

Exponentielle de matrices : correction

Exercice 1.

1. Les polynômes en A forment la \mathbf{C} -algèbre $\mathbf{C}[A] \subseteq M_n(\mathbf{C})$. La \mathbf{C} -algèbre $M_n(\mathbf{C})$ étant de dimension finie, $\mathbf{C}[A]$ est un fermé de $M_n(\mathbf{C})$. Puisqu'elle contient les sommes partielles $\sum_{k=0}^N A^k/k!$, elle doit en contenir la limite, donc $\exp A \in \mathbf{C}[A]$.

En outre, $\mathbf{C}[A]$ est l'image du morphisme $\mathbf{C}[X] \rightarrow M_n(\mathbf{C})$ qui associe à un polynôme P la matrice $P(A)$. À ce titre, elle est isomorphe au quotient $\mathbf{C}[X]/(\mu_A(X))$, où $\mu_A(X)$ est le polynôme minimal de A . D'après le théorème de Cayley-Hamilton, $\deg \mu_A \leq n$, ce qui montre que tout élément de $\mathbf{C}[A]$ s'écrit $P(A)$ avec un polynôme P de degré strictement inférieur à n .

2. Un même polynôme P ne peut évidemment pas convenir pour toutes les matrices. Si tel était le cas, on aurait par exemple pour tout $t \in \mathbf{R}$ l'égalité $\exp(tI_n) = e^t I_n = P(t)I_n = P(tI_n)$, ce qui contredit l'estimation $P = o(\exp)$ au voisinage de $+\infty$. En revanche, le polynôme

$$P_{\text{nil}}(X) = \sum_{k=0}^{n-1} \frac{X^k}{k!}$$

convient pour toutes les matrices nilpotentes.

Exercice 2.

1. Si $\text{Spec} A = \{a, b\}$, avec $a \neq b$, il existe une matrice $g \in \text{GL}_2(\mathbf{C})$ telle que $A = g^{-1} \text{diag}(a, b)g$. On a alors $\exp A = g^{-1} \text{diag}(e^a, e^b)g$. Si P est un polynôme envoyant a sur e^a et b sur e^b , on a donc $P(A) = P(g^{-1} \text{diag}(a, b)g) = g^{-1} \text{diag}(P(a), P(b))g = \exp A$. Il suffit alors de constater que le polynôme de degré 1

$$P(X) = \frac{e^a - e^b}{b - a}X + \frac{ae^b - be^a}{a - b}$$

convient.

2. Si $\text{Spec} A = \{a\}$, $A - aI_2$ est nilpotente et commute avec aI_2 donc

$$\exp A = \exp(A - aI_2)\exp(aI_2) = (I_2 + (A - aI_2))e^a I_2 = e^a A + (1 - a)e^a I_2.$$

Exercice 3.

1. $J_r(a) = aU$, où U est une matrice unipotente. Puisque $\exp : \mathbf{C} \rightarrow \mathbf{C}^*$ est surjective et que $\exp : \text{Nil}_n(k) \rightarrow \text{Uni}_n(k)$ est un homéomorphisme, on peut trouver $b \in \mathbf{C}$ et $N \in \text{Nil}_n(k)$ tels que $e^b = a$ et $\exp N = U$. On a alors

$$\exp(bI_r + N) = \exp(bI_r)\exp N = e^b \exp N = aU.$$

2. D'après la réduction de Jordan, tout $M \in \text{GL}_n(\mathbf{C})$ admet une diagonalisation par blocs : $PMP^{-1} = \text{diag}(B_1, \dots, B_k)$ où tous les B_i sont des blocs de Jordan. Puisque M est inversible, les coefficients diagonaux de ces blocs sont non nuls et donc, d'après la question précédente, les blocs sont dans l'image de l'exponentielle : soit C_i un antécédant de B_i . On a alors $M = \exp(P^{-1} \text{diag}(C_1, \dots, C_k)P)$.

Toute matrice inversible $M = \exp L$ est alors un carré : $M = \exp(2L/2) = \exp(L/2)^2$.

En revanche, \exp n'est pas injective : $\forall k \in \mathbf{Z}, \exp(2i\pi k I_n) = e^{2i\pi k} I_n = I_n$.

Exercice 4.

1. Si le spectre (dans \mathbf{C}) d'une matrice est $\{\lambda, \mu\}$, le spectre de son carré est $\{\lambda^2, \mu^2\}$. Si une matrice réelle avait un carré de spectre $\{-1\}$, il faudrait donc que son spectre soit $\{i, -i\}$. Elle serait alors diagonalisable sur \mathbf{C} et il en serait donc de même pour son carré. Puisque $J_2(-1)$ n'est pas diagonalisable ($-I_2$ est la seule matrice diagonalisable de spectre $\{-1\}$), on a une contradiction : $J_2(-1)$ n'est le carré d'aucune matrice réelle.
2. L'exponentielle de la matrice $A \in M_n(\mathbf{R})$ est le carré de la matrice réelle $\exp(A/2)$. La matrice $J_2(-1)$ n'est donc l'exponentielle d'aucune matrice réelle.

Exercice 5.

1. Soit S une matrice symétrique. On sait qu'il existe une matrice $O \in O_n(\mathbf{R})$ et des réels $\lambda_i \in \mathbf{R}$ tels que $S = O^{-1} \text{diag}(\lambda_1, \dots, \lambda_n)O$. La matrice $\exp S = O^{-1} \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n})O$ est alors clairement définie positive. L'exponentielle induit donc bien une application continue $\text{Sym}_n(\mathbf{R}) \rightarrow \text{SDP}_n(\mathbf{R})$.

Soit maintenant P une matrice symétrique définie positive. On peut l'écrire sous la forme $P = O^{-1} \text{diag}(\mu_1, \dots, \mu_n)O$ où $O \in O_n(\mathbf{R})$ et les μ_i sont des réels strictement positifs : on peut donc les écrire $\mu_i = e^{\lambda_i}$ pour des $\lambda_i \in \mathbf{R}$. Soit également f un polynôme réel tel que $f(\lambda_i) = \mu_i$. Si on pose $S = O^{-1} \text{diag}(\lambda_1, \dots, \lambda_n)O = f(P)$, on a bien $P = \exp S$.

Il reste maintenant à démontrer que $S = f(P)$ est le seul antécédant de P . Si S' en était un autre, on pourrait l'écrire $S' = \Omega^{-1} \text{diag}(\tau_1, \dots, \tau_n)\Omega$, où $\Omega \in O_n(\mathbf{R})$ et $\tau_i \in \mathbf{R}$ et on aurait $P = \Omega^{-1} \text{diag}(e^{\tau_1}, \dots, e^{\tau_n})\Omega$. Les e^{τ_i} sont donc les μ_i : quitte à composer Ω par une matrice de permutation (c'est-à-dire quitte à renuméroter les τ_i), on peut supposer $S' = \Omega^{-1} \text{diag}(\lambda_1, \dots, \lambda_n)\Omega$ et $P = \Omega^{-1} \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n})\Omega$: on a donc bien $S' = f(P)$.

2. Il s'agit de montrer que l'inverse de l'exponentielle est continu. Une solution est la suivante : si $P = \exp S$, $P \cdot B(I_n, 1)$ est un voisinage de P sur lequel la série entière du logarithme définit un inverse (continu) de l'exponentielle : l'unique inverse de P par l'exponentielle est en effet nécessairement $S + \log(I + P^{-1}H)$.

On peut également le démontrer à la main : soit (S_k) une suite de matrices symétriques telles que $\exp S_k \xrightarrow[k \rightarrow \infty]{} P \in \text{SDP}_n(\mathbf{R})$. On peut écrire $S_k = O_k^{-1} \text{diag}(\lambda_1(k), \dots, \lambda_n(k))O_k$ pour des suites λ_i de réels et O_k de matrices orthogonales. Puisque $O_n(\mathbf{R})$ est compact, il existe une sous-suite $O_{\varphi(k)} \xrightarrow[k \rightarrow \infty]{} \Omega \in O_n(\mathbf{R})$. On a donc

$$\text{diag}(e^{\lambda_1(\varphi(k))}, \dots, e^{\lambda_n(\varphi(k))}) \xrightarrow[k \rightarrow \infty]{} \Omega P \Omega^{-1}.$$

Les suites $\lambda_i(\varphi(k))$ convergent donc toutes, et leurs limites $\lambda_i(\infty)$ sont les logarithmes des valeurs propres de P . On a en particulier démontré que S_k admettait une valeur d'adhérence qui, par continuité de l'exponentielle, est l'unique antécédant de P .

De toute suite dont l'image converge vers $\exp S$, on peut donc extraire une sous-suite convergent vers S : il s'ensuit que l'inverse de l'exponentielle est continu en $\exp S$.

3. On obtient le même résultat en remplaçant $\text{Sym}_n(\mathbf{R})$ par les matrices hermitiennes et $\text{SDP}_n(\mathbf{R})$ par les matrices hermitiennes définies positives dans l'énoncé (et O_n par U_n dans la preuve).

Exercice 6.

1. Soit $\mathbf{\Pi} = \{\pm 1\}^{\mathbf{N}}$ le groupe (multiplicatif) des suites infinies de ± 1 , muni de la topologie produit. On sait que cet espace est métrisable, par exemple grâce à la *distance 2-adique*

$$d(\mathbf{x}, \mathbf{y}) = 2^{-\min\{i \in \mathbf{N} \mid x_i \neq y_i\}},$$

où l'on adopte la convention (naturelle) $2^{-\min \emptyset} = 2^{-\infty} = 0$. On vérifie alors sans peine que cette topologie rend la multiplication

$$\mu(\mathbf{x}, \mathbf{y}) = \mathbf{z}, \text{ avec } z_i = x_i y_i$$

et l'inversion

$$\text{inv}(\mathbf{x}) = \mathbf{x}$$

continues.

Tout voisinage de l'élément neutre \mathbf{e} défini par $e_i = 1$ contient alors une boule centrée en \mathbf{e} et notamment le sous-groupe non trivial (et même isomorphe à $\mathbf{\Pi}$)

$$\mathbf{\Pi}_{>N} = \{\mathbf{x} \in \mathbf{\Pi} \mid \forall k \in \llbracket 0, n \rrbracket, x_k = 1\} \subseteq \mathbf{\Pi}.$$

Un exemple de nature complètement différente est donné par le groupe $\text{Homéo}_c(\mathbf{R}^n)$ des homéomorphismes à support compact de \mathbf{R}^n , c'est-à-dire le groupe des homéomorphismes $f : \mathbf{R}^n \rightarrow \mathbf{R}^n$ tels qu'il existe un compact K en dehors duquel f est l'identité : $f|_{\mathbf{R}^n \setminus K} = \text{id}_{\mathbf{R}^n \setminus K}$. On peut en effet munir ce groupe de la topologie de la convergence uniforme, induite par la distance

$$d(f, g) = \max_{x \in \mathbf{R}^n} \|f(x) - g(x)\|$$

et vérifier que cela en fait bien un groupe topologique.

Pour tout ouvert borné $\Omega \subseteq \mathbf{R}^n$, le sous-groupe des homéomorphismes coïncidant avec l'identité hors de Ω est alors un sous-groupe non trivial contenu dans la boule de centre $\text{id}_{\mathbf{R}^n}$ et de rayon $\text{diam}(\Omega)$.

2. D'après le cours, l'exponentielle $\exp : M_n(\mathbf{C}) \rightarrow GL_n(\mathbf{C})$ est un homéomorphisme local au voisinage de 0. Soit donc $U \subseteq M_n(\mathbf{C})$ un voisinage de 0 et $V \subseteq GL_n(\mathbf{C})$ un voisinage de $\exp 0 = I_n$ tels que l'exponentielle réalise un difféomorphisme $U \rightarrow V$. Soit $U_0 \subseteq U$ tel que $2U_0 \subseteq U$ et V_0 l'image de U_0 par l'exponentielle.

Supposons par l'absurde que V_0 contienne un sous-groupe non trivial. Soit $N \in V_0$ un élément non trivial de ce groupe. Il admet un unique antécédant M dans U_0 . D'après les hypothèses, il existe un entier k tel que kM appartienne à $U \setminus U_0$. On a alors $\exp(kM) = M^k \in V \setminus V_0$, ce qui constitue une contradiction. $GL_n(\mathbf{C})$ n'admet donc pas de sous-groupe arbitrairement petit.

Remarque. On appelle *groupe de Lie* une variété différentielle admettant une structure de groupe pour laquelle la multiplication et l'inversion sont différentiables. Le théorème vu en cours, parfois appelé *théorème de Cartan-von Neumann*, garantit que c'est le cas des sous-groupes fermés de $GL_n(\mathbf{C})$. La preuve que nous avons donnée se retranscrit à peu près directement dans ce cadre : les groupes de Lie n'admettent pas de sous-groupes arbitrairement petit.

Un théorème difficile de Gleason, Montgomery et Zippin, datant des années 1950 et considéré par certains comme la solution du cinquième problème de Hilbert, garantit qu'un groupe topologique localement compact est en fait un groupe de Lie si et seulement s'il n'admet pas de sous-groupe arbitrairement petit.

Exercice 7.

1. Soit $A = D + N$ la décomposition de Dunford de A . On rappelle que cela signifie que D est diagonalisable, N nilpotente, et que $DN = ND$. En particulier,

$$\exp A = \exp D \cdot \exp N,$$

et $\exp D$ et $\exp N$ commutent (par exemple parce que ce sont des polynômes en D et N , respectivement). On pose alors

$$N' = \exp N - I_n = \sum_{k=1}^{n-1} \frac{N^k}{k!}.$$

La matrice N' commute alors avec $\exp D$ et est nilpotente (c'est un polynôme en N sans terme constant, donc on voit directement que $(N')^n = 0$.) On a alors

$$\exp A = \exp D \cdot (I_n + N') = \exp D + (\exp D) N'.$$

Puisque D est diagonalisable (disons $D = P \operatorname{diag}(d_1, \dots, d_n) P^{-1}$), $\exp D$ est diagonalisable ($\exp D = P \operatorname{diag}(e^{d_1}, \dots, e^{d_n}) P^{-1}$). Puisque $\exp D$ commute avec N' , $(\exp D) N'$ est nilpotente et $\exp D$ commute avec $(\exp D) N'$. L'expression $\exp A = \exp D + (\exp D) N'$ est donc bien la décomposition de Dunford de $\exp A$.

2. Supposons $\exp A = I_n$. Soit $A = D + N$ la décomposition de Dunford de A . D'après ce qui précède, la décomposition de Dunford de I_n est

$$I_n = \exp D + \exp D \sum_{k=1}^{n-1} \frac{N^k}{k!}.$$

Par unicité, cela entraîne $\exp D = I_n$ et $\exp D \sum_{k=1}^{n-1} \frac{N^k}{k!} = 0$.

La première équation est équivalente au fait que le spectre de D (et donc celui de A) est inclus dans $2i\pi\mathbf{Z}$. Pour la seconde, remarquons que

$$\begin{aligned} \exp D \sum_{k=1}^{n-1} \frac{N^k}{k!} = 0 &\Leftrightarrow \sum_{k=1}^{n-1} \frac{N^k}{k!} = 0 && \text{car } \exp D \text{ est inversible} \\ &\Leftrightarrow N \underbrace{\left(1 + \frac{N}{2} + \frac{N^2}{6} + \dots + \frac{N^{n-2}}{(n-1)!} \right)}_{N''} = 0 \\ &\Leftrightarrow N = 0 && \text{car } N'' \text{ est inversible.} \end{aligned}$$

Ainsi, la matrice A est diagonalisable, de spectre inclus dans $2i\pi\mathbf{Z}$.

La réciproque étant immédiate, on a donc que les matrices dont l'exponentielle est I_n sont exactement les matrices diagonalisables dont le spectre est inclus dans $2i\pi\mathbf{Z}$.

Exercice 8.

1. Un morphisme continu $\varphi : S^1 \rightarrow S^1$ définit en particulier un sous-groupe à un paramètre

$$\mathbf{R} \xrightarrow{\pi} S^1 \xrightarrow{\varphi} S^1 \hookrightarrow \mathbf{C},$$

où $\pi : \mathbf{R} \rightarrow S^1$ est le morphisme de groupe surjectif $t \mapsto e^{2i\pi t}$, de noyau \mathbf{Z} .

D'après le cours, il existe donc un unique élément $z \in \mathbf{C}$ tel que

$$\forall t \in \mathbf{R}, \varphi(\pi(t)) = e^{tz}.$$

Comme $\varphi(\pi(1)) = \varphi(e^{2i\pi}) = \varphi(1) = 1$, on doit avoir $e^z = 1$, c'est-à-dire qu'il existe un entier $k \in \mathbf{Z}$ tel que $z = 2i\pi \cdot k$. Ainsi, le morphisme φ associe $e^{2i\pi kt}$ à $e^{2i\pi t}$, c'est-à-dire que φ est le morphisme

$$\begin{aligned} e_k : S^1 &\rightarrow S^1 \\ \zeta &\mapsto \zeta^k. \end{aligned}$$

2. De la même façon qu'à la question précédente, si $\varphi : S^1 \rightarrow GL_n(\mathbf{C})$ est un morphisme de groupes continu, $\varphi \circ \pi : \mathbf{R} \rightarrow GL_n(\mathbf{C})$ est un sous-groupe à un paramètre. On a donc un unique élément $M \in M_n(\mathbf{C})$ tel que

$$\forall t \in \mathbf{R}, \varphi(\pi(t)) = \exp(tM).$$

On a donc en particulier $\exp M = I_n$, et l'exercice précédent entraîne qu'il existe une matrice inversible $P \in GL_n(\mathbf{C})$ et des entiers k_1, \dots, k_n tels que

$$M = P^{-1} \operatorname{diag}(2i\pi k_1, \dots, 2i\pi k_n)P.$$

On a alors

$$\forall t \in \mathbf{R}, \varphi(e^{2i\pi t}) = \exp(tM) = P^{-1} \operatorname{diag}(e^{2i\pi k_1 t}, \dots, e^{2i\pi k_n t})P$$

ou autrement dit

$$\forall \zeta \in S^1, \varphi(\zeta) = P^{-1} \operatorname{diag}(\zeta^{k_1}, \dots, \zeta^{k_n})P = P^{-1} \operatorname{diag}(e_{k_1}(\zeta), \dots, e_{k_n}(\zeta))P.$$

Remarque. On a en fait démontré un résultat analogue à un résultat bien connu de la théorie des représentations linéaires des groupes finis : toute représentation linéaire continue de S^1 se décompose en somme de *caractères linéaires*, c'est-à-dire de représentations de dimension 1. De manière générale, la théorie des représentations linéaires continues des groupes compacts est très semblable à la théorie des représentations linéaires des groupes finis (cf. par exemple *Représentations linéaires des groupes finis*, de Jean-Pierre Serre, §. 4 et exemple 5.2).