Leçon 127: Exponentielle de matrices

Aurélien Sagnier, Gautier Delannoy

18 mars 2012

Dans la suite, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$

1 Définitions, premières propriétés, calcul

1.1 Définition, régularité [M-T]

Définition 1. *Soit $A \in M_n(\mathbb{K})$. La série $\displaystyle\sum_{n=0}^{+\infty} \frac{A^n}{n!}$ est normalement convergente sur tout compact ; donc a un sens. On l'appelle exponentielle de la matrice A, et on la note $exp(A) = e^A$.*

Proposition 2. $\forall A \in M_n(\mathbb{K}), \exists P \in \mathbb{K}[X], e^A = P(A)$

Proposition 3. *L'application $A \mapsto e^A$ est C^∞, sa différentielle en 0 est l'identité.*

Proposition 4. *Soient $A, B \in M_n(\mathbb{K})$ deux matrices qui commutent. Alors*

$$e^{A+B} = e^A e^B$$

Proposition 5. *Soit $P \in GL_n(\mathbb{K}), A \in M_n(\mathbb{K})$.*

$$Pe^A P^{-1} = e^{PAP^{-1}}$$

Ainsi, quite à trigonaliser une matrice, on peut exprimer de déterminant de l'exponentielle d'une matrice :

$$\forall A \in M_n(\mathbb{K}), det(e^A) = e^{Tr(A)}$$

1.2 Image, Inversion [M-T]

On remarque immédiatement que l'application exponentielle est à valeurs dans $GL_n(\mathbb{K})$, son inverse étant $exp(A)^{-1} = exp(-A)$. En fait, on peut caractériser plus précisément son image :

Théorème 6.
- *Si $\mathbb{K} = \mathbb{C}$, alors*
  $exp : M_n(\mathbb{C}) \to GL_n(\mathbb{C})$ *est surjective*
- *Si $\mathbb{K} = \mathbb{R}$, alors*
  $exp : M_n(\mathbb{R}) \to \{M^2, M \in GL_n(\mathbb{R})\}$ *est surjective*

Nous cherchons dans la suite de cette partie à inverser cette application. En vertu de la proposition 3, on a immédiatement le résultat suivant, grâce au théorème d'inversion locale :

Proposition 7. *Il existe des voisinages U de 0 et V de I_n dans $GL_n(\mathbb{K})$ tels que :*
$exp : U \to V$ soit un C^1 difféomorphisme.

Corollaire 8. *$GL_n(\mathbb{K})$ n'a pas de sous-groupe arbitrairement petit.*

On peut être plus précis sur cette inversion. Nous suivrons ici [Far](p26) :

Définition 9. *Soit $A \in B(I_n, 1)$. On appelle logarithme de A, noté $log(A)$ la série absolument convergente :*

$$log(A) = \sum_{k=1}^{+\infty} \frac{(-1)^{k+1}}{k} (g - I_n)^k$$

Théorème 10. *1. $\forall A \; inB(I_n, 1)$*
$exp(log(A)) = A$

2. $\forall A \; inB(0, ln(2))$
$log(exp(A)) = A$

1.3 Calcul effectif

Théorème 11 (Décomposition de Dunford ([Gou] p192))**.** *Soit $A \in M_n(\mathbb{C})$. Il existe un unique couple (D, N) tels que :*

i) $A = D + N$

ii) $DN = ND$

iii) D est diagonalisable et N est nilpotente.

Corollaire 12. *A est diagonalisable ssi $exp(A)$ est diagonalisable*

Nous allons utiliser la décomposition de Dunford pour calculer l'exponentielle d'une matrice. Soit $A \in M_n(\mathbb{K})$, D et N comme dans le théorème. On a alors :

$$e^A = e^D e^N$$

Or,

1) N étant nilpotente, si on note q son indice de nilpotence, on a :

$$e^N = \sum_{k=0}^{q-1} \frac{N^p}{p!}$$

2) D étant diagonalisable,notons $\lambda_1, ..., \lambda_n$ ses valeurs propres. on a deux moyens de calculer son exponentielle :

   a) Si on connait une base de diagonalisation, soit P la matrice de passage. On a

$$e^D = P \begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix} P^{-1}$$

   b) Soit Π un polynôme interpolateur tel que $\Pi(\lambda_i) = e^{\lambda_i}$. Alors $e^A = \Pi(A)$.

2 Applications aux équations différentielles [Dem]

2.1 Systèmes différentiels

Proposition 13.

$$\frac{d}{dt}(exp(tA)) = A.exp(tA) \ \forall t \in \mathbb{R}, \forall A \in M_n(\mathbb{K})$$

Théorème 14. *Soit $A \in M_n(\mathbb{K})$. Alors le système différentiel* $\begin{cases} X' = AX \\ X(0) = X_0 \end{cases}$ *a une unique solution définie pour tout $t \in \mathbb{R}$, donnÃ©e par :*

$$X(t) = exp(tA).X_0$$

Corollaire 15. *On appelle sous-groupe à un paramètre de $GL_n(\mathbb{K})$ les morphismes continues de groupe de $\mathbb{R}$ dasn $GL_n(\mathbb{K})$. Les sous-groupes à un paramètre de $GL_n(\mathbb{K})$ sont de la forme $t \mapsto exp(tA)$.*

2.2 Approche qualitative

On rappelle ici les notions liées à la stabilité d'un système différentiel autonome : Prenons U un ouvert de $\mathbb{R}^n$, $f : U \to \mathbb{R}^n$ une fonction de classe C^1.
on considère le système différentiel autonome :

$$\begin{cases} y' = f(y) \\ y(0) = y_0 \end{cases} \tag{1}$$

Soit x un point d'équilibre de ce système ($f(x) = 0$).

- x est stable si

$$\forall \varepsilon > 0, \exists \eta > 0, \|y_0 - x\| < \eta \Rightarrow (\forall t > 0, \|y(t) - x\| < \varepsilon$$

- x est asymptotiquement stable, si de plus,

$$\lim_{t \to +\infty} \|y(t) - x\| = 0$$

Théorème 16 (stabilité de Lyapunov)**.** *Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ de classe C^1 telle que $f(0) = 0$ et $df(0)$ ait des valeurs propres de parties réelles strictement négatives. Alors 0 est asymptotiquement stable pour le système (1).*

Pour cela on démontre en fait les lemmes suivants.

Définition 17. *Soit $F : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ continue, localement lipschitzienne en la seconde variable et telle que $\forall t \in \mathbb{R}, F(t,0) = 0$. Soient $R > 0$ et $V : \mathbb{R}^+ \times B(0,R) \to \mathbb{R}$, on dit que V est une fonction de Lyapunov si*

1. *V est $\mathcal{C}^1$ et $\forall t \in \mathbb{R}^+, V(t,0) = 0$*
2. *il existe $W : B(0,R) \to \mathbb{R}^+$ continue telle que $\forall t, x, W(x) \leq V(t,x)$*
3. *$W(x) = 0 \Leftrightarrow x = 0$*
4. *l' expression $\tilde{V} := \frac{\partial V}{\partial t} + \langle F, \frac{\partial V}{\partial x} \rangle$ est négative ou nulle sur $\mathbb{R}^+ \times B(0,R)$*

Lemme 1. *Soit $F : \mathbb{R}^+ \times \mathbb{R}^n \to \mathbb{R}^n$ continue, localement lipschitzienne en la seconde variable et telle que $\forall t \in \mathbb{R}, F(t,0) = 0$. S'il existe $R > 0$ et $V : \mathbb{R}^+ \times B(0,R) \to \mathbb{R}$ telle que V soit une fonction de Lyapunov, alors la solution nulle est stable. Si en plus V vérifie :*

1. *il existe $\tilde{W} : B(0,R) \to \mathbb{R}^-$ continue telle que $\forall t, x, \tilde{V}(t,x) \leq \tilde{W}(x)$*
2. *$\tilde{W}(x) = 0 \Leftrightarrow x = 0$*

3. $\lim_{x\to 0}\sup_{t\geq 0} V(t,x) = 0$ *Alors la solution nulle est asymptotiquement stable.*

Démonstration. 1. D'abord la stabilité :

Soit V une fonction de Lyapunov du système (on a supposé qu'il en existait).

Pour toute solution $x(t)$, on a $\frac{d}{dt}V(t,x(t)) = \tilde{V}(t,x(t))$, donc V décroit le long des trajectoires.

Soit $\epsilon \in]0,R[$, posons $\alpha = \min_{||z||=\epsilon} W(x)$. Comme $V(0,0)=0$ et que V est continue, soit $\eta > 0$ tel que $\forall z \in B(0,\eta), V(0,z) < \alpha$. Soit $x(t)$ une solution telle que $x(0) \in B(0,\eta)$, alors la trajectoire ne peut sortir de $B(0,\eta)$ Ã cause de l'inégalité entre V et W et du fait que v décroit le long des trajectoires.

2. Maintenant la stabilité asymptotique en supposant les hypothèses supplémentaires sur V :

Déjà 0 est stable, il ne reste plus qu' à montrer que toutes les trajectoires tendent vers 0.

Par l'absurde soit $x(t)$ une solution avec $x(0) < \eta$ avec η comme précédemment qui ne tend pas vers 0 quand t tend vers $+\infty$. Soient alors $\xi \in]0,\eta[$ et $(t_n) \in \mathbb{R}^{\mathbb{N}}$ tendant vers $+\infty$ et telle que $\forall n \in \mathbb{N}, ||x(t_n)|| \geq \xi$. Posons $\beta = \inf_{\xi \leq z \leq \eta} W(x)$, alors $\forall n \in \mathbb{N}, V(t_n, x(t_n)) \geq \beta$. D'après 3 soit $\lambda > 0$ tel que pour tout $|z| < \lambda$ et $t \geq 0$ on a $V(t,z) < \beta$. Comme V est décroissante le long des trajectoires, on a $\forall t \in \mathbb{R}^+, V(t,x(t)) \geq \beta$, donc la trajectoire reste dans la couronne $\lambda \leq z \leq \eta$. Mais sur cette couronne W est strictement négative et continue donc majorée par un $M < 0$.

Or pour tout $t \in \mathbb{R}^+$ $\frac{d}{dt}V(t,x(t)) = \tilde{V}(t,x(t)) \leq \tilde{W}(x(t)) \leq M$ donc $V(t,x(t)) \to_{t\to\infty} -\infty$, ce qui est absurde car V est positive.

□

Lemme 2. *Soit $A \in M_n(\mathbb{R})$. Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres distinctes de A. Alors il existe $C > 0$ tel que $\forall (t,x) \in \mathbb{R}^+ \times \mathbb{R}^n, ||e^{tA}x||_2 \leq C(1 + |t|^{n-1})\left(\sum_{i=1}^k e^{t\Re(\lambda_i)}\right)||x||_2$.*

Démonstration. Par le lemme des noyaux et comme $\mathbb{C}$ est algébriquement clos, $\mathbb{C}^n = \bigoplus_{i\in[|1,k|]} \ker(A-\lambda_i I)^{m_i}$. On a alors pour $i \in [|1,k|]$

$$e^{tA}x_i = e^{t\lambda_i}\left(\sum_{0\leq j\leq m_i} \frac{t^j}{j!}(A-\lambda_i I)^j\right) x_i$$

Donc en utilisant la formule du binome et la définition de l'exponentielle réelle, on a :

$$||e^{tA}x_i||_2 \leq e^{t\Re(\lambda_i)} e^{||A-\lambda_i I||}(1+|t|)^{m_i-1}|x_i|$$

Donc $||e^{tA}|| \leq Cste(1+|t|)^{n-1}\left(\sum_{1\leq i\leq k} e^{t\Re(\lambda_i)}\right)||x||_\infty$ et on conclut par l'équivalence des normes en dimension finie. □

Démonstration. Posons $B = \int_0^\infty e^{tA^\star}e^{tA}dt$, d'après le lemme précédent B est bien définie.

On a alors $A^\star B + BA = -I$, $B^\star = B$ et $\forall x \in \mathbb{R}^n \backslash \{0\}, < x|Bx >> 0$, donc B est symétrique définie et positive.

Posons pour tout $(t,x) \in \mathbb{R}^+ \times \mathbb{R}^n, V(t,x) =< x|Bx >$.

Alors V est bien $\mathcal{C}^1$, positive et nulle seulement en 0, on peut poser $W = V$.

De plus pour tout $t,x) \in \mathbb{R}^+ \times \mathbb{R}^n$, $\tilde{V}(t,x) =< Ax + q(t,x)|Bx > + < x|B(Ax + q(t,x)) >= - < x,x > +2 < q(t,x)|Bx >$. Or $q(t,x) = o(||x||)$ uniforme en t, donc $< q(t,x)|Bx >= o(||x||^2)$ uniforme en t.

Donc soit $\alpha > 0$ tel que pour tout $||x|| \leq \alpha$, $\tilde{V} \leq -\frac{1}{2}||x||^2$.

Donc V est une fonction de Lyapunov qui vérifie les hypothèses supplémentaires du premier lemme, donc 0 est asymptotiquement stable. □

On peut à présent conclure :

Démonstration. Pour tout $x \in \mathbb{R}^n$, on a $F(x) = dF(0)x + q(x)$ avec $q(x) = o(||x||)$, on applique alors le théorème. □

3 Etudes des groupes classiques

3.1 Homéomorphisme induits par l'exponentielle

Théorème 18. *L'exponentielle est un homéomorphisme des matrices nilpotentes d'ordre p sur les matrices unipotentes d'ordre p.*

Théorème 19. *$exp : S_n(\mathbb{R})$ (resp. $H_n(\mathbb{R})$) $\to S_n^{++}(\mathbb{R})$ (resp $S_n(\mathbb{R})$) est un homéomorphisme. On en déduit les homéomorphismes suivants (liés à la décomposition polaire) :*

$$\begin{aligned} GL_n(\mathbb{R}) &\cong O(n) \times \mathbb{R}^{\frac{n(n+1)}{2}} \\ GL_n(\mathbb{C}) &\cong U(n) \times \mathbb{R}^{n^2} \end{aligned}$$

3.2 Algèbres de Lie

Définition 20. *Soit G un sous-groupe fermé de $GL_n(\mathbb{K})$. Soit $\mathfrak{g} = \{X \in M_n(\mathbb{K}), exp(tX) \in G, \forall t \in$ $\mathfrak{g}$ est l'algèbre de Lie du groupe G.*

On conservera ces notations dans toute cette sous-partie.

Proposition 21. *$\mathfrak{g}$ est un sous-espace vectoriel de $M_n(\mathbb{K})$, stable par l'application crochet de Lie : $(X, Y) \mapsto XY - YX$.*

Théorème 22 (Cartan-Von Neumann)**.** *Soit G un sous-groupe fermé de $GL_n(\mathbb{K})$. Alors G est une sous-variété réelle de $M_n(\mathbb{K})$. De plus, $\mathfrak{g}$ est l'espace tangeant en à G en I_n.*

On a $0 \in \mathfrak{g}$ et si G est discret, $\mathfrak{g} = \{0\}$, on montre maintenant que si G n'est pas discret $\mathfrak{g} \backslash \{0\} \neq \emptyset$

Lemme 3. *Soit $(h_n) \in G^{\mathbb{N}}$ telle que $h_n \to_{n\to\infty} I$ et $\forall n \in \mathbb{N}, h_n \neq I$. Soit h une valeur d'adhérence de la suite $\left(\frac{\lg h_n}{||\lg h_n||}\right)$ (qui est une suite de la sphère unité de $M_n(K)$ (compacte donc on peut en effet trouver un tel h)), alors $h \in \mathfrak{g}$.*

Démonstration. Quitte à extraire, on suppose que $\frac{\lg h_n}{||\lg h_n||}$ converge vers h. on veut montrer que $h \in \mathfrak{g}$ donc il suffit de calculer $\exp(th)$ pour tout $t \in \mathbb{R}$.

Soit $t \in \mathbb{R}$,

$$\exp(th) = \lim_{n\to\infty} \exp\left(t \frac{\lg h_n}{||\lg h_n||}\right) = \lim_{n\to\infty} h_n^{\lfloor \frac{\lg h_n}{||\lg h_n||} \rfloor}$$

Donc $\exp(th)$ est la limite d'une suite d'éléments de G. Comme G est fermé, $\exp(th) \in G$.

Donc $h \in \mathfrak{g}$. $\square$

Donc $\mathfrak{g} \neq \{0\}$

Lemme 4. *Soit $\mathfrak{f}$ un supplémentaire de $\mathfrak{g}$ dans $M_n(K)$, alors il existe un voisinage U de 0 dans $\mathfrak{f}$ tel que $\exp(U) \cap G = I$.*

Démonstration. Par l'absurde soit U un voisinage de 0 dans $\mathfrak{f}$ (qu'on choisit compact et étoilé par rapport Ã 0) tel que pour tout $n \in \mathbb{N}^\star$, $\exp\left(\frac{U}{n}\right) \cap G \neq \{I\}$.

Posons pour tout $n \in \mathbb{N}$, $h_n = \exp \frac{X_n}{n}$ avec $X_n \in U$ et $h_n \in G$ donc $h_n \neq I$. Comme U est borné, $\left(\frac{X_n}{n}\right)$ tend vers 0, donc (h_n) tend vers I, et pour n assez grand $\frac{\lg h_n}{||\lg h_n||} = \frac{X_n}{||X_n||} = y_n$. Donc la suite (y_n) possède une valeur d'adhérence h de norme 1 qui appartient à $\mathfrak{F}$ et Ã $\mathfrak{g}$, absurde. □

Lemme 5. *Il existe un voisinage V de 0 dans $\mathfrak{g}$, un voisinage W de I dans G, tels que* $\exp$ *réalise un difféomorphisme de V dans W.*

Démonstration. Soit $\mathfrak{g}'$ un supplémentaire de $\mathfrak{g}$ dans $M_n(K)$

Posons $\Phi : \mathfrak{g} \times \mathfrak{g}' \to GL(n, K), (X, X') \mapsto \exp(X)\exp(X')$. La différentielle de Φ en $(0,0)$ est l'application $(X, X') \mapsto X + X'$ qui est une application bijective.

Donc par le théorème d'inversion locale, soit U un voisinage ouvert de 0 dans $\mathfrak{g}$, U' un voisinage ouvert de 0 dans $\mathfrak{g}'$ et V un voisinage ouvert de I dans $GL(n, K)$ tels que Φ réalise un difféomorphisme entre $U \times U'$ et V.

D'après le lemme précédent soit U'' un voisinage ouvert de 0 dans $\mathfrak{g}'$ tel que $\exp(U'') \cap G = \{I\}$. Posons $\tilde{U} = U' \cap U''$, c'est un voisinage ouvert de 0 dans $\mathfrak{g}'$ et posons $\tilde{V} = \Phi(U \times \tilde{U})$, c'est un voisinage ouvert de I dans $GL(n, K)$ et Φ réalise un difféomorphisme de $U \times \tilde{U}$ dans $\tilde{V}$.

De plus $\tilde{V} \cap G = \exp(U)$, donc $\exp(U)$ est un voisinage ouvert de I dans G, cqfd. □

Démonstration. On a vérifié la définition de sous variété juste pour le point I de G, mais comme on peut aller de I à tout point de G par un difféomorphisme (multiplication à gauche), cqfd. De plus on a que la dimension de G est $\dim \mathfrak{g}$. □

Exemples :

i) $SO(n)$ est une sous-variété de $\mathbb{R}^{n^2}$ et de plus, son espace tangeant en l'identité est :

$$\overrightarrow{T_{SO(n)}I_n} = \{\text{ Matrices antisymetriques}\}$$

ii) $SL_n(\mathbb{K})$ est une sous-variété de $\mathbb{K}^{n^2}$ et son espace tangeant en l'identité est :

$$\overrightarrow{T_{SL_n(\mathbb{K})}I_n} = \{\, M \in M_n(\mathbb{K}), Tr(M) = 0\}$$

Références

[M-T] Mneimné-Testard, *Introduction à la théorie des groupes de Lie classique*

[Gou] Gourdon, *Algèbre*

[Dem] Demailly, *Analyse numérique et équation différentielle*

[Far] Faraut, *Analyse sur les groupes de Lie*

[GT] Gonnord-Tosel, *Calcul différentiel pour l'agrégation*