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

I Le développement

Le but de ce développement est de démontrer que le groupe $\mathrm{SO}_3(\mathbb{R})$ est un groupe simple, c'est-à-dire qu'il n'admet pas de sous-groupes distingués non triviaux (c'est-à-dire différent du groupe trivial et du groupe tout entier), grâce à une démonstration proche (dans le fond) de celle donnant la simplicité de $\mathfrak{A}_n$ pour $n \geq 5$.

Lemme 1 : [Hassan, p.714]
Soit $n \in \mathbb{N}^*$.
$\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs.

Preuve :
$*$ Pour $n = 1$, on a $\mathrm{SO}_n(\mathbb{R}) = \{1\}$ donc la propriété est vraie.

$*$ Pour $n \geq 2$ et $A \in \mathrm{SO}_n(\mathbb{R})$, on sait par la réduction des isométries vectorielles qu'il existe $P \in \mathrm{O}_n(\mathbb{R})$ et une matrice diagonale par blocs de la forme $D = \mathrm{diag}(I_r, -I_s, R(\theta_1), ..., R(\theta_k))$ telles que :

$$A = PDP^{\perp} \text{ et } \forall i \in [\![1;k]\!],\ R(\theta_i) = \begin{pmatrix} \cos(\theta_i) & -\sin(\theta_i) \\ \sin(\theta_i) & \cos(\theta_i) \end{pmatrix} \text{ avec } \theta_i \in]0;\pi[$$

Comme on a $\det(A) = 1$, on sait que s est pair et donc on peut écrire $-I_s$ sous la forme d'une matrice diagonale de $\frac{s}{2}$ blocs de la forme :

$$R(\pi) = \begin{pmatrix} \cos(\pi) & -\sin(\pi) \\ \cos(\pi) & \sin(\pi) \end{pmatrix}$$

On pose alors l'application :

$$\gamma : \left| \begin{array}{ccc} \mathrm{SO}_n(\mathbb{R}) & \longrightarrow & \mathrm{SO}_n(\mathbb{R}) \\ t & \longmapsto & P\,\mathrm{diag}(I_r, R(t\pi), ..., R(t\pi), R(t\theta_1), ..., R(t\theta_k))P^{\perp} \end{array} \right.$$

L'application γ est alors bien définie et continue et de plus, $\gamma(0) = I_n$ et $\gamma(1) = A$.

Finalement, en utilisant le fait que la relation d'être relié par un chemin continu est une relation d'équivalence, on en déduit que $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs.

■

Théorème 2 : [Francinou, p.67]
Le groupe $\mathrm{SO}_3(\mathbb{R})$ est simple.

Preuve :
$*$ Soit G un sous-groupe distingué de $\mathrm{SO}_3(\mathbb{R})$.
On note H la composante connexe de G contenant I_3.
Puisque l'application :

$$\lambda : \left| \begin{array}{ccc} H \times H & \longrightarrow & G \\ (h_1, h_2) & \longmapsto & h_1 \cdot h_2^{-1} = h_1 \,\mathrm{Com}(h_2)^{\intercal} \end{array} \right.$$

est continue (car polynomiale en les coefficients de h_1 et h_2), on en déduit que $\lambda(H \times H)$ est une partie connexe de G contenant $I_3 = \lambda(I_3, I_3)$. On a donc $\lambda(H \times H) \subseteq H$ et ainsi on a H qui est un sous-groupe de G par caractérisation.

$*$ Soit $\sigma \in \mathrm{SO}_3(\mathbb{R})$.
Posons l'application :

$$\alpha : \left| \begin{array}{ccc} H & \longrightarrow & G \\ h & \longmapsto & \sigma h \sigma^{-1} \end{array} \right.$$

L'application α est bien définie (car G est distingué dans $\mathrm{SO}_3(\mathbb{R})$) et elle est continue (pour les mêmes raisons que l'application λ précédente). On obtient alors que $\alpha(H) = \sigma H \sigma^{-1}$ est une partie connexe de G contenant $I_3 = \alpha(I_3)$, donc $\alpha(H) \subseteq H$ et ainsi H est distingué dans $\mathrm{SO}_3(\mathbb{R})$ (car stable par conjugaison).

$*$ Si H n'est pas le sous-groupe trivial :
On considère alors l'application $A : H \longrightarrow [0;\pi]$ qui associe à chaque élément de H son angle géométrique (c'est-à-dire son angle orienté au signe près car si l'on change l'orientation de l'axe de la rotation alors l'angle est changé en son opposé). En utilisant la forme réduite d'un élément de $\mathrm{SO}_3(\mathbb{R})$, une expression de A est :

$$\forall h \in H,\ A(h) = \mathrm{Arccos}\left(\frac{\mathrm{Tr}(h) - 1}{2}\right)$$

L'application A est ainsi continue.

Donc comme H est connexe et non trivial, $A(H)$ est un connexe de $[0;\pi]$ contenant $A(I_3) = 0$ et non réduit à un singleton. On en déduit qu'il existe $\varepsilon > 0$ tel que $[0;\varepsilon] \subseteq A(H)$. En particulier, il existe un entier $N \in \mathbb{N}^*$ tel que $\frac{\pi}{N} \in A(H)$, donc il existe une rotation $r \in H$ d'angle géométrique $\frac{\pi}{N}$. On en déduit que $r^N \in H$ est un retournement (car r^N est une symétrie orthogonale par rapport à un sous-espace de codimension 2).

Comme H est distingué dans $\mathrm{SO}_3(\mathbb{R})$, on en conclut que H contient tous les retournements et donc que $H = \mathrm{SO}_3(\mathbb{R})$ (car les retournements engendrent $\mathrm{SO}_3(\mathbb{R})$ et sont conjugués dans $\mathrm{SO}_3(\mathbb{R})$) et ainsi $G = \mathrm{SO}_3(\mathbb{R})$.

$*$ Si désormais $H = \{I_3\}$, alors pour $g \in G$, on définit l'application continue :

$$\beta_g : \left| \begin{array}{ccc} SO_3(\mathbb{R}) & \longrightarrow & G \\ \sigma & \longmapsto & [\sigma, g] = \sigma g \sigma^{-1} g^{-1} \end{array} \right.$$

Comme $SO_3(\mathbb{R})$ est connexe et que β_g est continue (pour les mêmes arguments que λ et α), l'image de β est connexe et contient $\beta_g(I_3) = I_3$. On en déduit que $\beta_g(SO_3(\mathbb{R})) \subseteq H = \{I_3\}$ et ainsi on a :

$$\forall \sigma \in SO_3(\mathbb{R}), \ \sigma g = g\sigma$$

Donc $g \in Z(SO_3(\mathbb{R})) = \{I_3\}$ et ainsi, on obtient que $G = \{I_3\}$.

Finalement, on en déduit que $SO_3(\mathbb{R})$ est un groupe simple.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Dans ce développement, on a utilisé de manière cruciale les deux propositions suivantes :

Proposition 3 : [Perrin, p.142]
Soit n un entier naturel supérieur ou égal à 3.
Le centre de $SO_n(\mathbb{R})$ est $\{-I_n; I_n\} \cap SO_n(\mathbb{R})$.

Preuve :
Soit n un entier naturel supérieur ou égal à 3.
On note τ_P le retournement de $\mathbb{R}^n$ de plan P.
Si $u \in SO_n(\mathbb{R})$ est dans le centre, alors pour tout plan P de $\mathbb{R}^n$, on a :

$$\tau_{u(P)} = u\tau_P u^{-1} = \tau_P$$

En effet, on utilise le fait que u est central et que $\tau_{u(P)}$ et $u\tau_P u^{-1}$ sont deux symétries orthogonales ayant les mêmes sous-espaces propres associés respectivement aux valeurs propres -1 et 1.

On en déduit que u laisse stable tous les plans de $\mathbb{R}^n$. Or comme $n \geq 3$, toute droite de $\mathbb{R}^n$ est l'intersection de deux plans de $\mathbb{R}^n$, on en déduit que toutes les droites sont stables par u. Ainsi u est une homothétie et donc $u \in \{-I_n; I_n\}$ (car u est une isométrie).

Donc on a finalement que $Z(SO_n(\mathbb{R})) = \{-I_n; I_n\} \cap SO_n(\mathbb{R})$.

■

Proposition 4 : [Perrin, p.143]
Soit n un entier naturel supérieur ou égal à 3.
L'ensemble des retournements engendre le groupe $SO_n(\mathbb{R})$.

Preuve :
Soit n un entier naturel supérieur ou égal à 3.
Soit $u \in SO_n(\mathbb{R})$.
L'élément u est le produit d'un nombre pair de réflexions (théorème de Cartan-Dieudonné) et ce produit est composé d'au plus n réflexions, donc il suffit de prouver qu'un produit de deux réflexions est un produit de retournements.

Si $n = 3$, alors pour u étant l'identité il n'y a rien a faire et sinon on a $u = \tau_1\tau_2$ avec τ_1 et τ_2 des réflexions. Or comme ici $n = 3$, $-\tau_1$ et $-\tau_2$ sont des retournements, donc $u = (-\tau_1)(-\tau_2)$.

Pour $n > 3$, on considère H_1, H_2 les hyperplans de deux réflexions τ_1 et τ_2 et V un sous-espace vectoriel de dimension $n-3$ de $H_1 \cap H_2$ (bien possible car $n > 3$). On a alors $(\tau_1\tau_2)|_V = \mathrm{Id}_V$, donc $(\tau_1\tau_2)\left(V^\perp\right) \subseteq V^\perp$ et par le cas $n = 3$ on a $(\tau_1\tau_2)|_{V^\perp}$ qui est un produit de deux retournements de $V^\perp$ et on obtient le résultat en prolongeant ces deux renversements par l'identité sur V.

■

Proposition 5 : [Perrin, p.144]
Soit n un entier naturel supérieur ou égal à 3.
Les retournements de $\mathbb{R}^n$ sont tous conjugués dans $SO_n(\mathbb{R})$.

Preuve :
Soit n un entier naturel supérieur ou égal à 3.
$*$ Montrons tout d'abord le résultat suivant :
Si V_1 et V_2 sont deux sous-espaces vectoriels de $\mathbb{R}^n$ de même dimension, alors il existe $u \in SO_n(\mathbb{R})$ tel que $u(V_1) = V_2$.

En effet, considérons V_1 et V_2 sont deux sous-espaces vectoriels de $\mathbb{R}^n$ de même dimension.
Notons $(e_1, ..., e_p)$ (respectivement $(\varepsilon_1, ..., \varepsilon_p)$) une base orthonormée de V_1 (respectivement une base orthonormée de V_2), que l'on complète avec une base orthonormée $(e_{p+1}, ..., e_n)$ (respectivement $(\varepsilon_{p+1}, ..., \varepsilon_n)$) de $V_1^\perp$ (respectivement de $V_2^\perp$).
En posant alors $u \in GL_n(\mathbb{R})$ tel que l'on ait pour tout $i \in [\![1;n]\!]$, $u(e_i) = \varepsilon_i$ on a $u(V_1) = V_2$ et puisque u transforme une base orthonormée en une base orthonormée, on en déduit que u est une isométrie. De plus, quitte à remplacer ε_1 par $-\varepsilon_1$, on a alors que $u \in SO_n(\mathbb{R})$.

$*$ Soient r_1, r_2 deux retournements de $\mathbb{R}^n$ par rapport aux sous-espaces respectifs V_1 et V_2 de codimension 2.
Par ce qui précède, il existe $u \in SO_n(\mathbb{R})$ tel que $u(V_1) = V_2$ et ainsi ur_1u^{-1} est la symétrie orthogonale par rapport à $u(V_1) = V_2$. Autrement dit, ur_1u^{-1} est le retournement par rapport à V_2 et donc $ur_1u^{-1} = r_2$.

■

Remarque 6 :
On déduit de ces deux propriétés que si G est un sous-groupe distingué de $SO_n(\mathbb{R})$ qui contient un retournement, alors $G = SO_n(\mathbb{R})$.

II.2 Pour aller plus loin...

II.2.1 Simplicité des groupes orthogonaux

Le groupe $SO_n(\mathbb{R})$ n'est pas simple si n est pair, car son centre est un sous-groupe distingué qui n'est pas trivial. On considère alors $PSO_n(\mathbb{R})$ le groupe quotient de $SO_n(\mathbb{R})$ par son centre.

Théorème 7 : [Perrin, p.150]
Si $n = 3$ ou $n \geq 5$, alors le groupe $PSO_n(\mathbb{R})$ est simple.

Preuve :
$*$ Le cas où $n = 3$ a été traité dans le développement (car $PSO_3(\mathbb{R}) \cong SO_3(\mathbb{R})$).

$*$ Supposons que $n \geq 5$.
On doit montrer que si G est un sous-groupe distingué de $SO_n(\mathbb{R})$ contenant strictement le centre de $SO_n(\mathbb{R})$, alors $G = SO_n(\mathbb{R})$. L'idée est de construire un sous-espace vectoriel F de $\mathbb{R}^n$ de dimension 3 tel que le sous-groupe distingué $SO(F) \cap G$ de $SO(F)$ est non trivial où l'on pose :

$$SO(F) = \{u \in SO_3(\mathbb{R}) \text{ tq } u(F) = F \text{ et } u_{F^\perp} = \mathrm{Id}_{F^\perp}\} \cong SO_3(\mathbb{R})$$

On en déduit alors avec le cas $n = 3$ que G contient un retournement.

On obtient donc finalement le résultat.

■

Remarque 8 :
$*$ Les groupes $SO_1(\mathbb{R})$ et $PSO_1(\mathbb{R})$ sont triviaux.
$*$ Le groupe $SO_2(\mathbb{R})$ est abélien, donc $PSO_2(\mathbb{R})$ est trivial.
$*$ Si $n \in \mathbb{N}\backslash\{0;1\}$ est un entier impair, alors $PSO_n(\mathbb{R}) \cong SO_n(\mathbb{R})$ est simple.

Le cas où $n = 4$ est exceptionnel, et on a même le résultat suivant :

Théorème 9 : [Perrin, p.166]
Le groupe $PSO_4(\mathbb{R})$ est isomorphe à $SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$.

Remarque 10 : [Perrin, p.167]
On en déduit en particulier que $PSO_4(\mathbb{R})$ n'est pas simple.

II.2.2 Simplicité des groupes unitaires

On donne ici l'analogue des résultats précédents dans le cas complexe.

On montre avec des méthodes analogues à celles exposées précédemment que le centre de $\mathrm{SU}_n(\mathbb{C})$ est $Z(\mathrm{SU}_n(\mathbb{C})) = \{\lambda \cdot I_n,\ \lambda \in \mathbb{C} \text{ tq } \lambda^n = 1\}$.

Théorème 11 :
Pour tout entier naturel n supérieur ou égal à 2, le groupe $\mathrm{PSU}_n(\mathbb{C})$ est simple.

Remarque 12 : [Perrin, p.167]
$*$ On a $\mathrm{SU}_1(\mathbb{C}) \cong \mathrm{SO}_2(\mathbb{R})$ est abélien, donc $\mathrm{PSU}_1(\mathbb{C})$ est trivial.
$*$ On a $\mathrm{PSU}_2(\mathbb{R}) \cong \mathrm{SO}_3(\mathbb{R})$ (donc on retrouve le fait que $\mathrm{PSU}_2(\mathbb{R})$ est simple).

II.2.3 Les groupes topologiques

Dans le développement, on a utilisé à la fois des notions de topologie et des notions sur les groupes. Certaines des propriétés vues dans la démonstration du développement se généralisent.

Rappelons qu'un groupe topologique est un groupe muni d'une topologie telle que les applications de multiplication $m : G \times G \longrightarrow G$ et d'inversion $\iota : G \longrightarrow G$ soient continues. Par exemple, le groupe $\mathrm{SO}_n(\mathbb{R})$ est un groupe topologique.

On a le résultat suivant dont la démonstration est identique à celle du développement :

Proposition 13 :
Soit G un groupe topologique d'élément neutre noté e_G.
La composante connexe de e_G est un sous-groupe distingué de G.

Citons également le résultat suivant :

Proposition 14 :
Soit G un groupe topologique.
Si H est un sous-groupe ouvert de G, alors il est aussi fermé.

Preuve :
Soit G un groupe topologique.
On considère H un sous-groupe ouvert de G.

On a alors $G \backslash H$ qui est la réunion des ouvert $g \cdot H$ pour $g \in G \backslash H$ et donc $G \backslash H$ est un ouvert de G.

Finalement, H est un fermé de G.

■

II.3 Recasages

Recasages : 103 - 106 - 108 - 158 - 161 - 204.

III Bibliographie

— Nawfal El Hage Hassan, *Topologie générale et espaces normés*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 3*.

— Daniel Perrin, *Cours d'algèbre*.