Étude de $O(p,q)$

Julie Parreaux

2018-2019

Référence du développement : H2G2 [1, p.210]

Leçons où on présente le développement : 106 (Groupe linéaire) ; 156 (Exponentielle de matrice) ; 170 (Forme quadratique).

1 Introduction

On souhaite étudier le groupe $O(p,q)$ formé de la forme quadratique standard sur $\mathbb{R}^{p+q}$. Pour cela, on fait apparaître un isomorphisme entre $O(p,q)$ et $O(p) \times O(p) \times \mathbb{R}^{pq}$. On utilise alors la notion d'orthogonalité et les propriétés de l'exponentielle de matrices.

On commence par donner le cadre et quelques définitions préliminaires.

Définition. On appelle groupe orthogonal l'ensemble $O_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}), {}^tAA = I_n\}$.

Définition. Soient $p,q \in \mathbb{N}$. On note $O(p,q)$ le sous-groupe de $GL_{p+q}(\mathbb{R})$ formé des isométries de la forme quadratique standard sur $\mathbb{R}^{p+q}$ de signature (p,q), c'est-à-dire $x_1^2 + \cdots + x_{p-1}^2 - \cdots - x_{p+q}^2$. La représentation matricielle de cette forme dans la base canonique est donnée par $I_{(p,q)} = \mathring{Diag}(\underbrace{1,\ldots,1}_{p \text{ fois}},\underbrace{-1,\ldots,-1}_{q \text{ fois}})$. On a alors $O(p,q) = \{M \mid MI_{(p,q)}\,{}^tM\}$.

Montrons alors l'isomorphisme de $O(p,q)$ dans les groupes orthogonaux correspondant : $O(p,q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$.

2 Étude de $O(p,q)$

Théorème. *Soit $p,q \neq 0$. Il existe un homéomorphisme*

$$O(p,q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$$

Schéma du développement

1. Par la décomposition polaire, on exhibe $S \in S_n^{++}(\mathbb{R})$ et $O \in O_n(\mathbb{R})$. De plus, $S, O \in O(p,q)$.
   (a) $O(p,q)$ est stable par transposition.
   (b) $S^2 \in O(p,q)$
   (c) $S \in O(p,q)$
2. $O(p,q) \cap O_n(\mathbb{R}) \simeq O(p) \times O(q)$
3. $O(p,q) \cap S_n^{++}(\mathbb{R}) \simeq \mathbb{R}^{pq}$

Démonstration. Soit $M \in O(p,q) \subset GL_n(\mathbb{R})$ avec $n = p+q$. Par la décomposition polaire, il existe deux matrices $O \in O_n(\mathbb{R})$ et $S \in S_n^+ + (\mathbb{R})$ telles que $M = OS$.

Étape 1 : Montrons que S et O sont dans $O(p,q)$. Pour cela, il suffit de montrer que S l'est (par la structure de groupe de $O(p,q)$ car $O = MS^{-1} \in O(p,q)$). Soit $T = {}^t MM$. On a $S^2 = T$.

Montrer que $O(p,q)$ est stable par transposition

$$\begin{array}{lll} M \in O(p,q) & \Rightarrow & MI_{(p,q)}\,{}^tM = I_{(p,q)} \quad \text{(définition de } O(p,q)) \\ \text{(on pose } \varphi(M) = {}^t M^{-1} \text{ un automorphisme de } GL_n(\mathbb{R})) & & \\ & \Rightarrow & {}^tM^{-1} I_{(p,q)} M^{-1} = I_{(p,q)} \quad \text{(applique } \varphi \text{ : commute avec la transposée et laisse stable } I_{(p,q)}) \\ & \Rightarrow & {}^tM^{-1} \in O(p,q) \quad \text{(définition de } O(p,q)) \\ & \Rightarrow & {}^tM \in O(p,q) \quad (O(p,q) \text{ est un groupe}) \end{array}$$

Montrer que $S \in O(p,q)$ Comme $O(p,q)$ est stable par transposition, $T = {}^t MM \in O(p,q)$ ($O(p,q)$ est un groupe). On en déduit que $T = S^2 \in O(p,q)$. Pour conclure, prenons la racine carrée de T via l'exponentielle diviser par deux. Comme T est définie positive, on peut écrire $T = \exp U$ pour $U \in S_n(\mathbb{R})$ convenable (exp réalise un homéomorphisme de S_n à S_n^{++}).

$$\begin{array}{lll} T \in O(p,q) & \Leftrightarrow & TI_{(p,q)}\,{}^tT = I_{(p,q)} \quad \text{(définition de } O(p,q)) \\ & \Leftrightarrow & {}^tT = I_{(p,q)}^{-1} T^{-1} I_{(p,q)} \quad \text{(multiplication par les inverses)} \\ & \Leftrightarrow & {}^t(\exp U) = I_{(p,q)}^{-1} (\exp U)^{-1} I_{(p,q)} \quad (T = \exp U) \\ & \Leftrightarrow & (\exp\,{}^tU) = \exp(-I_{(p,q)}^{-1} U I_{(p,q)}) \quad \text{(propriété de l'exponenetielle)} \\ & \Leftrightarrow & {}^tU = U = -I_{(p,q)}^{-1} U I_{(p,q)} \quad \text{(bijectivité de exp)} \\ & \Leftrightarrow & UI_{(p,q)} + I_{(p,q)} U = 0 \quad \text{(linéaire)} \\ & \Leftrightarrow & \frac{U}{2} I_{(p,q)} + I_{(p,q)} \frac{U}{2} = 0 \quad \text{(linéaire)} \\ & \Leftrightarrow & \frac{{}^tU}{2} = -I_{(p,q)}^{-1} \frac{U}{2} I_{(p,q)} \quad \text{(linéarité et } U = {}^t U) \\ & \Leftrightarrow & \exp\left(\frac{{}^tU}{2}\right) = \exp\left(-I_{(p,q)}^{-1} \frac{U}{2} I_{(p,q)}\right) \quad \text{(bijectivité de exp)} \\ & \Leftrightarrow & {}^t \exp\left(\frac{U}{2}\right) = -I_{(p,q)}^{-1} \exp\left(\frac{U}{2}\right)^{-1} I_{(p,q)} \quad \text{(propriété de l'exponentielle)} \end{array}$$

Or, on a $\exp\left(\frac{U}{2}\right) \in S_n(\mathbb{R})$ et $\exp^2\left(\frac{U}{2}\right) = \exp(U) = T$. On en déduit que $\exp\left(\frac{U}{2}\right) = S$ et $SI_{(p,q)}\,{}^tS = I_{(p,q)}$, c'est-à-dire $S \in O(p,q)$. Et, $O \in O(p,q)$ et la décomposition polaire $M = OS \mapsto (O,S)$ induit une bijection continue : $O(p,q) \simeq (O(p,q) \cap O(n)) \times (O(p,q) \cap S_n^{++})$.

Montrons que $O(p,q) \cap O_n(\mathbb{R}) \simeq O(p) \times O(q)$ Soit $O \in O(p,q) \cap O_n(\mathbb{R})$.

— On découpe O en blocs : $O = \begin{pmatrix} A & C \\ B & D \end{pmatrix} \in O(p,q)$.

$${}^tOI_{(p,q)}O = I_{(p,q)} \Leftrightarrow \begin{cases} {}^tAA - {}^tBB &= I_p \\ {}^tAC - {}^tBD &= 0 \\ {}^tCA - {}^tDB &= 0 \\ {}^tCC - {}^tDD &= -I_q \end{cases}$$

(application de la transposée et multiplication des matrices par bloc)

— Comme $O \in O(n)$ (car dans l'intersection), ${}^tOO = I_n$, on en déduit que $OI_{(p,q)} = I_{(p,q)}O$: O et $I_{(p,q)}$ commutent. Par calcul, on voit que B et C sont nuls, ainsi que $A \in O(p)$ et $D \in O(q)$.

— Ainsi $O(p,q) \cap O(n) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, A \in O(p), D \in O(q) \right\} \equiv O(p) \times O(q)$.

Montrons que $O(p,q) \cap S_n^{++}(\mathbb{R}) \simeq \mathbb{R}^{pq}$ On utilise le caractère bijectif de la fonction exponentielle : $\exp : S_n(\mathbb{R}) \to S_n^{++}(\mathbb{R})$.

— $\exp : L = \{u \in \mathcal{M}_n(\mathbb{R}), UI_{(p,q)} + I_{(p,q)} = 0\} \to O(p,q)$. D'où $S_n(\mathbb{R}) \cap L \simeq O(p,q) \cap S_n^{++}(\mathbb{R})$.

— $\dim \Sigma_n(\mathbb{R}) = \frac{n(n+1)}{2}$ et $\dim L \cap S_n(\mathbb{R}) = pq$. Donc $O(p,q) \cap S_n^{++} \simeq R^{pq}$.

□

3 Compléments autours du groupe $O(p,q)$

Groupe orthogonal

Soit E un $\mathbb{R}$-espace vectoriel. On va définir le groupe orthogonal, sous-groupe de $GL(E)$, $O_n(\mathbb{R})$ [3, p.141]. Le groupe orthogonal peut également être vu comme le groupe du stabilisateur de I_n par l'action de congruence sur $GL(E)$ [1, p.259]. Cette définition se généralise très bien à tous les corps.

Définition. Soit q une forme quadratique définie positive sur E de forme polaire f, on note $O(q)$ le groupe orthogonal composé de l'ensemble des transformations orthogonales : $O(q) = \{u \in \mathrm{End}(E) \mid f(u(x),u(y)) = f(x,y) \forall x,y \in E\}$.

Remarque : On définit un groupe orthogonal en fonction d'une forme quadratique de signature n (on passe de l'un à l'autre des représentation via les bases orthogonales).

Définition. On appelle groupe orthogonal l'ensemble $O_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}), {}^tAA = I_n\}$.

Définition. On appelle groupe orthogonal spécial l'ensemble $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}), \det A = 1\}$.

Théorème.
1. *Le centre de $O(q)$ est $Z = \{-Id, Id\}$.*
2. *Le centre de $SO(q)$ est $Z \cap SO(q)$.*

Démonstration. Si u commute avec tout le monde, u laisse invariante toute droite. □

Théorème. *Le groupe $O(q)$ est engendré par les réflexions orthogonales. Plus précisément, si $u \in O(q)$, u est le produit d'au plus n réflexions.*

Démonstration. Raisonnement par récurrence sur $p_u = n - \dim F_u$ où $F_u = \{x \in E \mid u(x) = x\}$: u produit d'au plus p_u réflexions. □

Théorème. *Le groupe $SO(q)$ est engendré par les renversements, si $n \geq 3$. Plus précisément, si $u \in SO(q)$, u est le produit d'au plus n renversements.*

Démonstration.
— Si $n = 3$, alors $u = \tau_1\tau_2$ produit de réflexions dont les inverses sont des renversements.
— Sinon, soient τ_1, τ_2 des réflexions, il existe des renversements σ_1, σ_2 tels que $\tau_1\tau_2 = \sigma_1\sigma_2$.

□

Application : Dans le cas de $O_2(\mathbb{R})$ et $O_3(\mathbb{R})$ leurs actions peuvent permettre de définir des angles.

Décomposition polaire et applications

Le principe diviser pour régner appairait aussi dans les mathématiques : les décompositions de Dunford ou polaire en sont des exemples intéressants [1, p.347]. La décomposition polaire nous permet de régner sur les groupes classiques, du moins topologiquement.

Matrices définies positives Soit n un entier naturel. L'ensemble des matrices définies positives de taille $n \times n$ est $S_n^{++}(\mathbb{R}) = \{S \in GL_n(\mathbb{R}) :^t S = S; \forall x \in \mathbb{R}^n \setminus 0, {}^t xSx > 0\} = \{P^tP \in \mathcal{M}_n(\mathbb{R}) : P \in GL_n(\mathbb{R})\}$. Pour $x \in \mathbb{C}^n$, on note $x^* =^t \overline{x}$ ke vecteur adjoint de x ; pour $H \in \mathcal{M}_n(\mathbb{C})$, on note $M^* =^t \overline{H}$, la matrice adjointe de H. L'ensemble des matrices hermitiennes définies positives $n \times n$ est : $H_n^{++}(\mathbb{C}) = \{H \in GL_n(\mathbb{C}) : H^* = H; \forall x \in \mathbb{C}^n \setminus 0, x^*Hx > 0\} = \{PP^* \in \mathcal{M}_n(\mathbb{C}) : P \in GL_n(\mathbb{C})\}$.

Lemme. *L'action de congruence (réelle) du groupe linéaire $GL_n(\mathbb{R})$ sur $S_n^{++}(\mathbb{R})$ permet de réaliser $S_n^{++}(\mathbb{R})$ comme quotient de $GL_n(\mathbb{R})$ par le groupe orthogonal $O_n(\mathbb{R})$.*

Démonstration. Par le théorème de Sylvester (ou Gram-Schmidt), l'action est transitive. Par homéomorphisme, $S_n^{++}(\mathbb{R})$ est le quotient de $GL_n(\mathbb{R})$ par le stabilisateur de I_n (le groupe orthogonal). □

La décomposition polaire Étudions maintenant cette décomposition.

Définition. Une application f est un homéomorphisme est une application bijective continue et de réciproque continue.

Théorème. *La multiplication matricielle induit des homéomorphismes :*

1. $\mu : O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \xrightarrow{\sim} GL_n(\mathbb{R})$, $(O,S) \mapsto OS$;

2. $\mu : \mathbb{U}_n(\mathbb{C}) \times H_n^{++}(\mathbb{C}) \xrightarrow{\sim} GL_n(\mathbb{C}), (U, H) \mapsto UH.$

Démonstration. 1. — μ est bien définie et continue

— μ est surjective :

— ${}^tMM \in S_n^{++}(\mathbb{R})$ (action de congruence)

— ${}^tMM$ est diagonalisable dans une base orthonormée de matrice diagonale réelle positive (théorème spectral)

— On pose S qui est la "racine carré" de ${}^tMM$ (car diagonale réelle positive) symétrique positive (matrice de passage orthogonale, définie positive dont ses coeffiscient diagonaux sont positifs).

— On pose $O = MS^{-1}$ et ${}^tOO = I_n$.

— μ est injective :

— On pose $M = OS = O'S' : S^2 = S'^2$.

— Soit Q un polynôme tel que $Q(\lambda_i) = \sqrt{\lambda_i}$ (polynôme de Lagrange) : $S = Q(S^2) = Q(S'^2)$

— S' commute avec S'^2 (associativité) S' commute avec $Q(S'^2) = S$ (manipulation de polynômes) ; S et S' sont diagonalisable (théorème spectrale) donc S' et S sont co-diagonalisable (théorème de co-diagonalisation).

— Par le caractère de matrices symétriques : $S = S'$.

— $\mu - 1$ est continue : caractérisation de la continuité par suite et compacité de O_n. On conclut par injectivité de μ.

2. Analogue

□

Application de la décomposition polaire

Corollaire. *Pour toute matrice inversible de $\mathcal{M}_n(\mathbb{R})$, on a $|||A|||_2 = \sqrt{\rho({}^tAA)}$ où ρ est le théorème spectral donné par $\rho(M) = \max_{1 \leq i \leq n}\{|\lambda_i| : \lambda_i \in \text{Spect}(M)\}$.*

Démonstration. $A = OS : |||A|||_2 = |||S|||_2$ ($\|OS(x)\|_2 = \|S(x)\|_2$ et $|||S|||_2 = \rho(S)$ (symétrique et diagonalisable). □

Corollaire (Maximalité du groupe orthogonal)**.** *Tout sous-groupe compact de $GL_n(\mathbb{R})$ qui contient le groupe orthogonal $O_n(\mathbb{R})$ est le groupe $O_n(\mathbb{R})$ lui-même.*

Démonstration. On prend un élément de ce groupe, on lui applique la décomposition polaire. On conclut grâce à sa compacité et au corollaire précédent. □

Proposition (Maximalité du groupe orthogonal)**.** *Tout sous-groupe fini G de $GL_n(\mathbb{R})$ est conjugué à un sous-groupe de $O_n(\mathbb{R})$.*

Démonstration. Il suffit de montrer que G est le stabilisateur d'une forme quadratique définie positive q : la forme quadratique euclidienne. □

Une méthode de Newton pour la décomposition polaire Un algorithme permettant de calculer efficacement une décomposition polaire est basé sur une relation de récurrence que l'on fait converger rapidement.

Proposition. *La suite $(M_k)_{k\in\mathbb{N}}$ de $GL_n(\mathbb{R})$ donné par $M_0 = M$ et $M_{k+1} = \frac{1}{2}M_k(I_n + ({}^tM_kM_k)^{-1})$ converge vers O, où $M = OS$ est la décomposition polaire de $M \in GL_n(\mathbb{R})$. La suite $({}^tM_kM)_k$ converge vers S.*

Démonstration. — Par récurrence, on montre que $M_k \in GL_n(\mathbb{R})$: congruence des matrices symétriques.

— Décomposition polaire pour $M_k = O_kS_k$: montrons que M_k tend vers O

— $O_{k+1} = O_k$ et $S_{k+1} = \frac{1}{2}(S_k + S_k^{-1})$: unicité de la décomposition polaire

— $S_k \to I_n$ et $O_k = O$: diagonalisation simultanée entre S_k et S_k^{-1}

□

Complément sur la réduction des endomorphismes autoadjoints [2, p.240] Nous allons étudier le théorème spectrale qui permet d'assurer que nous pouvons diagonaliser l'ensemble des matrices symétrique [2, p.240]. Plus généralement, on souhaite réduire les endomorphismes autoadjoints.

Définition. Soit E un espace euclidien ou hermitien. Un endomorphisme de E, u est dit autoadjoint si $u^* = u$.

Lemme. *Soit E un espace euclidien ou hermitien et $f \in \mathcal{L}(E)$ un endomorphisme autoadjoint. Si F est un sous-espace vectoriel de E stable par f, alors $F^\perp$ est stable par f.*

Démonstration. $\forall x \in F, \forall y \in F^\perp, x.f(y) = f(x).y = 0$. □

Théorème (Théorème spectral)**.** *Soit E un espace euclidien ou hermitien et $f \in \mathcal{L}(E)$ un endomorphisme autoadjoint. Alors, il existe une base orthonormée de vecteur propre pour f (de plus ses valeurs propres sont réelles).*

Démonstration. On raisonne par récurrence sur la dimension de E.

- $n = 1$: ok
- $n \in \mathbb{N}$ tel que la propriété est vrai pour $n - 1$
  - On pose $\psi : E \to \mathbb{R}$ tel que $x \mapsto x.f(x)$ est une forme quadratique : $\exists x_0 \in S$ (où S est la sphère unitaire) tel que $\psi(x_0) = \sup_{s \in S} \psi(x) = \lambda$ (dimension finie).
  - On considère $\psi_1(x) = \lambda \|x\|^2 - \psi(x)$ une forme quadratique dégénérée : l'application $\lambda Id_E - f$ n'est pas surjective : existence de e_1.
  - On pose $H = \text{Vect}(e_1)^\perp$ qui est stable par f. On peut alors restreindre f à H et appliqué l'hypothèse de récurrence.

□

Corollaire (Interprétation matricielle)**.** *Soit $M \in \mathcal{M}_n(\mathbb{R})$ (respectivement $M \in \mathcal{M}_n(\mathbb{C})$) une matrice symétrique (respectivement hermitienne). Alors, il existe une matrice C orthogonale (respectivement unitaire) telle que $C^{-1}MC = c^*MC = D$ où D est une matrice diagonale réelle.*

Démonstration. On muni E d'un produit scalaire, ce qui nous donne les bonnes bases pour appliquer le théorème spectral. □

Corollaire. *Soit ψ une forme quadratique (respectivement hermitienne) sur un espace euclidien (respectivement hermitien) E. Alors, il existe une base orthonormée de E dans laquelle la matrice est diagonale réelle.*

Démonstration. On utilise l'interprétation matricielle de ψ dans une base orthonormée et on applique le corollaire précédent. □

Corollaire. *Soient M, N deux matrices symétriques (respectivement hermitiennes) telle que M soit définie positive. Alors, il existe une matrice C inversible telle que $C^*MC = I_n$ et $C^*NC = D$ où D est diagonale réelle.*

Démonstration. On applique le corollaire précédent au produit scalaire définie par M et à la forme quadratique définie par N. □

Complément sur la réduction simultanée [2, p.240] On va étudier le cas de la réduction simultanée (dans le cadre de la diagonalisation et de la trigonalisation) [2, p.164].

Proposition. *Soient $f, g \in \mathcal{L}(E)$ tels que $f \circ g = g \circ f$. Alors,*

1. *Tout sous-espace propre de f est stable par g (en particulier* $\ker f$*).*
2. $\text{im} f$ *est stable par g*

Démonstration.
1. Définition de l'espace propre et commutativité
2. Définition de l'image et commutativité

□

Théorème (Diagonalisation simultanée)**.** *Si $f, g \in \mathcal{L}(E)$ sont diagonalisables et qu'ils commutent, alors il existe une base commune de diagonalisation de f et g (on dit que f et g sont co-diagonalisable).*

Démonstration. On utilise la proposition pour diagonaliser g dans les sous-espaces propres de f □

Remarque : La réciproque est vraie : on montre que f et g commutent dans cette base.

Théorème (Trigonalisation simultanée)**.** *Si $f, g \in \mathcal{L}(E)$ sont trigonalisables et qu'ils commutent, alors il existe une base commune de trigonalisation de f et g (on dit que f et g sont co-trigonalisable).*

Démonstration. **Préliminaire** Utilisation de la proposition pour montrer que g est trigonalisable sur les espaces propres de f. On procède par récurrence : pour montrer l'hérédité, on a deux méthodes

Méthode 1 On utilise les notions de transposée et d'orthogonalité

Méthode 2 On exhibe un élément de cette base et l'hypothèse de récurrence nous donne le reste.

□

Exponentielle de matrices

Nous allons étudier la construction de l'exponentielle et quelques une de ces propriétés algébriques et fonctionnelles [4, p.57]. Soit K un corps tel que $K = \mathbb{R}$ ou $\mathbb{C}$.

Définition. Soit A un élément de $\mathcal{M}_n(K)$; l'exponentielle de A, notée $\exp A$, est la somme dans $\mathcal{M}_n(K)$ (qui est complet), de la série normalement convergente $\sum_{n=0}^{+\infty} \frac{A^n}{n!}$.

Proposition. *La matrice* $\exp A$ *est un polynôme en* A*.*

Remarque : Il n'existe pas un unique polynôme P tel que pour tout A, $P(A) = \exp A$ (on se ramène au cas $n = 1$ et on pense aux dérivées).

Proposition. *Si* $BA = AB$, $\exp(A + B) = \exp A \exp B$.

Démonstration. Formule du binôme et convergence absolue des séries. □

Corollaire. $\exp A$ *est inversible d'inverse* $\exp(-A)$

Démonstration. On applique la proposition précédente à A et $-A$. □

Proposition. *On a* $P \exp(A) P^{-1} = \exp(PAP^{-1})$.

Démonstration. Argument de continuité. □

Proposition. *On a* $\det(\exp(A)) = \exp(\mathrm{Tr}(A))$.

Démonstration. Trigonalise (dans $\mathbb{C}$) et on applique la conjugaison. □

Théorème. *L'application* $\exp : \mathcal{M}_n(K) \to GL_n(K)$ *est une application de classe* $\mathcal{C}^1$ *(et même analytique) ; sa différentielle en* 0 *est l'identité.*

Démonstration. Utiliser le théorème sur les limites des fonctions différentielles dont les dérivées convergent uniformément sur les compacts ou utiliser le caractère polynomial. Le calcul de la différentielle est un développement à l'ordre 1. □

Références

[1] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries, tome 1*. Calvage et Mounet, 2013.

[2] X. Gourdon. *Algèbre*. Les maths en tête. Ellipses, 2009.

[3] D. Perrrin. *Cours d'algèbre*. Ellipse, 1996.

[4] R. Mneimne ; F. Testard. *Introduction à la théorue des groupes de Lie classiques*. Hermann, 1997.