

Simplicité de $\text{SO}_3(\mathbb{R})$

Développement pour les leçons 103¹, 106², 108³, 160⁴, 204⁵.

1 Introduction

Le but de cette leçon est de démontrer la simplicité du groupe $\text{SO}_3(\mathbb{R})$. On rappelle que

$$\text{SO}_3(\mathbb{R}) = \{g \in \text{GL}_3(\mathbb{R}) \mid \det(g) = 1\}$$

Les éléments de $\text{SO}_3(\mathbb{R})$ sont les rotations de l'espace. Dans une bonne base orthonormée, pour tout $g \in \text{SO}_3(\mathbb{R})$, il existe $\theta \in]-\pi, \pi]$ tel que

$$g = \begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

La preuve repose sur les propriétés topologiques de $\text{SO}_3(\mathbb{R})$. L'idée de la preuve consiste d'abord à démontrer le résultat de simplicité dans le cas où G est connexe par arc. Pour cela, on obtient des propriétés essentielles sur G_0 la composante connexe par arc de Id dans G . On explique tout ce qu'il y a à savoir sur les composantes connexes par arc dans la partie **Vocabulaire**. Quant à la preuve, celle-ci repose sur le fait de montrer que, dès que G est distingué est que G_0 n'est pas réduit à $\{\text{Id}\}$, on a $G = G_0 = \text{SO}_3(\mathbb{R})$. Pour cela, on va montrer que si G est un sous-groupe distingué connexe par arc de $\text{SO}_3(\mathbb{R})$, alors $G = \text{SO}_3(\mathbb{R})$. Pour se faire, on montre que G contient un renversement. Comme ces derniers sont conjugués dans $\text{SO}_3(\mathbb{R})$ et engendrent $\text{SO}_3(\mathbb{R})$, on aura gagné. Enfin, dans le cas général, on applique le résultat précédent si $G_0 \neq \{\text{Id}\}$ et si on a l'égalité, on montre alors que G est réduit à l'identité.

2 Vocabulaire

On considère $g, h \in \text{SO}_3(\mathbb{R})$. On dit que g et h sont **reliés** dans $\text{SO}_3(\mathbb{R})$ s'il existe une application continue $\gamma : [0, 1] \rightarrow \text{SO}_3(\mathbb{R})$ tel que pour tout $t \in [0, 1]$, $\gamma(t) \in \text{SO}_3(\mathbb{R})$, $\gamma(0) = g$ et $\gamma(1) = h$. Ainsi, pour tout $t \in [0, 1]$, $\gamma(t)$ est un élément de $\text{SO}_3(\mathbb{R})$. Si on a un chemin de g à h , on a un chemin de h à g en considérant $\gamma'(t) = \gamma(1 - t)$.

On sait que l'application $g \mapsto g^{-1}$ est continue, donc si γ est un chemin reliant $g \in \text{SO}_3(\mathbb{R})$ et $h \in \text{SO}_3(\mathbb{R})$, on peut définir le chemin $\gamma^{-1} : [0, 1] \rightarrow \text{SO}_3(\mathbb{R})$ par $\gamma^{-1}(t) = (\gamma(t))^{-1}$. Ainsi, γ^{-1} est un chemin reliant g^{-1} à h^{-1} .

Si γ relie g à h et γ' relie h à k , alors en posant

$$\gamma''(t) = \begin{cases} \gamma(2t) & \text{si } t \in [0, \frac{1}{2}] \\ \gamma'(2t - 1) & \text{si } t \in [\frac{1}{2}, 1] \end{cases}$$

Ces petits points nous permettent de montrer que la relation "est relié à" est une relation d'équivalence. Les classes d'équivalences de cette relation d'équivalence sont appelées les **composantes connexes par arc** de $\text{SO}_3(\mathbb{R})$. Si G est un sous-groupe de $\text{SO}_3(\mathbb{R})$, on notera G_0 la composante connexe par arc de l'identité dans G .

3 Preuve de la simplicité de $\text{SO}_3(\mathbb{R})$

L'idée de la preuve est plutôt simple : on montre que si G est un sous-groupe connexe par arc et distingué de $\text{SO}_3(\mathbb{R})$ qui n'est pas réduit à l'identité, alors $G = G_0 = \text{SO}_3(\mathbb{R})$. Cette preuve se fera en plusieurs étapes. En premier lieu, on démontre deux résultats qui auront leurs importances dans la preuve finale de la simplicité de $\text{SO}_3(\mathbb{R})$, à savoir que si G est un sous-groupe de $\text{SO}_3(\mathbb{R})$, alors la composante connexe de l'identité dans G est un sous-groupe de G qui est distingué dès que G l'est. Ceci concerne les points (1) et (2). Ensuite, on montrera que si G est un sous-groupe distingué non réduit à l'identité et connexe par arc, alors c'est $\text{SO}_3(\mathbb{R})$. Enfin, on montre qu'un sous-groupe distingué de $\text{SO}_3(\mathbb{R})$ différent de $\text{SO}_3(\mathbb{R})$ est réduit à l'identité.

1. On va tout d'abord montrer que si G est un sous-groupe de $\text{SO}_3(\mathbb{R})$, alors G_0 est un sous-groupe de G . On a bien $\text{Id} \in G_0$. Soient $g, h \in G_0$. On veut montrer que $gh^{-1} \in G_0$, ce qui revient à montrer qu'il existe un chemin γ reliant Id à gh^{-1} . Comme $g, h \in G_0$, il existe γ et γ' reliant respectivement Id à g et Id à h . Or, l'application $\gamma'' : t \mapsto \gamma(t)(\gamma'(t))^{-1}$ est continue, est bien un élément de G (car pour tout $t \in [0, 1]$, $\gamma(t) \in G$ et $\gamma'(t) \in G$

1. Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

2. Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de $\text{GL}(E)$. Applications.

3. Exemples de parties génératrices d'un groupe. Application

4. Endomorphisme remarquable d'un espace vectoriel euclidien (de dimension finie)

5. Connexité. Exemples et applications

comme, par définition, $g, h \in G_0$). Ainsi, le chemin γ'' relie Id à gh^{-1} dans G , donc $gh^{-1} \in G_0$ et on a bien le fait que G_0 est un sous-groupe de G .

2. On va maintenant montrer que si G est un sous-groupe distingué de $\text{SO}_3(\mathbb{R})$, il en est de même pour G_0 . Soit $g \in G_0$, γ un chemin reliant Id à g est $h \in \text{SO}_3(\mathbb{R})$. On veut montrer que $hgh^{-1} \in G_0$. On considère le chemin $\gamma' : t \mapsto h\gamma(t)h^{-1}$. Comme la composition à gauche et à droite par un élément de $\text{SO}_3(\mathbb{R})$ est continue (les éléments de $\text{SO}_3(\mathbb{R})$ sont des applications linéaires en dimension finies, donc elles sont continues), on en déduit que le chemin γ' est continue. De plus, comme G est distingué, pour tout $t \in [0, 1]$, on a $\gamma'(t) \in G$. Mais alors on a trouvé un chemin dans G reliant Id à hgh^{-1} . Ainsi, on a $hgh^{-1} \in G_0$ et donc G_0 est un sous-groupe distingué de $\text{SO}_3(\mathbb{R})$.

3. On va dans un premier temps supposer que G est connexe par arc et que G est distinct de $\{\text{Id}\}$. Sous ces conditions, on a $G = G_0$. L'objectif est de montrer que G contient un retournement, c'est à dire une rotation d'angle π . En effet, les retournements engendrent $\text{SO}_3(\mathbb{R})$ et sont conjugués entre-eux. Le caractère distingué de G nous permettra, une fois l'existence de ce retournement démontrée, de dire que $G = \text{SO}_3(\mathbb{R})$.

En fait, on va juste montrer qu'il existe une rotation d'angle $\frac{\pi}{2}$. En effet, en notant cet élément r , on a r^2 qui est une rotation d'angle π et on aura ainsi le résultat souhaité. Soit $g \in G$ différent de l'identité. À l'aide de l'écriture matricielle, en notant θ l'angle de rotation de g , on obtient que

$$\text{tr}(g) = 2 \cos(\theta) - 1$$

On peut alors définir la fonction $\theta \mapsto \cos(\theta) = \frac{\text{tr}(g)+1}{2}$. Cette dernière est continue (car l'application trace l'est). De plus, elle s'annule pour un angle de $\frac{\pi}{2}$. Il suffit donc de montrer que cette application s'annule en un élément de G pour montrer l'existence d'une rotation d'angle $\frac{\pi}{2}$ dans G . Pour cela, on va raisonner par étapes. On va d'abord montrer qu'il existe un élément $g \in G$ d'angle θ vérifiant $\cos(\theta) \leq 0$. Quitte à considérer g^{-1} , on peut supposer sans perte de généralité que $0 < \theta \leq \pi$. Si $\theta \in [\frac{\pi}{2}, \pi]$, il n'y a rien à faire. Si maintenant $\theta \in]0, \frac{\pi}{2}[$, du fait que $\mathbb{R}$ est archimédien, il existe $N \in \mathbb{N}$ tel que $N\theta \in [\frac{\pi}{2}, \pi]$. Ainsi, on a bien $g^N \in G$ et g^N est une rotation d'angle $N\theta \in [\frac{\pi}{2}, \pi]$.

C'est maintenant que nous utilisons l'hypothèse que G est connexe par arc. On note $s = g^N$ l'élément construit précédemment et θ l'angle associé (et donc $\cos(\theta) \leq 0$). On a de plus que l'angle associé à l'identité est 0 et donc que $\cos(0) = 1$. Or, G est connexe par arc, donc il existe un chemin γ reliant Id à s . De plus, la fonction

$$t \mapsto \frac{\text{tr}(\gamma(t)) + 1}{2}$$

est continue et pour tout $t \in [0, 1]$, $\gamma(t) \in G$. Ainsi, $\gamma(0) = 1$ et $\gamma(1) = \cos(\theta) \leq 0$. Ainsi, il existe t_0 tel que $\frac{\text{tr}(\gamma(t_0)) + 1}{2} = 0$, et comme $\gamma(t_0) \in G$, on a bien ce que l'on cherche, à savoir un élément de G qui est une rotation d'angle $\frac{\pi}{2}$. Ainsi, on a bien $G = \text{SO}_3(\mathbb{R})$.

4. On va maintenant juste supposer que G est distingué dans $\text{SO}_3(\mathbb{R})$. On a vu au point 2 que, sous ces hypothèses, la composante connexe de l'identité G_0 est un sous-groupe distingué et connexe par arc de $\text{SO}_3(\mathbb{R})$. Ainsi, s'il existe $g \neq \text{Id}$ dans G_0 , alors par le point 3 que $G_0 = \text{SO}_3(\mathbb{R})$ et c'est fini. Si jamais $G_0 = \{\text{Id}\}$, on va montrer que $G = G_0$. Dans ces conditions, toute les composantes connexes de G sont des singletons : si jamais il existe g et g' dans la même composante connexe, il existe un chemin γ reliant g à g' et alors le chemin $t \mapsto g^{-1}\gamma(t)$ relie Id à $g'g^{-1}$. mais comme $G_0 = \{\text{Id}\}$, on en déduit que $g = g'$. Ainsi, les composantes connexes de G sont des singletons. On va maintenant raisonner par l'absurde en supposant que $G \neq \{\text{Id}\}$. Soit $g \in G$ différent de l'identité, $h \in \text{SO}_3(\mathbb{R})$ d'angle de rotation θ . On note h_t la rotation d'angle $t\theta$. L'application $t \mapsto h_t$ est continue et, pour tout $g \in \text{SO}_3(\mathbb{R})$, l'application $t \mapsto h_tgh_t^{-1}$ qui est un chemin de G , du fait que G est distingué. Ce chemin relie g et hgh^{-1} . Comme la composante connexe de G est réduite à un singleton, on a que $hgh^{-1} = g$. Or, si g est une rotation de droite D , alors hgh^{-1} est une rotation de droite $h(D)$. Ainsi, pour tout $h \in \text{SO}_3(\mathbb{R})$, $h(D) = D$, ce qui est impossible : il n'est pas possible d'avoir une droite stable par toute isométrie de $\mathbb{R}^3$ (il suffit de prendre une rotation d'angle différent de 0 et de droite différente de D). Ainsi, $G = \{\text{Id}\}$ et donc $\text{SO}_3(\mathbb{R})$ est simple.

4 Quelques remarques en vrac

4.1 Simplicité de $\text{PSO}_n(\mathbb{R})$

Pour $n \geq 2$, on peut définir le groupe $\text{PSO}_n(\mathbb{R})$ comme étant le quotient du groupe spécial orthogonal $\text{SO}_n(\mathbb{R})$ par son centre. Selon si n est pair ou impair, le centre de $\text{SO}_n(\mathbb{R})$ est restreint à Id ou à $\pm \text{Id}$. Un fait général, que l'on peut retrouver dans *Cours d'Algèbre* de Perrin page 150, est le fait que le groupe $\text{PSO}_n(\mathbb{R})$ est simple pour $n \geq 5$ et $n \neq 4$. L'idée de la preuve est de se ramener au cas de $\text{SO}_3(\mathbb{R})$ et d'utiliser la simplicité de ce groupe afin de conclure.

4.2 Sur l'importance des hypothèses

Juste quelques remarques un peu culturelles avec des références sur l'importance de toutes les hypothèses. Ça dépasse pas mal le cadre de l'agreg pour les derniers points mais c'est stylé.

Tout d'abord, le fait que l'on travaille avec des matrices orthogonales associées à la forme quadratique $q(x, y, z) = x^3 + y^3 + z^3$ est crucial. En effet, avec une forme quadratique générale, les renversements ne sont pas nécessairement conjugués. Je renvoie à Perrin, page 150, pour plus de détails.

Le fait que $\mathbb{R}$ soit euclidien apparaît lorsque l'on dit que les renversements sont tous conjugués dans $\mathrm{SO}_3(\mathbb{R})$, ce qui est par exemple faux dans $\mathrm{SO}_3(\mathbb{Q})$. Il y a un contre-exemple à cela dans Perrin, page 155 exo 3.

Le fait que $\mathbb{R}$ soit archimédien est aussi vital. En effet, si l'on considère $\mathbb{K}$ un corps qui est "presque" $\mathbb{R}$, à savoir un corps euclidien et totalement ordonné⁶.

5 Bibliographie

Il faut détailler quelques lemmes et bout de démonstration, mais la preuve qui se trouve dans *Oraux d'X-ENS Algèbre 3* de Francinou se suffit à elle-même. J'ai suivi le même plan de preuve que ce qui est proposé, qui selon moi fonctionne bien. Pour les pré-requis et des infos sur $\mathrm{SO}_3(\mathbb{R})$, j'ai utilisé le *Cours d'algèbre* de Perrin (notamment sur le fait que $\mathrm{SO}_3(\mathbb{K})$ n'est pas simple pour un corps qui est "presque" $\mathbb{R}$).

6. Au cas-ou vous vous demandez, ça existe bien. On prend un ordre sur $\mathbb{R}[X]$, on l'étend en un ordre sur $\mathbb{R}(X)$. L'idée est après de prendre une clôture euclidienne de $\mathbb{R}(X)$, mais là on sort complètement du programme de l'agreg. Si jamais ça vous intéresse, une telle construction est faite dans *Algebra* de Lang, au chapitre IX.