# Exponentielle de matrices : correction

**Exercice 1.**

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

   En outre, $\mathbf{C}[\mathrm{A}]$ est l'image du morphisme $\mathbf{C}[\mathrm{X}] \to \mathrm{M}_n(\mathbf{C})$ qui associe à un polynôme P la matrice P(A). À ce titre, elle est isomorphe au quotient $\mathbf{C}[\mathrm{X}]/(\mu_{\mathrm{A}}(\mathrm{X}))$, où $\mu_{\mathrm{A}}(\mathrm{X})$ est le polynôme minimal de A. D'après le théorème de Cayley-Hamilton, $\deg \mu_{\mathrm{A}} \leq n$, ce qui montre que tout élément de $\mathbf{C}[\mathrm{A}]$ 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 $\exp(t\mathrm{I}_n) = e^t\mathrm{I}_n = \mathrm{P}(t)\mathrm{I}_n = \mathrm{P}(t\mathrm{I}_n)$, ce qui contredit l'estimation $\mathrm{P} = o(\exp)$ au voisinage de $+\infty$. En revanche, le polynôme
$$\mathrm{P}_{\mathrm{nil}}(\mathrm{X}) = \sum_{k=0}^{n-1} \frac{\mathrm{X}^n}{n!}$$
convient pour toutes les matrices nilpotentes.

**Exercice 2.**

1. Si $\operatorname{Spec} \mathrm{A} = \{a, b\}$, avec $a \neq b$, il existe une matrice $g \in \mathrm{GL}_2(\mathbf{C})$ telle que $\mathrm{A} = g^{-1} \operatorname{diag}(a, b)g$. On a alors $\exp \mathrm{A} = g^{-1} \operatorname{diag}(e^a, e^b)g$. Si P est un polynôme envoyant $a$ sur $e^a$ et $b$ sur $e^b$, on a donc $\mathrm{P}(\mathrm{A}) = \mathrm{P}(g^{-1} \operatorname{diag}(a, b)g) = g^{-1} \operatorname{diag}(\mathrm{P}(a), \mathrm{P}(b))g = \exp \mathrm{A}$. Il suffit alors de constater que le polynôme de degré 1
$$\mathrm{P}(\mathrm{X}) = \frac{e^a - e^b}{b - a}\mathrm{X} + \frac{ae^b - be^a}{a - b}$$
convient.
2. Si $\operatorname{Spec} \mathrm{A} = \{a\}$, $\mathrm{A} - a\mathrm{I}_2$ est nilpotente et commute avec $a\mathrm{I}_2$ donc
$$\exp \mathrm{A} = \exp(\mathrm{A} - a\mathrm{I}_2) \exp(a\mathrm{I}_2) = (\mathrm{I}_2 + (\mathrm{A} - a\mathrm{I}_2))\, e^a\mathrm{I}_2 = e^a\mathrm{A} + (1 - a)e^a\mathrm{I}_2.$$

**Exercice 3.**

1. Soit $\mathbf{\Pi} = \{\pm 1\}^{\mathbf{N}}$ le groupe (multiplicatif) des suites infinies de $\pm 1$, muni de la topologie produit. On sait que cet espace est métrisable, par exemple grâce à la *distance* 2*-adique*
$$d(\mathbf{x}, \mathbf{y}) = 2^{-\{i \in \mathbf{N} \mid x_i \neq y_i\}},$$
où l'on adopte la convention (naturelle) $2^{-\min \varnothing} = 2^{-\infty} = 0$. 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

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

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 $\mathbf{\Pi}$)

$$\mathbf{\Pi}_{>\mathrm{N}} = \left\{ \mathbf{x} \in \mathbf{\Pi} \,\middle|\, \forall k \in [\![0, n]\!], x_k = 1 \right\} \subset \mathbf{\Pi}.$$

Un exemple de nature complètement différente est donné par le groupe $\mathrm{Homéo}_c(\mathbf{R}^n)$ des homéomorphismes à support compact de $\mathbf{R}^n$, c'est-à-dire le groupe des homéomorphismes $f : \mathbf{R}^n \to \mathbf{R}^n$ tels qu'il existe un compact K en dehors duquel $f$ est l'identité : $f_{|\mathbf{R}^n \setminus \mathrm{K}} = \mathrm{id}_{\mathbf{R}^n \setminus \mathrm{K}}$. 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 $\Omega \subset \mathbf{R}^n$, le sous-groupe des homéomorphismes coïncidant avec l'identité hors de $\Omega$ est alors un sous-groupe non trivial contenu dans la boule de centre $\mathrm{id}_{\mathbf{R}^n}$ et de rayon $\mathrm{diam}(\Omega)$.

2. D'après le cours, l'exponentielle $\exp : \mathrm{M}_n(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$ est un homéomorphisme local au voisinage de 0. Soit donc $\mathrm{U} \subset \mathrm{M}_n(\mathbf{C})$ un voisinage de 0 et $\mathrm{V} \subset \mathrm{GL}_n(\mathbf{C})$ un voisinage de $\exp 0 = \mathrm{I}_n$ tels que l'exponentielle réalise un difféomorphisme $\mathrm{U} \to \mathrm{V}$. Soit $\mathrm{U}_0 \subset \mathrm{U}$ tel que $2\mathrm{U}_0 \subset \mathrm{U}$ et $\mathrm{V}_0$ l'image de $\mathrm{U}_0$ par l'exponentielle.

   Supposons par l'absurde que $\mathrm{V}_0$ contienne un sous-groupe non trivial. Soit $\mathrm{N} \in \mathrm{V}_0$ un élément non trivial de ce groupe. Il admet un unique antécédant M dans $\mathrm{U}_0$. D'après les hypothèses, il existe un entier $k$ tel que $k\mathrm{M}$ appartienne à $\mathrm{U} \setminus \mathrm{U}_0$. On a alors $\exp(k\mathrm{M}) = \mathrm{M}^k \in \mathrm{V} \setminus \mathrm{V}_0$, ce qui constitue une contradiction. $\mathrm{GL}_n(\mathbf{C})$ n'admet donc pas de sous-groupe arbitrrairement 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 $\mathrm{GL}_n(\mathbf{C})$. 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 Glaeson, Montgomery et Zippin, datant des années 1950 et considéré par certain 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 4.**

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

   Soit maintenant P une matrice symétrique définie positive. On peut l'écrire sous la forme $\mathrm{P} = \mathrm{O}^{-1} \operatorname{diag}(\mu_1, \ldots, \mu_n)\mathrm{O}$ où $\mathrm{O} \in \mathrm{O}_n(\mathbf{R})$ et les $\mu_i$ 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 $\mathrm{S} = \mathrm{O}^{-1} \operatorname{diag}(\lambda_1, \ldots, \lambda_n)\mathrm{O} = f(\mathrm{P})$, on a bien $\mathrm{P} = \exp \mathrm{S}$.

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 $S' = \Omega^{-1}\operatorname{diag}(\tau_1, \dots, \tau_n)\Omega$, où $\Omega \in O_n(\mathbf{R})$ et $\tau_i \in \mathbf{R}$ et on aurait $P = \Omega^{-1}\operatorname{diag}(e^{\tau_1}, \dots, e^{\tau_n})\Omega$. Les $e^{\tau_i}$ sont donc les $\mu_i$ : quitte à composer $\Omega$ par une matrice de permutation (c'est-à-dire quitte à renuméroter les $\tau_i$), on peut supposer $S' = \Omega^{-1}\operatorname{diag}(\lambda_1, \dots, \lambda_n)\Omega$ et $P = \Omega^{-1}\operatorname{diag}(e^{\lambda_1}, \dots, e^{\lambda_n})\Omega$ : 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 $\exp S_k \xrightarrow[k\to\infty]{} P \in SDP_n(\mathbf{R})$. On peut écrire $S_k = O_k^{-1}\operatorname{diag}(\lambda_1(k), \dots, \lambda_n(k))O_k$ pour des suites $\lambda_i$ de réels et $O_k$ de matrices orthogonales. Puisque $O_n(\mathbf{R})$ est compact, il existe une sous-suite $O_{\phi(k)} \xrightarrow[k\to\infty]{} \Omega \in O_n(\mathbf{R})$. On a donc

$$\operatorname{diag}(e^{\lambda_1(\phi(k))}, \dots, e^{\lambda_n(\phi(k))}) \xrightarrow[k\to\infty]{} \Omega P \Omega^{-1}.$$

   Les suites $\lambda_i(\phi(k))$ 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 convergeant vers S : il s'ensuit que l'inverse de l'exponentielle est continu en $\exp S$.

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

**Exercice 5.**

Déjà, si $U \in M_n(k)$ est une matrice unipotente, on peut définir son logarithme via la série entière du logarithme, qui est dans ce cas-là un polynôme :

$$\log U = \sum_{k=1}^{n-1} (-1)^{k+1} \frac{(U - I_n)^k}{k}.$$

Cette matrice est une somme de matrices nilpotentes qui commutent, donc elle est elle-même nilpotente. On a donc une application continue $\log : \operatorname{Uni}_n(k) \to \operatorname{Nil}_n(k)$. En outre, une matrice est nilpotente (resp. unipotente) si et seulement si son spectre (dans $\mathbf{C}$) est le singleton $\{0\}$ (resp. $\{1\}$). L'exponentielle st donc une application continue $\exp : \operatorname{Nil}_n(k) \to \operatorname{Uni}_n(k)$. Il reste donc simplement à démontrer que ces deux applications sont réciproques.

Commençons par démontrer que $\log \circ \exp_{|\operatorname{Nil}_n(k)} = \operatorname{id}_{\operatorname{Nil}_n(k)}$. Pour cela, soit $N \in \operatorname{Nil}_n(k)$. Soit $f : \mathbf{R} \to \operatorname{Nil}_n(k)$ la fonction définie par $f(t) = \log(\exp(tN))$. Notons $Z(t)$ la quantité $\exp(tN) - I_n$. On a donc $Z(t) = tN + (t^2N^2)/2 + \dots + (t^{n-1}N^{n-1})/(n-1)!$ et $Z(t)$ est nilpotente et commute avec $Z'(t)$. La dérivée de $f(t)$ est alors

$$\begin{aligned}
\frac{d}{dt}f(t) &= \frac{d}{dt}\left(Z(t) - \frac{Z(t)^2}{2} + \dots + (-1)^n \frac{Z(t)^n}{n}\right) \\
&= Z'(t) - Z'(t)Z(t) + \dots + (-1)^{n+1}Z'(t)Z(t)^{n-1} \\
&= Z'(t)\,(1 + Z(t))^{-1} \\
&= N\exp(tN)(\exp(tN))^{-1} \\
&= N \\
&= \frac{d}{dt}(tN).
\end{aligned}$$

La fonction $f(t)$ a donc la même dérivée que $t\mathrm{N}$, et elles coïncident par ailleurs en 0. On a donc pour tout $t \in \mathbf{R}$, $f(t) = t\mathrm{N}$ et en particulier

$$\log(\exp \mathrm{N}) = \mathrm{N}.$$

Le cours garantit que $\exp \circ \log = \mathrm{id}$ sur un voisinage de $\mathrm{I}_n$. Si $\mathrm{N} \in \mathrm{Nil}_n(k)$, l'application

$$\begin{array}{ccc} \mathbf{R} & \to & \mathrm{M}_n(k) \\ t & \mapsto & \exp(\log(\mathrm{I}_n + t\mathrm{N})) - (\mathrm{I}_n + t\mathrm{N}) \end{array}$$

est alors une application polynomiale nulle sur un voisinage de 0. Elle est donc identiquement nulle, ce qui implique $\exp(\log(\mathrm{I}_n + \mathrm{N})) = \mathrm{I}_n + \mathrm{N}$. On a donc

$$\forall \mathrm{U} \in \mathrm{Uni}_n(k), \exp(\log \mathrm{U}) = \mathrm{U}.$$

L'exponentielle et le logarithme sont des homéomorphismes réciproques entre les ensembles de matrices nilpotentes et unipotentes.

**Exercice 6.**

1. $\mathrm{J}_r(a) = a\mathrm{U}$, où U est une matrice unipotente. Puisque $\exp : \mathbf{C} \to \mathbf{C}^*$ est surjective et que $\exp : \mathrm{Nil}_n(k) \to \mathrm{Uni}_n(k)$ est un homéomorphisme, on peut trouver $b \in \mathbf{C}$ et $\mathrm{N} \in \mathrm{Nil}_n(k)$ tels que $e^b = a$ et $\exp \mathrm{N} = \mathrm{U}$. On a alors
$$\exp(b\mathrm{I}_r + \mathrm{N}) = \exp(b\mathrm{I}_r) \exp \mathrm{N} = e^b \exp \mathrm{N} = a\mathrm{U}.$$
2. D'après la réduction de Jordan, tout $\mathrm{M} \in \mathrm{GL}_n(\mathbf{C})$ admet une diagonalisation par blocs : $\mathrm{PMP}^{-1} = \mathrm{diag}(\mathrm{B}_1, \dots, \mathrm{B}_k)$ où tous les $\mathrm{B}_i$ 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 $\mathrm{C}_i$ un antécédant de $\mathrm{B}_i$. On a alors $\mathrm{M} = \exp\left(\mathrm{P}^{-1} \mathrm{diag}(\mathrm{C}_1, \dots, \mathrm{C}_k)\mathrm{P}\right)$.
Toute matrice inversible $\mathrm{M} = \exp \mathrm{L}$ est alors un carré : $\mathrm{M} = \exp(2\mathrm{L}/2) = \exp(\mathrm{L}/2)^2$.
En revanche, exp n'est pas injective : $\forall k \in \mathbf{Z}, \exp(2i\pi k\mathrm{I}_n) = e^{2i\pi k}\mathrm{I}_n = \mathrm{I}_n$.

**Exercice 7.**

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 $\mathrm{J}_2(-1)$ n'est pas diagonalisable ($-\mathrm{I}_2$ est la seule matrice diagonalisable de spectre $\{-1\}$), on a une contradiction : $\mathrm{J}_2(-1)$ n'est le carré d'aucune matrice réelle.
2. L'exponentielle de la matrice $\mathrm{A} \in \mathrm{M}_n(\mathbf{R})$ est le carré de la matrice réelle $\exp(\mathrm{A}/2)$. La matrice $\mathrm{J}_2(-1)$ n'est donc l'exponentielle d'aucune matrice réelle.