sous la forme suivante, compte tenu de la preuve que nous venons de faire :

Théorème 3. *Une matrice réelle inversible A est le carré d'une matrice réelle B si et seulement si elle est semblable à une matrice par blocs*

$$\begin{pmatrix} U & 0 & 0 \\ 0 & T & 0 \\ 0 & 0 & T \end{pmatrix}$$

avec U n'ayant aucune valeur propre réelle négative et T n'ayant (dans son spectre complexe) que des valeurs propres réelles négatives.

Mais ce dernier énoncé semble moins « constructif » que le précédent (dans la mesure où l'on peut considérer constructif un énoncé qui implique a priori d'avoir déterminé les valeurs propres).

Rappels

Soit V un espace vectoriel réel de dimension finie d et soit ϕ un endomorphisme. Comme nous allons utiliser des nombres complexes, nous supposerons $V = \mathbb{R}^d$, c'est-à-dire qu'on a choisi une base de V. Mais les sous-espaces de V que nous allons construire ne dépendent pas de cette base (puisque ce seront des noyaux de certains endomorphismes dépendant de ϕ).

Le polynôme caractéristique $P(X) = \det(X\,\mathrm{Id} - \phi)$ se factorise sur $\mathbb{R}$ en un produit de facteurs irréductibles $\prod_{1 \leqslant i \leqslant I}(X - \lambda_i)^{m_i} \prod_{1 \leqslant j \leqslant J}(X^2 + a_j X + b_j)^{n_j}$ avec $\sum_i m_i + 2\sum_j n_j = d$. Bien sûr I ou J peut être vide.

Les λ_i sont les valeurs propres réelles de ϕ, les noyaux $\mathrm{Ker}(\phi - \lambda_i\,\mathrm{Id})$ ne sont donc pas les espaces nuls.

Il est aussi vrai que les $\mathrm{Ker}(\phi^2 + a_j\phi + b_j\,\mathrm{Id})$ ne sont pas des espaces nuls. Car en notant A la matrice de ϕ dans la base canonique, on a $\det(\phi^2 + a_j\phi + b_j\,\mathrm{Id}) = \det(A^2 + a_jA + b_jI_d)$. Or ce dernier déterminant est $\det(A - \mu_jI_d)\det(A - \overline{\mu_j}I_d)$ avec $\mu_j, \overline{\mu_j}$ les racines complexes de $t^2 + a_jt + b_j = 0$ car $(A - \mu_jI_d)(A - \overline{\mu_j}I_d) = A^2 + a_jA + b_jI_d$ par les relations coefficients-racines. Et $\det(A - \mu_jI_d) = 0$.

Nous avons donc des espaces « caractéristiques » tous non nuls :

$$E_i = \ker(X - \lambda_i)^{m_i}, \quad 1 \leqslant i \leqslant I$$
$$F_j = \ker(X^2 + a_jX + b_j)^{n_j}, \quad 1 \leqslant j \leqslant J$$

qui sont stables par ϕ. Le Lemme des Noyaux permet d'affirmer que V se décompose en somme directe des E_i et des F_j (on pourrait le re-démontrer entièrement ici mais par confort je préfère l'admettre car mon objectif est d'ajouter des remarques additionnelles).

Sur E_i, $\phi - \lambda_i\,\mathrm{Id}$ est nilpotent. Et nous pouvons affirmer que la dimension d_i de E_i est exactement m_i : car le polynôme caractéristique $P(X) = \det(X\,\mathrm{Id} - \phi)$ sur V est le produit des polynômes caractéristiques sur chacun des E_i et F_j et les facteurs $X - \lambda_i$ ne peuvent provenir que de E_i ; comme le polynôme caractéristique de $\phi|_{E_i}$ est $(X - \lambda_i)^{\dim E_i}$, on en déduit $d_i = \dim E_i = m_i$.

Sur F_j, c'est un peu plus complexe (sic). Notons f_j sa dimension. Choisissons une base réelle de F_j et notons A_j la matrice de $\phi|_{F_j}$ dans cette base. Pour tout i, la matrice $A_j - \lambda_iI_{f_j}$ est inversible puisque $F_j \cap E_i = \{0\}$. De même pour tout $k \neq j$, la matrice $A_j^2 + a_kA_j + b_kI_{f_j}$ est inversible puisque $F_j \cap F_k = \{0\}$. Donc le polynôme caractéristique de A_j n'a aucun des λ_i ni aucun des $\mu_k, \overline{\mu_k}$ $(k \neq j)$ parmi ses racines complexes. Comme il doit diviser $P(X)$ il est un facteur de $(X^2 + a_jX + b_j)^{n_j}$.

Ceci étant vrai pour chaque j, la seule possibilité est qu'il est exactement égal à $(X^2 + a_jX + b_j)^{n_j}$ et par conséquent $f_j = \dim F_j = 2n_j$.

Jusqu'à présent nous n'avons utilisé que des vecteurs réels. Je vais maintenant utiliser des vecteurs complexes mais sans tout le formalisme qu'on pourrait développer à ce propos.

Je rappelle qu'on a choisi dans F_j une base. Ce sont des vecteurs de $V = \mathbb{R}^d$. Notons-les $w_1, ..., w_{f_j}$ bien qu'ils ne jouent pas un grand rôle. La matrice A_j réelle de taille $f_j \times f_j$ exprime l'action de ϕ dans cette base $(w_1, \ldots, w_{f_j})$ de F_j.

Considérons A_j maintenant comme la matrice d'un endomorphisme α_j sur $\mathbb{C}^{f_j}$. On utilise donc tacitement l'isomorphisme $F_j \simeq \mathbb{R}^{f_j} \subset \mathbb{C}^{f_j}$ qui identifie $(w_1, \ldots, w_{f_j})$ à la base canonique de $\mathbb{C}^{f_j}$. Attention donc que les w_k sont originellement des vecteurs de $\mathbb{R}^d$, mais maintenant sont aussi considérés comme les vecteurs canoniques de $\mathbb{C}^{f_j}$.

Cet endomorphisme α_j sur $\mathbb{C}^{f_j}$ de matrice A_j a comme polynôme caractéristique complexe $(X-\mu_j)^{n_j}(X-\overline{\mu_j})^{n_j}$. Ainsi $\mathbb{C}^{f_j}$ est la somme directe $G_j \oplus H_j$ avec G_j l'espace caractéristique complexe pour μ_j et H_j celui pour $\overline{\mu_j}$. Clairement (car l'endomorphisme commute avec la conjugaison complexe) une bijection entre ces deux sous-espaces de $\mathbb{C}^{f_j}$ est obtenue par la conjugaison complexe agissant sur $\mathbb{C}^{f_j}$ coordonnée par coordonnée. On prend une $\mathbb{C}$-base z_1, ..., z_p de $G_j \subset \mathbb{C}^{f_j}$, alors $\overline{z_1}, \dots, \overline{z_p}$ est une $\mathbb{C}$-base de H_j. Ainsi $2p = f_j = 2n_j$ donc $p = n_j$. Si C est la matrice complexe donnant l'action de α_j sur $(z_1, \dots, z_p)$, alors $\overline{C}$ (c'est-à-dire la matrice des conjugués complexes des coefficients de C) est celle donnant son action sur $(\overline{z_1}, \dots, \overline{z_p})$. Ainsi il existe une matrice de passage complexe P telle que

$$A_j = P\begin{pmatrix} C & 0 \\ 0 & \overline{C} \end{pmatrix} P^{-1}, \qquad P = \begin{pmatrix} Q & \overline{Q} \\ R & \overline{R} \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} S & T \\ \overline{S} & \overline{T} \end{pmatrix}$$

P exprime la base complexe $(z_1, \dots, z_p, \overline{z_1}, \dots, \overline{z_p})$ dans la base canonique $(w_1, \dots, w_{f_j})$, et a donc la structure indiquée plus haut. Son inverse exprime les vecteurs de la base canonique de $\mathbb{C}^{f_j}$ dans la base $(z_1, \dots, z_p, \overline{z_1}, \dots, \overline{z_p})$, donc en passant aux conjugués complexes et par unicité on voit qu'elle a l'écriture indiquée.

Calculons maintenant

$$D_j = P\begin{pmatrix} \mu_j I_p & 0 \\ 0 & \overline{\mu_j} I_p \end{pmatrix} P^{-1} = \begin{pmatrix} Q & \overline{Q} \\ R & \overline{R} \end{pmatrix}\begin{pmatrix} \mu_j I_p & 0 \\ 0 & \overline{\mu_j} I_p \end{pmatrix}\begin{pmatrix} S & T \\ \overline{S} & \overline{T} \end{pmatrix}$$

$$D_j = \begin{pmatrix} \mu_j Q & \overline{\mu_j Q} \\ \mu_j R & \overline{\mu_j R} \end{pmatrix}\begin{pmatrix} S & T \\ \overline{S} & \overline{T} \end{pmatrix} = \begin{pmatrix} \mu_j QS + \overline{\mu_j QS} & \mu_j QT + \overline{\mu_j QT} \\ \mu_j RS + \overline{\mu_j RS} & \mu_j RT + \overline{\mu_j RT} \end{pmatrix}$$

C'est une matrice réelle !

On vérifie immédiatement que D_j commute avec A_j (suffit de conjuguer avec P) et que $N_j = A_j - D_j$ est nilpotente (idem). Bien sûr on aurait pu invoquer une décomposition de Dunford sur $\mathbb{C}$, puis l'unicité et la conjugaison complexe pour affirmer qu'elle est définie sur $\mathbb{R}$, mais ça ne fait pas de mal de faire des calculs explicites de temps en temps. Et on n'aurait pas eu à faire tout ce travail si le programme officiel ne se limitait pas au cas d'un polynôme caractéristique scindé lorsqu'il évoque la décomposition de Dunford, ce qui rend la discussion détaillée que je viens de faire peu fréquente dans les ouvrages mis à votre disposition.

La matrice D_j est caractérisée de manière unique par le fait qu'elle est diagonalisable sur les complexes, qu'elle commute avec A_j et que la différence $N_j = A_j - D_j$ est nilpotente. En effet soit D_j' une autre solution. Comme D_j' commute avec A_j l'endomorphisme associé laisse stable dans $\mathbb{C}^{f_j}$ le sous-espace G_j. Cet endomorphisme (qui commute à la conjugaison complexe) est donc représenté dans la base $(z_1, \dots, z_p, \overline{z_1}, \dots, \overline{z_p})$

par une matrice $P^{-1}D'_jP$ avec deux blocs diagonaux conjugués complexes, et par conséquent commute avec la matrice $P^{-1}D_jP$. Ainsi D'_j commute avec D_j, et $N'_j = A_j - D'_j$ commute avec $N_j = A_j - D_j$. Il en résulte que $N'_j - N_j$ est nilpotente. Mais c'est aussi $D_j - D'_j$ qui est diagonalisable sur les complexes. Il s'agit donc de la matrice nulle et l'unicité est établie.

Nous sommes en mesure maintenant de démontrer :

Théorème 4. *Soit ϕ un endomorphisme inversible d'un espace vectoriel réel V de dimension finie, ne possédant aucune valeur propre négative. Alors ϕ peut s'écrire sous la forme ψ^2 avec ψ un autre endomorphisme réel.*

Preuve. Il suffit de le faire sur chaque espace caractéristique E_i ou F_j. En fait il *faut* le faire sur ces espaces : si $\psi^2 = \phi$ alors ψ commute avec ϕ donc laisse stable chaque E_i et chaque F_j et y fournit par conséquent partout une « racine carrée » de la restriction de ϕ.

Le cas d'une valeur propre réelle positive. Laissé en exercice car c'est plus simple que ce qui suit. Attention cependant de bien faire attention que la valeur propre est non-nulle, par hypothèse d'inversibilité de ϕ. Le résultat est faux pour les endomorphismes non nécessairement injectifs. Donc il vous faudra comprendre là où la démonstration ne passe pas.

Le cas de valeurs propres complexes conjuguées. On reprend les mêmes notations : on est donc dans un F_j associé à un facteur $(X^2 + a_jX + b_j)^{n_j}$ qui a pour racines complexes $\mu_j, \overline{\mu_j}$, et on a choisi $\operatorname{Im}\mu_j > 0$. La restriction de ϕ à F_j est exprimée par une matrice A_j dans une base prise arbitrairement et on a alors défini D_j.

Soit ν_j la racine carrée de μ_j qui a partie imaginaire strictement positive (pour fixer les idées). Son conjugé complexe $\overline{\nu_j}$ est alors une racine carrée de $\overline{\mu_j}$. Bien sûr on va maintenant considérer la matrice

$$K_j = P \cdot \begin{pmatrix} \nu_j I_p & 0 \\ 0 & \overline{\nu_j} I_p \end{pmatrix} \cdot P^{-1}$$

puisque, par exactement le même calcul qui montrait que D_j était une matrice réelle, K_j est une matrice réelle qui commute avec A_j, D_j et $N_j = A_j - D_j$ et vérifie $K_j^2 = D_j$. Ainsi $A_j = K_j^2(I_{f_j} + D_j^{-1}N_j)$.

Il suffit alors d'utiliser la série de Newton

$$\sqrt{1+h} = 1 + \frac{1}{2}h + \frac{1}{2}(-\frac{1}{2})\frac{h^2}{2} + \frac{1}{2}(-\frac{1}{2})(-\frac{3}{2})\frac{h^3}{6} + \cdots$$

Comme D_j commute avec N_j, D_j^{-1} également et $D_j^{-1}N_j$ est nilpotent. La série ci-dessus s'arrête avec un nombre fini de termes et permet de trouver M_j nilpotente avec $I_{f_j} + D_j^{-1}N_j = (I_{f_j} + M_j)^2$. Comme M_j est un polynôme en D_j^{-1} et N_j elle commute avec K_j.

Finalement $K_j(I_{f_j} + M_j)$ au carré vaut $K_j^2(I_{f_j} + D_j^{-1}N_j) = A_j$. □