Surjectivité de l'exponentielle matricielle

Théorème : L'application $\exp : \mathcal{M}_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est surjective.

Preuve du théorème : Soit $A \in GL_n(\mathbb{C})$.

0) L'application est bien définie :

La convergence de la série vient de la sous-multiplicativité de la norme triple (et on sait que la série exponentielle à valeurs réelles converge) et comme A et $-A$ commutent, $\exp(A)^{-1} = \exp(-A)$.

i) Montrons que $\exp(A) \in \mathbb{C}[A]$:

On sait que $\mathbb{C}[A]$ est un sous-espace vectoriel (de dimension finie) de $\mathcal{M}_n(\mathbb{C})$ et il est donc fermé. Comme $\left(\sum_{k=0}^{n} \frac{A^k}{k!}\right)_{n\in\mathbb{N}}$ est une suite à valeurs dans $\mathbb{C}[A]$ qui converge, sa limite est encore dans $\mathbb{C}[A]$ et donc $\exp(A) \in \mathbb{C}[A]$.

ii) Montrons que $\mathbb{C}[A]^\times = \mathbb{C}[A] \cap GL_n(\mathbb{R})$:

On peut avoir l'impression que c'est immédiat aux premiers abords mais la subtilité réside dans le fait qu'il n'y a, *a priori*, aucune raison pour que l'inverse d'un élément inversible de $\mathbb{C}[A]$ soit aussi dans $\mathbb{C}[A]$. L'inclusion de gauche à droite est évidente (par définition) par contre, on se donne donc un élément M de $\mathbb{C}[A] \cap GL_n(\mathbb{R})$. On note π_M le polynôme minimale de M. On peut alors écrire $\pi_M(X) = \sum_{k=0}^{d} a_k X^k$ avec $a_0 \neq 0$. En effet, si $a_0 = 0$, $X|\pi_M(X)$ et donc 0 serait valeur propre de M, absurde car M est inversible. Ainsi,

$$M^{-1} = \frac{\sum_{k=1}^{d} a_k M^{k-1}}{-a_0},$$

et donc M^{-1} est un polynôme en M qui est lui-même un polynôme en A. Comme la composée de 2 polynômes en est encore un, m^{-1} est bien un polynôme en A ce qui montre ce que l'on veut.

iii) Montrons que $\mathbb{C}[A]^\times$ est un ouvert connexe de $\mathbb{C}[A]$:

Le fait que ce soit un ouvert vient du fait que $\mathbb{C}[A]^\times = \det^{-1}(\mathbb{C}^*) \cap \mathbb{C}[A]$ (grâce au ii)) et $\det$ est continue donc $\det^{-1}(\mathbb{C}^*)$ est ouvert car $\mathbb{C}^*$ est ouvert dans $\mathbb{C}$. Pour montrer la connexité on va montrer que $\mathbb{C}[A]^\times$ est connexe par ars. Soit $M, N \in \mathbb{C}[A]^\times$. On note $f : \mathbb{C} \to \mathcal{M}_n(\mathbb{C})$ telle que $f(z) = \det(zM + (1-z)N)$. Il est clair que f est une fonction polynomiale en z et admet donc un nombre fini de points en lesquels elle s'annule. Comme $\mathbb{C}$ privé d'un nombre fini de points est connexe, on peut trouver un chemin $\gamma : [0,1] \to \mathbb{C}$

entre 0 et 1 qui ne contient aucune racine de f (en remarquant évidemment que $f(0)$ et $f(1)$ sont différents de 0 par hypothèse). De plus, pour tout $z \in \mathbb{C}$, $zM + (1-z)N \in \mathbb{C}[A]$. Ainsi, le chemin $\Gamma : [0,1] \to \mathbb{C}[A]^\times$ qui à x associe $\gamma(x)M + (1-\gamma(x))N$ est bien définie et relie M et N comme voulue. Finalement, $\mathbb{C}[A]^\times$ est bien un ouvert connexe par arc de $\mathbb{C}[A]$.

iv) Montrons que $\exp(\mathbb{C}[A])$ est un ouvert de $\mathbb{C}[A]^\times$:

Déjà $\exp(\mathbb{C}[A]) \subset \mathbb{C}[A]^\times$ par i) et ii). Montrons qu'il est ouvert.
On sait que la différentielle de l'exponentielle en 0 est Id (la différentielle est invariante par restriction de par son unicité). Par le théorème d'inversion locale il existe alors un voisinage U de 0 dans $\mathbb{C}[A]$ et un voisinage V de Id dans $\mathbb{C}[A]^\times$ tels que $\exp_U \to V$ soit un difféomorphisme. Soit maintenant $M \in \mathbb{C}[A]$. Comme la multiplication par un élément inversible dans $GL_n(\mathbb{C})$ est un difféomorphisme, $\exp(M)V$ est un ouvert de $\mathbb{C}[A]^\times$. De plus, comme tous les élements de $\mathbb{C}[A]$ commutent (car polynômes en A), $\exp(M)V = \exp(M)\exp(U) = \exp(M+U)$. Ainsi, $\exp(M)V$ est bien un voisinage ouvert de $\exp(M)$ inclus dans $\exp(\mathbb{C}[A])$ ce qui montre que $\exp(\mathbb{C}[A]$ est un ouvert de $\mathbb{C}[A]^\times$. Petit récapitulatif :

$$\exp(M) \in \underbrace{\exp(M)V}_{\text{ouvert de} \mathbb{C}[A]^\times} \subset \mathbb{C}[A]^\times.$$

v) On conclut :

On commence par montrer que $\exp(\mathbb{C}[A])$ est un fermé de $\mathbb{C}[A]^\times$. Comme $\exp(\mathbb{C}[A])$ est un voisinage ouvert de l'identité on peut écrire

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

Ainsi $\mathbb{C}[A]^\times \setminus \exp(\mathbb{C}[A])$ est ouvert comme union d'ouverts et donc $\exp(\mathbb{C}[A])$ est fermé. L'inclusion de gauche à droite est directe (car $M \in M\exp(\mathbb{C}[A])$) et pour l'autre inclusion, si $M\exp(P(A)) = \exp(Q(A))$, $M = \exp(Q(A) - P(A))$ donc $M \in \exp(\mathbb{C}[A])$.

Finalement, $\exp(\mathbb{C}[A])$ est ouvert et fermé dans $\mathbb{C}[A]^\times$ qui est connexe donc $\exp(\mathbb{C}[A]) = \mathbb{C}[A]^\times$. Comme $A \in \mathbb{C}[A]^\times$il existe $P \in \mathbb{C}[X]$ tel que $\exp(P(A)) = A$ et donc A est bien dans l'image de exp.$\square$

Remarques importantes :

- À vous de voir ce que vous sautez/préciser. Typiquement ça ne m'intéresse pas beaucoup de montrer que $\exp(A)\exp(B) = \exp(A+B)$ si A et B commutent mais vous pouvez le détailler sans soucis.
- Réfléchissez bien à la partie sur l'inversion locale etc. ça peut être piégeux.
- Il faut avoir réfléchi aux petites choses que j'admets (la convergence de la série exponentielle, le fait que $\mathbb{C}$ privé d'un nombre fini de points est connexe etc.)