Surjectivité de l'exponentielle matricielle.

2013 – 2014

Théorème.
La fonction $\exp : \mathcal{M}_n(\mathbb{C}) \longrightarrow GL_n(\mathbb{C})$ *est surjective.*

Lemme.
Soit G un groupe topologique et H un sous-groupe de G contenant un voisinage de e. Alors H est ouvert et fermé, en particulier H contient la composante connexe de e.

Démonstration. Soit V un voisinage de e dans H, alors pour $h \in H$, hV est un voisinage de h dans H et donc H est ouvert. On a d'autre part

$$H^c = \bigcup_{g \notin H} gH$$

donc H^c est ouvert en tant qu'union d'ouverts, donc H est fermé. $\square$

Démonstration du théorème. Soit $M \in \mathcal{M}_n(\mathbb{C})$. Alors $\mathbb{C}[M]$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ de dimension finie donc est fermé. Or pour tout $N \in \mathbb{N}$ et pour tout $X \in \mathbb{C}[M]$,$\sum_{n=0}^{N} \frac{1}{n!} X^n \in \mathbb{C}[M]$, donc $\exp(X) \in \mathbb{C}[M]$.
Par ailleurs, $\exp(X) \in GL_n(\mathbb{C})$ car d'inverse $\exp(-X)$, donc l'application

$$\begin{aligned} \varphi : \mathbb{C}[M] &\longrightarrow \mathbb{C}[M]^\times \\ X &\longmapsto \exp(X) \end{aligned}$$

est bien définie et est un morphisme de groupes car les éléments de $\mathbb{C}[M]$ commutent. En notant $H := \operatorname{Im}(\varphi)$, H est donc un sous-groupe du groupe topologique $\mathbb{C}[M]^\times$. Pour montrer que $H = \mathbb{C}[M]^\times$, il suffit donc par le lemme de montrer que H contient un voisinage de I_n et que $\mathbb{C}[M]^\times$ est connexe.

Pour montrer que H contient un voisinage de I_n, nous allons appliquer le théorème d'inversion locale. On commence donc par montrer que φ est de classe $\mathcal{C}^1$.

$$\begin{aligned} \varphi(X+H) &= \exp(X+H) \\ &= \exp(X)\exp(H) \\ &= \exp(X)(I_n + H + o(\|H\|)) \\ &= \varphi(X) + \exp(X)H + o(\|H\|). \end{aligned}$$

Donc φ est différentiable et $D\varphi(X)$ est la multiplication par $\exp(X)$. On a alors

$$\|D\varphi(X) - D\varphi(Y)\| = \|\exp(X) - \exp(Y)\|$$

donc $D\varphi$ est continue et φ est donc de classe $\mathcal{C}^1$.

La différentielle en 0 de φ est l'identité donc, d'après le théorème d'inversion locale, φ réalise un $\mathcal{C}^1$-difféomorphisme entre un voisinage de 0 dans $\mathbb{C}[M]$ et un voisinage de I_n dans $\mathbb{C}[M]^\times$. Si $\mathbb{C}[M]^\times$ est connexe, alors le lemme implique que le morphisme φ est surjectif.

Il suffit donc de montrer que $\mathbb{C}[M]^\times$ est connexe. Soit $A, B \in \mathbb{C}[M]^\times$, alors $P(z) := \det(zA + (1-z)B)$ est un polynôme non nul donc l'ensemble Z de ses racines est fini. $\mathbb{C} \setminus Z$ est connexe par arcs et contient 0 et 1 donc il existe un chemin γ reliant 0 à 1 dans $\mathbb{C} \setminus Z$. Le chemin $\gamma(t)A + (1-\gamma(t))B$ relie alors B à A dans $\mathbb{C}[M]^\times$. $\square$

Corollaire.
$GL_n(\mathbb{C})$ n'admet pas de sous-groupe arbitrairement petit.

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 $\mathcal{M}_n(\mathbb{C})$ tels que exp réalise un difféomorphisme de U sur V. On pose $U' := \frac{U}{2}$ et $V' := \exp(U')$.

Alors V' est ouvert et c'est un voisinage de I_n. Soit $M \in V' \setminus \{I_n\}$, montrons qu'il existe $k \in \mathbb{N}$ tel que $M^k \notin V'$.
On écrit $M = \exp(A)$ avec $A \in U' \setminus \{0\}$. Il existe $k \in \mathbb{N}$ tel que $kA \in U \setminus U'$ et on a alors $\exp(kA) = M^k \in V \setminus V'$. $\square$

Proposition.
Soit $A \in GL_n(\mathbb{R})$, alors il existe $M \in \mathcal{M}_n(\mathbb{R})$ telle que $\exp(M) = A$ *si et seulement s'il existe $B \in \mathcal{M}_n(\mathbb{R})$ telle que $A = B^2$.*

Démonstration. Si $\exp(M) = A$, alors $\left(\exp\left(\frac{M}{2}\right)\right)^2 = A$.

Soit $B \in \mathcal{M}_n(\mathbb{R})$ telle que $B^2 = A \in GL_n(\mathbb{R})$. Alors $B \in GL_n(\mathbb{R})$ car de déterminant non nul, donc il existe $Q \in \mathbb{C}[X]$ telle que $\exp(Q(B)) = B$. Or $B = \overline{B} = \exp(\overline{Q}(B))$, donc $A = B \times \overline{B} = \exp(Q(B) + \overline{Q}(B))$ car $Q(B)$ et $\overline{Q}(B)$ commutent. Or $Q + \overline{Q} \in \mathbb{R}[X]$, d'où le résultat. $\square$

Exemple. $A := \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ n'a pas d'antécédent dans $\mathcal{M}_2(\mathbb{R})$ par exp. Supposons qu'il existe $B \in \mathcal{M}_2(\mathbb{R})$ telle que $\exp(B) = A$, alors si λ est valeur propre de B, $\exp\lambda$ est valeur propre de A donc $\lambda = i\pi + 2k\pi$ pour $k \in \mathbb{Z}$. Donc $\lambda \neq \bar{\lambda}$, or B est réelle donc $\bar{\lambda}$ est aussi valeur propre de B, donc B est diagonalisable. On en déduit que A est diagonalisable, ce qui est absurde.