Le théorème de Cartan-von Neumann

Théorème (Cartan-von Neumann)**.** *Tout sous-groupe fermé de $GL_n(\mathbf{R})$ est une sous-variété de $\mathcal{M}_n(\mathbf{R})$.*

Preuve. Soit G un sous-groupe fermé de $GL_n(\mathbf{R})$. On montre que G est localement difféomorphe à un ouvert de $\mathcal{M}_n(\mathbf{R}) \simeq \mathbf{R}^{n^2}$. À cause de la structure de groupe et du caractère C^∞ de la translation, il suffit de la prouver pour un voisinage de I_n dans G.

Étape 1. Une sous-algèbre digne d'intérêt

On pose :

$$\mathcal{L}_G := \{m \in \mathcal{M}_n(\mathbf{R}),\ \forall t \in \mathbf{R},\, e^{tm} \in G\}$$

et on montre que c'est une sous-algèbre de $\mathcal{M}_n(\mathbf{R})$. La seule chose à vérifier est la stabilité par la somme. Pour cela, remarquons d'abord que la différentielle de exp en 0 est inversible donc, exp est localement inversible et on note L son inverse. Pour m au voisinage de 0 :

$$e^m = I_n + m + o(\|m\|) \ \text{ et } \ L(I_n + m) = m + o(\|m\|).$$

Soient $a, b \in \mathcal{L}_G$ et $t \in \mathbf{R}$, on a pour $k \in \mathbf{N}$ suffisamment grand :

$$\begin{array}{rcl} (e^{ta/k}e^{tb/k})^k & = & e^{kL(e^{ta/k}e^{tb/k})} \\ & = & e^{kL(I_n + t\frac{a+b}{k} + o(1/k))} \\ & = & e^{t(a+b)+o(1)} \\ & \underset{k\to+\infty}{\longrightarrow} & e^{t(a+b)} \end{array}$$

et la fermeture de G montre que $a + b \in \mathcal{L}_G$.

Étape 2. Là où le théorème d'inversion locale intervient de façon cruciale.

Soient M un supplémentaire de $\mathcal{L}_G$ dans $\mathcal{M}_n(\mathbf{R})$ et $\varphi : \mathcal{M}_n(\mathbf{R}) \to GL_n(\mathbf{R})$ l'application qui a $x = l + m$, $(l, m) \in \mathcal{L}_G \times M$, associe $\varphi(x) = e^l e^m$. φ est C^∞ et sa différentielle en 0 vaut l'identité. Par le théorème d'inversion locale, il existe un voisinage U de 0 dans $\mathcal{M}_n(\mathbf{R})$ tel que φ soit un C^1-difféomorphisme de U sur $\varphi(U)$. On va montrer que, quitte à restreindre U,

$$\varphi : U \cap \mathcal{L}_G \to \varphi(U) \cap G$$

est un C^1-difféomorphisme, ce qui conclura (en on aura aussi $\dim G = \dim \mathcal{L}_G$). Il suffit pour cela, de montrer que $\varphi(U \cap \mathcal{L}_G) = \varphi(U) \cap G$. Remarquons que l'inclusion $\subset$ est évidente : c'est la définition de $\mathcal{L}_G$.

Étape 3. L'autre inclusion et c'est fini.

On veut montrer qu'il existe un voisinage U de 0 dans $\mathcal{M}_n(\mathbf{R})$ tel que $\varphi(U) \cap G \subset \varphi(U \cap \mathcal{L}_G)$. On va montrer :

$$\exists k \in \mathbf{N}^*, \forall x_k \in B(0, 1/k), \varphi(x_k) \in G \Longrightarrow x_k \in \mathcal{L}_G.$$

Si ça n'était pas le cas, alors comme $\mathcal{M}_n(\mathbf{R}) = \mathcal{L}_G \oplus M$, il existerait deux suites $(l_k)_k$ et $(m_k)_k$ respectivement de $\mathcal{L}_G$ et $M \setminus \{0\}$, de limites nulles, et telles que pour tout $k \in \mathbf{N}$, $\varphi(l_k + m_k)$ soit dans G. Alors, par définition de $\mathcal{L}_G$, on aurait $e^{m_k} \in G$ pour tout k. Puisque $m_k \neq 0$ posons, pour tout $k \in \mathbf{N}^*$:

$$\varepsilon_k = \frac{m_k}{\|m_k\|} \in M.$$

Quitte à extraire, on peut supposer que (ε_k) converge vers $\varepsilon \in M$ de norme 1. Soit $t \in \mathbf{R}$ et notons :

$$\frac{t}{\|m_k\|} = \lambda_k + \mu_k, \quad \text{où } \lambda_k \in \mathbf{Z} \text{ et } |\mu_k| < \frac{1}{2}.$$

Alors :

$$e^{t\varepsilon} = \lim_{k \to +\infty} e^{t \frac{m_k}{\|m_k\|}} = \lim_{k \to +\infty} e^{\lambda_k m_k}$$

car $e^{\mu_k m_k} \to I_n$. Comme $\lambda_k \in \mathbf{Z}$, $e^{t\varepsilon} \in G$ comme limite d'une suite de points de G qui est fermé. Ce qui prouve que $\varepsilon \in \mathcal{L}_G \cap M = \{0\}$. C'est absurde puisque ε est de norme 1. $\square$

Quelques remarques complémentaires

- En fait, $\mathcal{L}_G$ est une sous-algèbre de Lie de $\mathcal{M}_n(\mathbf{R})$, c'est à dire un sous-espace de $\mathcal{M}_n(\mathbf{R})$ stable par $(a,b) \mapsto [a,b] = ab - ba$. Pour le voir, il suffit de montrer en développant à l'ordre 2 :
$$(e^{a/k} e^{b/k} e^{-a/k} e^{-b/k})^{k^2} \to e^{ab-ba}.$$

- Il vaut mieux définir le "logarithme matriciel" :
$$L(I_n + m) = \sum_{k=0}^{+\infty} \frac{(-1)^k m^{k+1}}{k+1}, \quad \|m\| < 1$$
qui vérifie $e^{L(1+m)} = 1 + m$.

- On peut voir que G est discret si et seulement si $\mathcal{L}_G = \{0\}$. Pour le sens réciproque, on montre en réutilisant le résultat sur les suites de l'étape 3 que I_n est isolé, ce qui est suffisant.

- Soit $m \in \mathcal{L}_G$. Alors $t \mapsto e^{tm}$ est une courbe tracée dans G passant par I_n en $t = 0$ et le vecteur tangent à cette courbe en I_n est m. Par suite, $\mathcal{L}_G$ est inclus dans l'espace tangent à G en Id. Mais on a prouvé qu'ils ont même dimension, ils sont donc égaux.

- Le sous-groupe de G engendré par $\exp \mathcal{L}_G$ est la composante connexe de I_n dans G.

- En pratique, ça ne sert pas à grand chose.

Références.

S. Gonnord, N. Tosel, *Calcul différentiel*

R. Mneimné, F. Testard, *Introduction aux groupes de Lie classiques*

106 Groupe linéaire d'un espace vectoriel de dimension fini E, sous-groupe de $GL(E)$. Applications.
156 Exponentielle de matrices. Applications.
214 Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie
215 Applications différentiables sur un ouvert de $\mathbf{R}^n$. Exemples et applications.