Surjectivité de l'exponentielle

Leçons : 156, 204, *153, 214, 215*

[Zav], problème 9.II

Théorème

Soit $n \in \mathbb{N}^*$, on a : $\forall A \in \mathrm{GL}_n(\mathbb{C}), \exists P \in \mathbb{C}[X], A = \exp(P(A))$.
Ce résultat implique la surjectivité de la fonction $\exp : \mathcal{M}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$.

Démonstration :

Étape 1 : Rappelons que $\forall A \in \mathcal{M}_n(\mathbb{C}), \exp(A) \in \mathbb{C}[A]$.[1]

Désormais, fixons $A \in \mathcal{M}_n(\mathbb{C})$.

Étape 2 : On va montrer que $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$.

$\subset$ **:** Trivial.

$\supset$ **:** Soit $B \in \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$, dont on note μ_B le polynôme minimal.
Si $X|\mu_B$, alors $\mu_B = XQ$, avec $Q \in \mathbb{C}[X]$, puis $0 = BQ(B)$; mais $B \in \mathrm{GL}_n(\mathbb{C})$ donc $Q(B) = 0$.
Ceci contredit la minimalité de μ_B.
Donc $\mu_B = \alpha + XQ$, avec $\alpha \in \mathbb{C}^*$ et $Q \in \mathbb{C}[X]$; alors $0 = \alpha + BQ(B)$ et donc

$$B^{-1} = \frac{-Q(B)}{\alpha} \in \mathbb{C}[B] \subset \mathbb{C}[A].$$

Étape 3 : On a donc :

- $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C}) = \mathbb{C}[A]^\times$.
- $\forall M, N \in \mathbb{C}[A], \exp(M+N) = \exp(M)\exp(N)$ car M et N commutent.

Étape 4 : Montrons que $\mathbb{C}[A]^\times$ est un ouvert connexe de $\mathbb{C}[A]$.

$\mathrm{GL}_n(\mathbb{C})$ étant ouvert[2] dans $\mathcal{M}_n(\mathbb{C})$, on déduit de $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap \mathrm{GL}_n(\mathbb{C})$ que $\mathbb{C}[A]^\times$ est ouvert dans $\mathbb{C}[A]$.

On va montrer que $\mathbb{C}[A]^\times$ est connexe par arcs ; soient $M, N \in \mathbb{C}[A]^\times$.[3]

---

1. En effet, $\exp(A) = \lim_{n\to\infty} \underbrace{\sum_{k=0}^{n} \frac{A^k}{k!}}_{\in \mathbb{C}[A]}$ et $\mathbb{C}[A]$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ donc de dimension finie et donc fermé.
2. $\mathrm{GL}_n(\mathbb{C}) = \det^{-1}(\mathbb{R}^*)$ et le déterminant est continu.
3. Petit rappel sur la connexité.

Lemme

1. L'image continue d'un connexe de (E, d) dans (F, d') est connexe.
2. Un espace métrique (E, d) est connexe si et seulement si toute application continue f de (E, d) dans $(\{0,1\}, \delta)$ où δ est la distance discrète est constante.
3. Un espace métrique connexe par arcs est connexe.

En effet :

1. Soit A une partie ouverte et fermée de $f(E)$. Comme f est continue, $f^{-1}(A)$ est ouverte et fermée dans E. Par connexité de E, on a :
   - soit $f^{-1}(A) = \varnothing$ et alors il n'existe pas de $x \in E$ tel que $f(x) \in A$ et donc $A = f(E) \cap A = \varnothing$;
   - soit $f^{-1}(A) = E$ et alors $\forall x \in E, f(x) \in A$ donc $A = f(E)$.

   Donc $f(E)$ est connexe.
2. - Si E est connexe, et $f : E \to \{0,1\}$ est continue, alors $f(E)$ est connexe, donc $f(E) \neq \{0,1\}$ (car $\{0,1\}$ est une réunion de deux singletons, donc de deux fermés). Ainsi, f est constante.
   - Supposons que E ne soit pas connexe : $E = F_0 \sqcup F_1$, où F_0 et F_1 sont deux fermés non-vides. On définit f par $f|_{F_0} \equiv 0$ et $f|_{F_1} \equiv 1$. On va montrer que f est continue ; soit F un fermé de $\{0,1\}$, on va montrer que $f^{-1}(F)$ est fermé dans E. Si $F = \{0,1\}$, alors $f^{-1}(F) = E$ est fermé. Si $F = \{0\}$, alors $f^{-1}(F) = F_0$ est fermé. Si $F = \{1\}$, alors $f^{-1}(F) = F_1$ est fermé. Si $F = \varnothing$, alors $f^{-1}(F) = \varnothing$ est fermé.
3. Soit $f : E \to \{0,1\}$ une fonction continue ; on va montrer que f est constante. Soient $x, y \in E$. Comme E est connexe par arcs, il existe un chemin continu $\gamma : [0,1] \to E$ tel que $\gamma(0) = x$ et $\gamma(1) = y$. L'application $f \circ \gamma : [0,1] \to \{0,1\}$ est alors continue ; mais $[0,1]$ étant connexe, $f \circ \gamma$ est donc constante. Alors : $f(y) = f(\gamma(1)) = f(\gamma(0)) = f(x)$.

On a : $\det(zM + (1-z)N) \in \mathbb{C}[z]\backslash\{0\}$, car le déterminant est polynomial et M inversible.
On note Z l'ensemble des racines de ce polynôme ; c'est un ensemble fini, donc $\mathbb{C}\backslash Z$ est connexe par arcs, contient 0 et 1 ; donc il existe un chemin γ continu reliant 0 et 1 dans $\mathbb{C}\backslash Z$.
Alors le chemin $t \mapsto \gamma(t)M + (1-\gamma(t))N$ est continu et relie M et N dans $\mathbb{C}[A]^\times$.

Étape 5 : Montrons que $\exp(\mathbb{C}[A])$ est ouvert.
On sait que exp est de classe $\mathcal{C}^1$ sur $\mathbb{C}[A]$ et que $\mathrm{D}(\exp)(0) = \mathrm{Id}_{\mathbb{C}[A]}$ est bijective.
Par le théorème d'inversion locale, il existe $\mathcal{U}$ un voisinage ouvert de 0 dans $\mathbb{C}[A]$, $\mathcal{V}$ un voisinage ouvert de I_n dans $\mathbb{C}[A]^\times$ tels que : $\exp : \mathcal{U} \to \mathcal{V}$ soit un $\mathcal{C}^1$-difféomorphisme.
En particulier, $\mathcal{V} \subset \exp(\mathbb{C}[A])$.
Soit $B \in \mathbb{C}[A]$, on a : $\exp(B + \mathcal{U}) = \exp(B)\mathcal{V}$.[4]
Or $\exp(B) \in \mathrm{GL}_n(\mathbb{C})$ donc la multiplication à gauche par $\exp(B)$ est bicontinue, par conéquent $\exp(B)\mathcal{V}$ est un ouvert, donc un voisinage de $\exp(B) \in \mathbb{C}[A]^\times$.
Mais $\exp(B)\mathcal{V} = \exp(U + \mathcal{U}) \subset \exp(\mathbb{C}[A])$, donc $\exp(\mathbb{C}[A])$ est voisinage de chacun de ses points, donc ouvert.

Étape 6 : Montrons que $\exp(\mathbb{C}[A])$ est fermé dans $\mathbb{C}[A]^\times$.
On a : $\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]) = \bigcup_{M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])} M \exp(\mathbb{C}[A])$.[5]
Comme dans l'étape précédente, on montre que $\forall M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A]), M\exp(\mathbb{C}[A])$ est ouvert (car M est inversible et $\exp(\mathbb{C}[A])$ est ouvert).
Donc $\exp(\mathbb{C}[A])$ est fermé dans $\mathbb{C}[A]^\times$.

Comme $\mathbb{C}[A]^\times$ est connexe et comme $\exp(\mathbb{C}[A])$ est ouvert, fermé, non-vide dans $\mathbb{C}[A]^\times$, on a :

$$\mathbb{C}[A]^\times = \exp(\mathbb{C}[A]).$$

Conséquemment, $\forall A \in \mathrm{GL}_n(\mathbb{C}), \exists P \in \mathbb{C}[X], A = \exp(P(A))$. D'où la surjectivité de l'exponentielle.[6] ■

Références

[Zav] M. ZAVIDOVIQUE – *Un max de maths*, Calvage & Mounet, 2013.

4. Cela se fait très bien par double inclusion. Si $M \in \mathcal{U}$, $\exp(B+M) = \exp(B)\exp(M) \in \exp(B)\mathcal{V}$. Si $N \in \mathcal{V}$, alors $\exists M \in \mathcal{U}, N = \exp(M)$ et $\exp(B)N = \exp(B)\exp(M) = \exp(B+M) \in \exp(B+\mathcal{U})$.
5. Là encore, cette égalité se vérifie simplement par double-inclusion. L'inclusion "$\subset$" découle du fait que $\mathrm{I}_n \in \exp(\mathbb{C}[A])$. L'inclusion "$\supset$" demande un peu plus de rédaction : si $M \in \mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])$ et si $N \in M\exp(\mathbb{C}[A])$, alors $M \in N\exp(\mathbb{C}[A])$. Supposons que $N \in \exp(\mathbb{C}[A])$, alors on aurait $M \in \exp(\mathbb{C}[A])$, ce qui est exclu.
6. Citons un corollaire pour terminer.

Corollaire

On a l'égalité ensembliste : $\exp(\mathcal{M}_n(\mathbb{R})) = \{A^2 | A \in \mathrm{GL}_n(\mathbb{R})\}$.

En effet :

$\subset$: Soit $M \in \mathcal{M}_n(\mathbb{R})$, on a : $\exp(M) = \underbrace{\exp\left(\frac{M}{2}\right)}_{\in \mathrm{GL}_n(\mathbb{R})}^2$.

$\supset$: Soit $A \in \mathcal{M}_n(\mathbb{R})$, telle que $A = C^2$ où $C \in \mathrm{GL}_n(\mathbb{R})$; par le théorème : $\exists P \in \mathbb{C}[X], C = \exp(P(C))$.
Et comme $C \in \mathcal{M}_n(\mathbb{R}), C = \overline{C} = \exp\left(\overline{P}(C)\right)$. (Non, là, franchement, débrouillez-vous pour le détail, j'ai la flemme.)
Puis : $A = C^2 = C\overline{C} = \exp\left(P(C) + \overline{P}(C)\right)$ car $P(C)$ et $\overline{P}(C)$ commutent.
Or $P + \overline{P} \in \mathbb{R}[X]$ donc $P(C) + \overline{P}(C) \in \mathcal{M}_n(\mathbb{R})$.