Exponentielle de matrices

Tristan Vaccon

septembre 2012

Table des matières

Références

[1] Serre, Denis Les matrices

[2] Mneimé & Testard Introduction à la théorie des groupes de Lie classiques

[3] Gourdon, Xavier Les Maths en tête

[4] Beck, Peyré, Malick Objectif Agreg

[5] Rouvière Calcul différentiel

[6] Demailly Analyse numérique et équations différentielles

[7] Nourdin Épreuve orale, etc...

1 Définitions et premières propositions

On munit $M_n(\mathbb{C})$ d'une norme d'algèbre quelconque. On pose pour $A \in M_n(\mathbb{C})$,

$$\exp(A) = \sum_{n=0}^{+\infty} \frac{1}{n!} A^n.$$

Alors,

$$\sum_{n=0}^{N} \frac{1}{n!} \|A^n\| \leqslant \sum_{n=0}^{+\infty} \frac{1}{n!} \|A\|^n \leqslant exp(\|A\|).$$

On en déduit que l'application exponentielle est C^0 sur $M_n(\mathbb{C})$ car cette série converge normalement sur tout compact.

Proposition 1.1. *Soit $A \in M_n(\mathbb{C})$, alors $\exists P \in \mathbb{C}[X]$ tel que $exp(A) = P(A)$.*

Démonstration. $\mathbb{C}[A]$ est un sous-espace vectoriel de $M_n(\mathbb{C})$, et est donc complet (ou fermé...), comme nous sommes en dimension finie. Ainsi,

$$\forall N \in \mathbb{N}, \sum_{n=0}^{N} \frac{1}{n!} A^n \in \mathbb{C}[A]$$

donc $exp(A) \in \mathbb{C}[A]$ (comme on est fermé...). □

Proposition 1.2. *Si U et V commutent, alors $\exp(U+V) = \exp(U)\exp(V)$.*

Démonstration. Soit $n \in \mathbb{N}$, comme les deux matrices commutent,

$$\frac{(U+V)^n}{n!} = \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} U^k V^{n-k} = \sum_{i+j=n} \frac{1}{i!} U^i 1j! V^j$$

$exp(U+V)$ est le produit de Cauchy de $exp(U)$ et de $exp(V)$, donc on a le résultat. □

Corollaire 1.3. exp *est à valeur dans* $GL_n(\mathbb{C})$ *:* M *et* $-M$ *commutent,* $M+(-M)=0$, $\exp(0)=I_n$.

Proposition 1.4. *Si* $P \in GL_n(\mathbb{C})$ *et* $A \in (M_n(\mathbb{C})$*, alors* $exp(P^{-1}AP) = P^{-1}\exp(A)P$.

Démonstration. Continuité du morphisme d'algèbre $A \mapsto P^{-1}AP$. □

Proposition 1.5.

$$\exp(Tr(A)) = \det(\exp(A)).$$

$$\exp(Sp(A)) = Sp(\exp(A)).$$

Démonstration. On trigonalise, et on sait ce qu'il se passe sur la diagonale, plus la proposition précédente. □

Remarque. Si on considère exp : $M_n(\mathbb{C}) \to GL_n(\mathbb{C})$, alors $\exp\left(\begin{bmatrix} 2i\pi & 0 \\ 0 & 2i\pi \end{bmatrix}\right) = I_2 = \exp(0)$.

2 Calcul de l'exponentielle

La référence est un document sur la page de Richard Leroy. Il y a quelques cas où l'on peut calculer explicitement l'exponentielle d'une matrice donnée.

2.1 Cas où l'on peut reconnaître des séries entières

En voici un exemple. On pose $A = A_t = \begin{bmatrix} 0 & -t \\ t & 0 \end{bmatrix}$. Alors, on montre que $A^{2k} = \begin{bmatrix} (-1)^k t^{2k} & 0 \\ 0 & (-1)^k t^{2k} \end{bmatrix}$ et $A^{2k+1} = \begin{bmatrix} 0 & (-1)^k t^{2k+1} \\ (-1)^k t^{2k+1} & 0 \end{bmatrix}$.

Ainsi, $e^{A_t} = \begin{bmatrix} cos(t) & -sin(t) \\ sin(t) & cos(t) \end{bmatrix}$.

2.2 Cas nilpotent

On est réduit à une somme finie.

2.3 Cas diagonalisable, si l'on connaît les valeurs propres

On peut utiliser la proposition 1.4, si l'on connaît les valeurs propres, et diagonaliser notre matrice. Ceci nécessite de calculer les matrices de passages, ce qui peut se révéler un petit peu "tricky" et fastidieux si l'on n'y est pas habitué... (note : voir le Paugam si l'on n'est pas très à l'aise avec le concept de matrice de passage).

Il existe une méthode plus simple (appréciée par le jury) qui se fonde sur l'interpolation de Lagrange.

Soit A une matrice diagonalisable sur $\mathbb{C}$, et soit $\lambda_1, \ldots, \lambda_n$ ses valeurs propres (complexes, non nécessairement distinctes).

Alors :

$$\exists P \in GL_n(\mathbb{C}, A = P^{-1} Diag(\lambda_1, \ldots, \lambda_n) P = P^{-1} D P.$$

On peut trouver un polynôme $Q \in \mathbb{C}[X]$ tel que $\exp(A) = Q(A)$. Cela existe vu la proposition 1.1, mais pour une matrice diagonale, on peut être explicite.

En effet, si $Q \in \mathbb{C}[X]$, alors $Q(A) = P^{-1} Q(D) P$. Il suffit de trouver Q tel que

$$Q(D) = Diag(Q(\lambda_1), \ldots, Q(\lambda_n)) = Diag(e^{\lambda_1, \ldots, \lambda_n}) = \exp(D).$$

Cela se fait très bien par interpolation de Lagrange : $Q = \sum_{i=1}^{n} e^{\lambda_i} P_i$ avec $P_i = \prod_{j=1,\ldots,n,\, j \neq i} \frac{X - \lambda_j}{\lambda_i - \lambda_j}$.

Au final, $Q(A) = P^{-1} Q(D) P = P^{-1} \exp(D) P = \exp(A)$, ce que l'on souhaitait.

Exemple. On reprend l'exemple précédent.

On trouve $Spec(A) = \{it, -it\}$.

Alors, on calcule comme polynôme interpolateur $Q(X) = \frac{\sin(t)}{t} X + \cos(t)$. On en déduit alors directement : $e^{A_t} = \begin{bmatrix} cos(t) & -sin(t) \\ sin(t) & cos(t) \end{bmatrix}$.

3 Dunford et exponentielles

3.1 Calcul et diagonalisabilité

La décomposition de Dunford est bien adaptée à l'étude de l'exponentielle d'une matrice : on peut ramener certains problèmes à l'étude du cas diagonale et du cas nilpotent. C'est le cas pour le calcul ici.

Si $A \in M_n(\mathbb{C})$ et $A = D + N$ sa décomposition de Dunford, alors $\exp(A) = \exp(D) \exp(N)$. On est ramené au cas précédent.

Proposition 3.1. *On trouve alors que la décomposition de Dunford de e^A est $e^A = e^D + e^D(e^N - I_n)$.*

Démonstration. D et N sont des polynômes en A, et avec 1.1, il en est de même des deux termes de la somme. Le premier est bien diagonalisable (1.4) et le second est bien nilpotent. En effet, $Spec(e^N) = \{1\}$ et donc $Spec(e^D(e^N - I_n)) = \{0\}$, ce qui donne le fait que cette matrice est nilpotente. On conclut par unicité. □

Théorème 3.2. *Soit $A \in M_n(\mathbb{C})$, alors A est diagonalisable si et seulement si $\exp(A)$ est diagonalisable.*

Démonstration. Le sens direct est évident vu la proposition 1.4.

Pour la réciproque, on utilise la décomposition de Dunford que l'on vient de voir. On a alors, par unicité, $e^N = I_n$.

Soit a l'indice de nilpotence de N. Son polynôme minimal est X^a, mais alors, si $a > 1$, on a $e^N = I_n$ qui peut s'écrire $I_n + N + \cdots + \frac{1}{a-1}N^{a-1} + 0 = I_n$ et alors $N + \cdots + \frac{1}{a-1}N^{a-1} = 0$ ce qui contredit la définition du polynôme minimal ($a-1 < a$...). D'où $a = 1$ et $N = 0$ et le résultat est montré. $\square$

Corollaire 3.3. $\exp(A) = I_n \Leftrightarrow A$ *est diagonalisable et* $Spec(A) \subset 2i\pi\mathbb{Z}$.

3.2 une première démonstration de surjectivité de l'exponentielle

Théorème 3.4. *Soit* A $GL_n(\mathbb{C})$, *alors il existe* $P \in \mathbb{C}[X]$ *tel que* $A = \exp(P(A))$.

Démonstration. On utilise à nouveau la décomposition de Dunford $A = D + N$ que l'on réécrit $A = D(I_n + D^{-1}N)$.

D est diagonalisable, il est facile de l'écrire comme l'exponentielle d'une matrice polynôme en A en faisant une interpolation de Lagrange, mais cette fois-ci avec un log (complexe) des λ_i ses valeurs propres. On remarque que ceci requiert de connaître le cas $n = 1$, mais il se déduit du cas réel, qui est évident connaissant la fonction exponentielle réelle.

Pour $I_n + D^{-1}N$, il se trouve que $D^{-1}N$ est nilpotente, donc on peut écrire le log de la matrice unipotente $I_n + D^{-1}N$, qui est une somme finie, avec pour un certain l :

$$I_n + D^{-1}N = \exp\left(\sum_{k=1}^{l} \frac{(-1)^{k-1}}{k}(D^{-1}N)^k\right).$$

On a donc le résultat étant donné que D et N sont des polynômes en A. $\square$

4 De la surjectivité de l'exponentielle

4.1 Groupes topologiques et exponentielle complexe

Théorème 4.1. *Soit* A $GL_n(\mathbb{C})$, *alors il existe* $P \in \mathbb{C}[X]$ *tel que* $A = \exp(P(A))$.

Pour cela nous allons développer la notion de groupe topologique.

Définition 4.2. Un groupe topologique est une triplet $(G, ., T)$ où $(G, .)$ est un groupe, (G, T) est un espace topologique, et ces deux notions sont compatibles : les applications $(g, h) \mapsto gh$ et $g \mapsto g^{-1}$ sont continues.

Nous allons utiliser de manière cruciale le lemme suivant :

Lemme 4.3. *Soit* G *un groupe topologique , et soit* H *un sous-groupe de* G *contenant un voisinage de* e. *Alors* H *est ouvert et fermé dans* G.

Démonstration. Montrons que H est ouvert. Par définition, on peut prendre V voisinage ouvert de e dans G qui est inclus dans H. Mais alors, si $h \in H$, on a $h \in hV \subset H \subset G$, et ainsi, hV est un voisinage ouvert de h inclus dans H (on utilise la continuité du morphisme de translation par multiplication à gauche par h...). On en déduit que H est un voisinage de chacun de ses points, donc est ouvert.

Montrons maintenant que H est fermé. On remarque que $H^c = \bigcup_{g \notin H} gV$ et que si $g \notin H$, $gV \subset H^c$. Comme gV est ouvert pour tout g, H^c est ouvert, et le résultat est montré.

□

Démonstration. On considère la sous-algèbre $\mathbb{C}[A]$ de $M_n(\mathbb{C})$ engendrée par A. C'est une algèbre commutative de dimension finie sur $\mathbb{C}$, isomorphe à $\mathbb{C}[X]/(\Pi)$ avec Π le polynôme minimal de A.

- Pour toute matrice M de $\mathbb{C}[A]$, on a $\exp(M) \in \mathbb{C}[A]$ (avec 1.1, mais aussi $\exp(M) \in GL_n(\mathbb{C})$. On note que l'inverse de $\exp(M)$ est $\exp(-M)$ et est donc aussi bien dans $\mathbb{C}[A]$.
- Tout les éléments de $\mathbb{C}[A]$ commutent, on en déduit que exp induit un homomorphisme du groupe additif de $\mathbb{C}[A]$ dans le groupe multiplicatif U des inversibles de $\mathbb{C}[A]$.
- Montrons que l'image de ce morphisme, $\exp(\mathbb{C}[A])$ est un ouvert-fermé de U. La différentielle de $\exp : \mathbb{C}[A] \to U \subset \mathbb{C}[A]$ en $0 \in \mathbb{C}[A]$ est l'identité de $\mathbb{C}[A]$, qui est bien inversible. On peut donc appliquer le théorème d'inversion locale : exp réalise un difféomorphisme entre un voisinage ouvert V_0 de 0 et un voisinage ouvert V de $I_n \subset U \subset \mathbb{C}[A]$.
  Par le lemme précédent, $\exp(\mathbb{C}[A])$ est alors un ouvert-fermé de U.
- Il nous reste à donner un argument de connexité pour conclure : U est connexe.
  En effet, si M et N sont dans U, alors la droite complexe formée des points $zM + (1-z)N$ ne rencontre $\mathbb{C}[A] \setminus U$ qu'en un nombre fini de points : les zéros du polynôme $\det(zM + (1-z)N)$, dont ne font pas partie 0 et 1. Or, la droite complexe $\mathbb{C}$ privée d'un nombre fini de points est connexe par arcs. On en déduit qu'il existe un chemin continu contenu dans U entre M et N. Ainsi, U est connexe par arc, donc connexe.
- En conclusion, $\exp(\mathbb{C}[A])$ est alors un ouvert-fermé de U, qui est connexe. On a donc le résultat : $\exp(\mathbb{C}[A]) = U$.

□

Remarque. On a aussi montré ici le cas $n = 1$.

Remarque. L'essentiel des lemmes se trouvent dans le Nourdin [7] et le Mneimné-Testard [2].

Corollaire 4.4. *Si $A \in GL_n(\mathbb{C})$ et $p \in \mathbb{N}^*$, il existe $B \in GL_n(\mathbb{C})$ tel que $A = B^p$.*

4.2 Le cas réel

On n'a pas cette fois-ci de surjectivité de exp : $M_n(\mathbb{R}) \to GL_n(\mathbb{R})$. En effet, exp est continue et $GL_n(\mathbb{R})$ a deux composantes connexes (*cf* la décomposition polaire et [2]) tandis que $M_n(\mathbb{R})$ est connexe.

Cela dit, une application amusante du résultat complexe permet de donner une caractérisation :

Proposition 4.5. *Soit A une matrice de $GL_n(\mathbb{R})$, montrer qu'il existe une matrice réelle M telle que $A = e^M$ si et seulement si il existe une matrice réelle B telle que $A = B^2$.*

Démonstration. Le sens direct est évident.

Maintenant, soit $A \in GL_n(\mathbb{R})$ telle qu'il existe une matrice réelle B telle que $A = B^2$, et soit B une telle matrice.

Remarquons que $B \in GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ donc le théorème de surjectivité précédent permet de dire qu'il existe un polynôme $Q \in \mathbb{C}[X]$ tel que $B = \exp(Q(B))$.

Mais alors, on a aussi, comme B est une matrice réelle, $B = \overline{B} = \overline{\exp(Q(B))} = \exp(\overline{Q}(B))$. Ainsi, $A = B^2 = B \times B = B \times \overline{B} = \exp(Q(B)) \times \exp(\overline{Q}(B))$. Comme tout commute comme polynôme en B, on a donc $A = \exp(Q(B) + \overline{Q}(B)) = \exp((Q + \overline{Q})(B))$, et $Q + \overline{Q} \in \mathbb{R}[X]$, B est réelle, donc on a bien le résultat. □

4.3 Autre application

Proposition 4.6. *$GL_n(\mathbb{C})$ n'admet pas de sous-groupes arbitrairement petits.*

Démonstration. On montre qu'il existe un voisinage V de I_n dans $GL_n(\mathbb{C})$ tel que le seul sous-groupe contenu dans V soit $\{I_n\}$.

Soit V un voisinage de I_n dans $GL_n(\mathbb{C})$ et U un voisinage de 0 dans $M_n(\mathbb{C})$ tel que exp réalise un difféomorphisme de U sur V.

On pose $U' = \frac{U}{2}$ et $V' = \exp(U)$.

V' est ouvert, c'est un voisinage de I_n.

Soit $M \in V'$. On va montrer qu'il existe $k \in \mathbb{N}$ tel que $M^k \notin V'$, ce qui permettra de conclure.

On peut écrire $M = \exp(A)$ avec $A \in U'$. Il existe alors $k \in \mathbb{N}$ tel que $kA \in U \setminus U'$. On a alors $\exp(kA) = M^k \in V \setminus V'$ et donc $M^k \notin V'$, ce que l'on souhaitait démontrer. □