

Partie I - $\mathbb{K} = \mathbb{C}$

Soit $A \in \mathcal{M}_n(\mathbb{C})$.

1) $\mathbb{C}[A]$ est une sous-algèbre de l'algèbre $\mathcal{M}_n(\mathbb{C})$. C'est donc également un sous-espace vectoriel de l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$. Comme $\mathcal{M}_n(\mathbb{C})$ est un espace vectoriel de dimension finie (n^2), $\mathbb{C}[A]$ est également de dimension finie (plus précisément, sa dimension est égal au degré du polynôme minimal de A). Donc $\boxed{\mathbb{C}[A] \text{ est fermé}}$.

Soit $B \in \mathbb{C}[A]$. Il existe donc $P \in \mathbb{C}[X]$ tel que $B = P(A)$.

$$\exp(B) = \lim_{n \rightarrow \infty} S_n$$

avec

$$\forall n \in \mathbb{N} \quad S_n = \sum_{k=0}^n \frac{1}{k!} B^k = \left(\sum_{k=0}^n \frac{1}{k!} P^k \right) (A) \in \mathbb{C}[A]$$

Par caractérisation séquentielle des fermés, $\exp(B) \in \mathbb{C}[A]$.

Donc $\boxed{\mathbb{C}[A] \text{ est stable par } \exp}$.

2) Soit $P \in \mathbb{C}[X]$.

- Supposons que P est premier avec π_A où π_A désigne le polynôme minimal de A . Par le théorème de Bézout, il existe $U, V \in \mathbb{C}[X]$ tels que

$$1 = UP + V\pi_A$$

On a donc :

$$I_n = 1(A) = U(A)P(A) + V(A)\pi_A(A) = U(A)P(A) + 0_n = P(A)U(A)$$

Donc $P(A)$ est inversible d'inverse $U(A)$.

- Prouvons la réciproque par contraposée. Supposons que P n'est pas premier avec π_A . Soit Δ le pgcd de P et π_A et soient $Q = \frac{P}{\Delta}$ et $S = \frac{\pi_A}{\Delta}$.

$\Delta(A)$ n'est pas inversible car sinon, notant 0_n la matrice nulle de $\mathcal{M}_n(\mathbb{C})$, comme $0_n = \Delta(A)S(A)$, on aurait $S(A) = 0$ avec $-\infty < \deg(S) < \deg(\pi_A)$, ce qui est contradictoire.

Comme $P(A) = Q(A)\Delta(A)$ et que $\Delta(A)$ n'est pas injective, $P(A)$ ne l'est pas non plus donc n'est pas inversible.

3) Soit $B \in \mathrm{GL}_n(\mathbb{C}) \cap \mathbb{C}[A]$.

Comme $B \in \mathbb{C}[A]$, il existe un polynôme P tel que $B = P(A)$. D'après la question précédente, P est premier avec π_A .

Dans les notations précédentes, $\boxed{B^{-1} = U(A) \in \mathbb{C}[A]}$.

On pose $G = \mathrm{GL}_n(\mathbb{C}) \cap \mathbb{C}[A]$.

4) a) G est non vide car il contient $I_n = 1(A)$.

Soient $B, C \in G$. Alors $B^{-1}C$ est inversible, et c'est le produit de deux polynômes en A (car B^{-1} est un polynôme en A par la question précédente. Donc $B^{-1}C$ est un polynôme en A . Donc $B^{-1}C \in G$.

Donc $\boxed{G \text{ est un sous-groupe de } (\mathrm{GL}_n(\mathbb{C}), \times)}$.

b) H est non vide car il contient $I_n = \exp(0_n)$.

H est inclus dans G car pour toute matrice $C \in H$, il existe $B \in \mathbb{C}[A]$ telle que $C = \exp(B)$ donc C est inversible d'inverse $\exp(-B)$, et comme $-B \in \mathbb{C}[A]$, on a $C^{-1} \in H$.

Soit $C' \in H$ et $B' \in \mathbb{C}[A]$ telle que $C' = \exp(B')$.

Dans les notations précédentes,

$$C^{-1}C' = \exp(-B)\exp(B') = \exp(-B+B')$$

car $-B$ et B' commutent car ce sont deux polynômes en A .

De plus, $-B+B'$ est un polynôme en A .

Donc $C^{-1}C' \in H$.

Donc H est un sous-groupe de (G, \times) .

On admet que H est un ouvert relatif de G .

5) Soit $B \in \mathbb{C}_G H$. Alors $B = BI_n \in BH \subset \bigcup_{M \in G \setminus H} MH$.

Réiproquement, soit $B \in \bigcup_{M \in G \setminus H} MH$. Il existe alors $M \in G \setminus H$ telle que $B \in MH$. Il existe donc $C \in H$ tel que $B = MC$.

Comme $BC^{-1} = M \notin H$, comme $C \in H$ et comme H est un sous-groupe de G , B ne peut appartenir à H . De plus B appartient à G car G est stable par multiplication.

Donc $B \in \mathbb{C}_G H$

Ainsi $\mathbb{C}_G H = \bigcup_{M \in G \setminus H} MH$.

Soit $M \in G \setminus H$.

$$MH = f^{-1}(H)$$

où $f : G \rightarrow G$, $C \mapsto M^{-1}C$.

f est continue par continuité du produit matriciel, et H est un ouvert relatif de G , donc $f^{-1}(H)$ est un ouvert relatif de G .

Ainsi $\bigcup_{M \in G \setminus H} MH$ est réunion d'ouverts relatifs de G , donc est un ouvert relatif de G .

Donc H est un fermé relatif de G .

6) a) Soient M et N dans G . Soit P le polynôme $\det((1-X)M + XN) \in \mathbb{C}[X]$. Comme $\tilde{P}(0) = \det(M) \neq 0$, P n'est pas le polynôme nul et a donc un nombre fini de racines.

Donc l'ensemble $\{z \in \mathbb{C} \text{ , } (1-z)M + zN \text{ non inversible}\}$ est fini.

b) Soient M et N dans G . Soient z_1, \dots, z_p les racines du polynôme P défini dans la question précédente. Remarquons que ni 0, ni 1 ne sont racines de P car $\det(M)$ et $\det(N)$ sont non nuls.

Soit $\gamma : [0, 1] \rightarrow \mathbb{C}$ une application continue ne prenant aucune des valeurs z_1, \dots, z_p . Un tel chemin peut par exemple être construit à l'aide de deux segments de droite :

-parmi les droites passant par 0, on peut en choisir une ne passant par aucun des points z_1, \dots, z_p (il suffit pour cela que l'angle orienté que fait cette droite avec l'axe réel ait une mesure θ qui ne soit congrue modulo π à aucun des arguments de z_1, \dots, z_p)

-puis parmi les droites passant par 1, on peut en choisir une non parallèle à la précédente et ne passant par aucun des points z_1, \dots, z_p (il suffit pour cela que l'angle orienté que fait cette droite avec l'axe réel ait une mesure qui ne soit congrue modulo π ni à θ ni à aucun des arguments de $z_1 - 1, \dots, z_p - 1$)

-les deux droites ainsi construites se coupent en un point z et il suffit de définir γ par $\gamma(t) = 2tz$ si $t \in [0, \frac{1}{2}]$ et $\gamma(t) = z + 2(t - \frac{1}{2})(1-z)$ si $t \in [\frac{1}{2}, 1]$.

L'application $t \in [0, 1] \mapsto (1 - \gamma(t))M + \gamma(t)N$ est alors un chemin continu à valeurs dans G de M vers N (elle ne prend que des valeurs inversibles et à termes dans $\mathbb{C}[A]$ car $\mathbb{C}[A]$ est stable par combinaisons linéaires)

Donc G est connexe par arcs.

- 7) a) Soit $M \in H$ et $N \in G$. Soit $\gamma : [0, 1] \rightarrow G$ un chemin continu de M à N et soit $t_0 = \sup X$ où $X = \{a \in [0, 1], \gamma([0, a]) \subset H\}$

Soit $\|\cdot\|$ une norme sur $\mathcal{M}_n(\mathbb{C})$. Comme H est un ouvert relatif de G et comme $M \in H$, il existe $\varepsilon > 0$ tel que $\forall M' \in G, \|M' - M\| \leq \varepsilon \Rightarrow M' \in H$

Comme γ est continue et $\gamma(0) = M$, il existe $\delta > 0$ tel que $\forall t \in [0, \delta] \|\gamma(t) - M\| \leq \varepsilon$.

Ainsi $\forall t \in [0, \delta] \gamma(t) \in H$.

Donc $t_0 \geq \delta > 0$.

Soit $t \in [0, t_0]$. t n'est pas un majorant de X car t_0 est le plus petit majorant de X . Donc il existe $a \in X$ tel que $a > t$. Comme $t \in [0, a]$, on a donc $\gamma(t) \in H$.

Comme H est un fermé relatif de G et comme γ est continue, on a

$$\gamma(t_0) = \lim_{t \rightarrow t_0^-} \gamma(t) \in H$$

Raisonnons par l'absurde et supposons que $t_0 \neq 1$. Par le même raisonnement que précédemment, il existe $\delta \in]0, 1 - t_0[$ tel que $\forall t \in [t_0, t_0 + \delta] \gamma(t) \in H$.

On a alors $t_0 + \delta \in X$, ce qui est contradictoire (car t_0 majore X).

Ainsi $t_0 = 1$, et comme $\gamma(t_0) \in H$, on a donc $\boxed{N \in H}$.

- b) Fixons $M \in H$ (M existe car H est non vide, il contient I_n). Pour tout $N \in G$, il existe bien un chemin continu de M à N à valeurs dans G car G est connexe par arcs, donc $N \in H$ par la question précédente.

Ainsi $G \subset H$ donc $H = G$.

On a ainsi prouvé que $\forall A \in \mathcal{M}_n(\mathbb{C}) \exp(\mathbb{C}[A]) = \mathbb{C}[A] \cap GL_n(\mathbb{C})$.

En particulier si A est une matrice $\boxed{\text{inversible}}$, alors $A = 1(A) \in \mathbb{C}[A] \cap GL_n(\mathbb{C})$ donc

$\boxed{A \text{ a un antécédent dans } \mathbb{C}[A] \text{ par } \exp}$.

Partie II - $\mathbb{K} = \mathbb{R}$

Soit $A \in GL_n(\mathbb{R})$.

- 8) On suppose qu'il existe $M \in \mathcal{M}_n(\mathbb{R})$ tel que $A = \exp(M)$.

Posons $B = \exp(M/2)$. Alors $B \in GL_n(\mathbb{R})$ et comme $M/2$ commute avec elle-même, $B^2 = \exp(2M/2) = A$. Donc $\boxed{A \text{ a une racine carrée dans } GL_n(\mathbb{R})}$.

- 9) Réciproquement, on suppose qu'il existe $B \in GL_n(\mathbb{R})$ tel que $A = B^2$.

Par la première partie, il existe un polynôme $P \in \mathbb{C}[X]$ tel que $\exp(P(B)) = B$

Comme B est à coefficients réels, $\bar{P}(B) = \overline{P(B)}$.

Ainsi $\exp(\bar{P}(B)) = \sum_{k=0}^{\infty} \frac{(\bar{P}(B))^k}{k!} = \sum_{k=0}^{\infty} \frac{\overline{(P(B))^k}}{k!} = \overline{\exp(P(B))} = \bar{B} = B$

Donc

$$A = BB = \exp(P(B))\exp(\bar{P}(B)) = \exp(P(B) + \bar{P}(B))$$

car $P(B)$ et $\bar{P}(B)$ commutent puisque ce sont deux polynômes en B .

Posant $Q = P + \bar{P}$, Q est à coefficients réels et $A = \exp(Q(B))$.

Donc

$$\boxed{A \in \exp(\mathbb{R}[B]) \subset \exp(\mathcal{M}_n(\mathbb{R}))}$$