Leçon 150 Exemples d'actions de groupes sur des espaces de matrices

Dorian Cacitti-Holland

2020-2021

Références.

1. Analyse matricielle de Jean-Etienne Rombaldi
2. Algèbre linéaire de Joseph Grifone
3. Algèbre et géométrie de Jean-Etienne Rombaldi
4. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
5. Algèbre de Xavier Gourdon

Développements.

1. Réduction dans $O_n(\mathbb{R})$
2. Loi de réciprocité quadratique

Table des matières

1 Action par translation

1.1 Définitions et matrices élémentaires

(Chapitre 5.4 de Analyse matricielle de Jean-Etienne Rombaldi)

1. Définition : L'action par translation à gauche de $GL_n(K)$ sur $M_n(K)$ est définie par $P.A = PA$, et celle à droite par $P.A = AP^{-1}$
2. Remarque : On peut définir de même l'action par translation à droite
3. Définition : Une matrice de transvection (respectivement dilatation) est de la forme $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ (respectivement $D_i(\lambda) = I_n + (\lambda - 1)E_{ii}$, de plus on appelle matrice élémentaire une matrice de transvection ou de dilatation
4. Proposition : $T_{ij}(\lambda)$ et $D_i(\lambda)$ sont inversibles d'inverses $(T_{ij}(\lambda))^{-1} = T_{ij}(-\lambda)$ et $(D_i(\lambda))^{-1} = D_i(\lambda^{-1})$
5. Théorème : Soit $A \in M_n(K)$, alors $T_{ij}(\lambda)A$ est la matrice A en ajoutant λ fois la j-ième ligne à la i-ième ligne de A et $D_i(\lambda)A$ est la matrice A en multipliant la i-ième ligne par λ
6. Exemple : Soit $A \in M_n(K)$, alors pour échanger les lignes i et j de A on fait agir $D_j(-1)T_{ij}(1)T_{ji}(-1)T_{ij}(1)$ sur A

1.2 Caractérisations des orbites par le pivot de Gauss

(Chapitre 5.5 de Analyse matricielle de Jean-Etienne Rombaldi et Exercice 2.1 d'Algèbre linéaire de Joseph Grifone)

1. Théorème : Soit $A \in M_n(K)$ et $b \in K^n$, alors en faisant agir des matrices élémentaires sur A, on peut transformer le système linéaire $Ax = b$ en $Rx = c$ avec R triangulaire supérieure et $det(A) = det(R)$
2. Proposition : Soit $A \in GL_n(K)$, alors la méthode est la suivante :
   — Il existe $i \in [\![1, n]\!], a_{i1} \neq 0$, donc on permute les lignes i et 1 de A pour se ramener à $A^{(1)}$ avec $a_{11}^{(1)} \neq 0$
   — On élimine les $a_{i1}^{(1)}$ en faisant agir $T_{i1}\left(-\frac{a_{i1}^{(1)}}{a_{11}^{(1)}}\right)$ sur $A^{(1)}$
   — Il existe $i \in [\![2, n]\!]$ tel que $a_{i2}^{(2)} \neq 0$, donc on permute les lignes i et 2 de $A^{(2)}$ pour se ramener à $A^{(3)}$ avec $a_{11}^{(3)}, a_{22}^{(3)} \neq 0$ et $\forall i [\![2, n]\!], a_{i1}^{(3)} = 0$
   — On répète ces étapes pour obtenir $R = A^{(k)}$ triangulaires supérieures de diagonale sans élément nul
3. Remarque : On obtient donc un représentant simple de l'orbite de A
4. Application : Ce représentant permet de résoudre le système linéaire $Ax = b$
5. Exemple : Si $A = \begin{pmatrix} 2 & 1 & -2 \\ 1 & 1 & 4 \\ 7 & 5 & 1 \end{pmatrix}$ alors un représentant simple de l'orbite de A est $R = \begin{pmatrix} 1 & 1 & 4 \\ 0 & 1 & 10 \\ 0 & 0 & 7 \end{pmatrix}$, ainsi la solution de $Ax = \begin{pmatrix} 10 \\ -9 \\ 14 \end{pmatrix}$ est $x = \begin{pmatrix} 1 \\ 2 \\ -3 \end{pmatrix}$

1.3 Restriction à $O_n(\mathbb{R})$ et décomposition polaire

(Chapitre 22.9.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Remarque : On peut restreindre l'action présente à $O_n(R)$
2. Lemme : Soit $A \in S_n^+(\mathbb{R})$ (respectivement $S_n^{++}(\mathbb{R})$), alors il existe $B \in S_n^+(\mathbb{R})$ (respectivement $S_n^{++}(\mathbb{R})$) unique tel que $A = B^t B$
3. Théorème : Soit $A \in GL_n(\mathbb{R})$, alors il existe un unique couple $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $A = OS$
4. Corollaire : Soit $A \in M_n(\mathbb{R})$, alors il existe $(O, S) \in O_n(\mathbb{R}) \times S_n^+(\mathbb{R})$ tel que $A = OS$
5. Application : Soit $A \in M_n(\mathbb{R})$, alors il existe dans l'orbite de A une matrice symétrique positive
6. Exemple : $\begin{pmatrix} -2 & -3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}$
7. Remarque : Plus précisément on a un homéomorphisme entre $O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ et $GL_n(\mathbb{R})$, de plus grâce à l'exponentielle matricielle $GL_n(\mathbb{R}) \simeq O_n(\mathbb{R}) \times S_n(\mathbb{R})$

2 Action par équivalence

2.1 Définitions et théorème du rang

(Chapitres I.1 et I.2 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

1. Définition : L'action par équivalence de $GL_m(K) \times GL_n(K)$ sur $M_{m,n}(K)$ est définie par $(P, Q).A = PAQ^{-1}$
2. Définition : L'orbite de A sous l'action de $GL_m(K) \times GL_n(K)$ est $Orb(A) = \{B \in M_{m,n}(K), \exists (P, Q), B = PAQ^{-1}\}$
3. Proposition : $Orb(A) = \{B \in M_{m,n}(K), rg(B) = rg(A)\}$
4. Corollaire : Deux matrices A, B sont dans la même orbites si et seulement si $rg(A) = rg(B)$, en particulier les orbites sont paramétrées par le rang $r \in [\![0, min(m, n)]\!]$
5. Théorème : Soit $A \in M_{m,n}(K)$ de rang r, alors il existe $P \in GL_m(K), Q \in GL_n(K)$ tel que $A = Pdiag(I_r, 0)Q^{-1}$
6. Remarque : On retrouve la formulation classique du théorème du rang $n = rg(A) + dim(ker(A))$
7. Application : Un élément simple dans l'orbite de $A \in M_{m,n}(K)$ est $diag(I_r, 0)$ avec $r = rg(A)$

2.2 Stabilisateur et bijection quotient et orbites

(Chapitre I.3 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

On considère K un corps et $m, n \in \mathbb{N}^*$.

1. Définition : Soit $A \in M_{m,n}(K)$, alors le stabilisateur de A est $Stab(A) = \{(P,Q) \in GL_m(K) \times GL_n(K), PAQ^{-1} = A\}$
2. Remarque : $Stab(A) < GL_m(K) \times GL_n(K)$
3. Lemme : Soit G un groupe agissant sur un ensemble X, $A \in X$, $\pi : G \longrightarrow G/Stab(A)$ la surjection canonique et $\alpha : G \longrightarrow Orb(A)$ l'application canonique, alors il existe une unique application $\overline{\alpha} : G/Stab(A) \longrightarrow Orb(A)$ telle que $\alpha = \overline{\alpha} \circ \pi$, de plus $\overline{\alpha}$ est bijectif
4. Remarque : Les applications du théorème précédent ne sont pas des morphismes de groupes a priori car $Orb(A)$ n'est pas nécessairement un groupe et $Stab(A)$ n'est pas nécessairement distingué dans G
5. Corollaire : Si K est un corps fini alors $|Orb(A)| = \frac{|GL_m(K)||GL_n(K)|}{|Stab(A)|}$
6. Proposition : Si $|K| = q$ alors $|GL_n(K)| = \prod_{i=0}^{n-1}(q^n - q^i)$
7. Exemple : $|GL_2(\mathbb{F}_2)| = (2^2 - 2^1)(2^2 - 2^0) = 6$
8. Proposition : $Stab(g.A) = gStab(A)g^{-1}$
9. Théorème : $Stab(A) = Stab(diag(I_r, 0)) \simeq \begin{pmatrix} GL_r(K) & M_{r,m-r}(K) \\ 0 & GL_{m-r}(K) \end{pmatrix} \times \begin{pmatrix} GL_r(K) & 0 \\ M_{n-r,r}(K) & GL_{n-r}(K) \end{pmatrix}$
10. Corollaire : Si K fini alors on en déduit le cardinal de $Stab(A)$ puis de $Orb(A)$

2.3 Topologie des orbites

(Chapitre I.4 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

On considère K le corps des réels ou des complexes et une norme sur K^n pour obtenir une topologie.

1. Définition : On définit $O_r := Orb(diag(I_r, 0))$ l'orbite des matrices de rang r
2. Proposition : $\overline{O_r} = \bigsqcup_{0 \leq k \leq r} O_k$
3. Corollaire : L'unique orbite fermée est $O_0 = \{0\}$
4. Corollaire : Soit $(A_n)_{n \in \mathbb{N}} \in M_{n,m}(K)$ de rang r et convergent vers B, alors $rg(B) \leq r$

3 Action par conjugaison

3.1 Définition et orbites

1. Définition : L'action par conjugaison de $GL_n(K)$ sur $M_n(K)$ est définie par $P.A = PAP^{-1}$
2. Définition : On dit que deux matrices $A, B \in M_n(K)$ sont semblables si A, B sont dans la même orbite
3. Exemple : Soit E un K-espace vectoriel de dimension n, $u \in End(E)$, e, f bases de E de matrice de passage P, alors $Mat_f(u) = PMat_e(u)P^{-1}$, autrement dit les matrices représentants u dans une base sont semblables

4. Proposition : Soit $A, B \in M_n(K)$ semblables, alors A, B ont même rang, trace, déterminant, valeurs propres, polynôme minimal, polynôme caractéristique
5. Remarque : Autrement dit ce sont des invariants partiels de similitudes
6. Exemple : J et 0 ont même polynôme caractéristique mais ne sont pas semblables
7. Théorème : Soit $A \in M_n(K)$, alors A diagonalisable (respectivement trigonalisable) si et seulement si π_A est scindé à racines simples (respectivement scindé)
8. Corollaire : Dans ce cas, un représentant simple de $Orb(A)$ est la matrice diagonale (respectivement triangulaire) correspondante

3.2 Invariants de similitude et réduction de Frobenius

(Annexe B d'Algèbre de Xavier Gourdon)

1. Définition : Soit $x \in E$, alors π_x est le polynôme unitaire tel que $(\pi_x) = \{P \in K[X], P(u)(x) = 0\}$ et $E_x = \{P(u)(x), P \in K[X]$
2. Proposition : Soit $x \in E$, alors E_x est sous-espace de E de dimension $deg(\pi_x)$ et de base $(x, ..., u^{deg(\pi_x)-1})$
3. Théorème : Il existe $x \in E$ tel que $\pi_x = \pi_u$
4. Définition : On dit que u est cyclique s'il existe $x \in E$ tel que $E_x = E$
5. Théorème : Si u cyclique alors il existe une base b de E tel que $Mat_b(u) = C(\pi_u)$ matrice compagnon associée à π_u
6. Théorème : Il existe $F_1, ..., F_r$ sous-espaces de E stables par u tels que $E = F_1 \oplus ... \oplus F_r$, $u_i := u_{|F_i}$ cyclique et $P_i := \pi_{u_i} \mid P_{i-1}$
7. Remarque : La suite des polynômes P_i ne dépend que de u
8. Définition : La suite des polynômes P_i est appelée les invariants de similitude de u
9. Théorème de réduction de Frobenius : Il existe une base b de E telle que $Mat_b(u) = diag(C(P_1), ..., C(P_r))$
10. Corollaire : Deux endomorphismes sont semblables si et seulement s'ils ont les mêmes invariants de similitude
11. Application : Soit $A, B \in M_n(K)$ semblables sur une extension de corps de K alors A et B sont semblables sur K

3.3 Restriction à $O_n(\mathbb{R})$

(Chapitres 22.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 7.13 d'Algèbre linéaire de Joseph Grifone)

On considère E un espace vectoriel euclidien de dimension n.

1. Définition : On dit que $P \in M_n(\mathbb{R})$ est orthogonale si ${}^tPP = I_n = P{}^tP$, on note $O_n(\mathbb{R})$ leur sous-groupe de $GL_n(\mathbb{R})$
2. Remarque : On peut donc considérer la restriction de l'action par conjugaison à $O_n(\mathbb{R})$
3. Proposition : Cette action équivaut à un changement de bases orthonormées dans E

4. Lemme : Soit $u \in O(E)$, alors il existe des sous-espaces vectoriels $F_1, ..., F_r$ de E deux à deux orthogonaux de dimension 1 ou 2 et stables par u tels que $E = \bigoplus_{i=1}^{r} F_i$
5. Proposition : Soit $u \in O(E)$ et F sous-espace vectoriel de E stable par F, alors $F^{\perp}$ est stable par u
6. Théorème de réduction des endomorphismes orthogonaux : Soit $u \in O(E)$, alors il existe une base orthonormée e de E telle que $Mat_e(u) = diag(I_p, I_q, R_1, ..., R_r)$ avec $p, q \in [\![1, n]\!], R_i = R(\theta_i), \theta_i \in]0, 2\pi[\setminus \{\pi\}$
7. Corollaire : Soit $A \in O_n(\mathbb{R})$, alors un représentant simple dans $Orb(A)$ est $diag(I_p, I_{-q}, R(\theta_1), ..., R(\theta_r))$
8. Application : Les composantes connexes de $O(E)$ sont les fermés $SO(E)$ et $O^-(E)$
9. Définition : Soit $u \in End(E)$, alors on dit que u est symétrique si $\forall x, y \in E, \langle u(x), y\rangle = \langle x, u(y)\rangle$, et on note $S(E)$ leur ensemble
10. Remarque : Soit $u \in End(E)$, alors $u \in S(E)$ si et seulement si pour toute base orthonormée b de E, $Mat_b(u) \in S_n(\mathbb{R})$
11. Théorème spectral : Soit $u \in S(E)$, alors u est diagonalisable dans une base orthonormée
12. Corollaire : Soit $A \in S_n(\mathbb{R})$, alors il existe $P \in O_n(\mathbb{R})$ tel que ${}^tPAP$ soit diagonale
13. Application : Soit $A \in S_n(\mathbb{R})$, alors il existe une matrice diagonale dans l'orbite de A sous l'action de $O_n(\mathbb{R})$ par conjugaison, donc deux matrices symétriques sont dans la même orbite si et seulement si elles ont le même polynôme caractéristique

4 Action par congruence

4.1 Définition et lien avec les matrices symétriques

(Chapitre 15.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : L'action par congruence de $GL_n(K) \times GL_n(K)$ sur $M_n(K)$ est définie par $(X, Y).A = {}^tXAY$
2. Théorème : Soit φ forme bilinéaire sur E et e, f deux bases de E de matrice de passage P, alors $Mat_f(\varphi) = {}^tPMat_eP$
3. Définition : Le discriminant d'une forme bilinéaire φ sur E dans une base e est $\Delta_e(\varphi) = det(Mat_e(\varphi))$
4. Remarque : Dans ce cas, soit e, f bases de E de matrice de passage P, alors $\Delta_f(\varphi) = (det(P))^2\Delta_e(\varphi)$

4.2 Réduction des formes quadratiques

(Chapitres 7.3 et 9.5 d'Algèbre linéaire de Joseph Grifone)

1. Définition : Une base $(e_i)_{1 \leq i \leq n}$ de E est dite orthogonale (respectivement orthonormé) pour φ si $\varphi(e_i, e_j) = \delta_{ij}\varphi(e_i, e_i)$ (respectivement δ_{ij}

2. Proposition : Soit $(e_i)_{1\leq i\leq n}$ base de E, alors e est une base orthogonale pour φ si et seulement si $Mat_e(q) = diag(q(e_1), ..., q(e_n))$
3. Remarque : Dans ce cas le rang de q est le nombre de $q(e_i)$ non nuls
4. Proposition : S'il existe une base orthonormée alors q est de rang n
5. Théorème : Il existe une base orthogonale de E pour q, autrement dit il existe une base e de E telle que $q(x) = a_1x_1^2 + ... + a_rx_r^2$ avec $a_i = q(e_i)$ et $r = rg(q)$, autrement dit $Mat_e(q) = diag(a_{11}, ..., a_{rr}, 0, ..., 0)$
6. Corollaire : Théorème spectral : Soit $A \in S_n(K)$, alors il existe $P \in GL_n(K)$ tel que ${}^tPAP$ soit diagonale
7. Application : Deux matrices A, B symétriques sont congruentes si et seulement si $\chi_A = \chi_B$

4.3 Classification et signature

(Chapitres 15.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 9.5 d'Algèbre linéaire de Joseph Grifone)

1. Théorème : Si E un $\mathbb{C}$-espace vectoriel, alors il existe une base e de E tel que $q(x) = x_1^2 + ... + x_r^2$ avec $r = rg(q)$, autrement dit $Mat_e(q) = diag(I_r, 0_{n-r})$
2. Corollaire : Dans ce cas il existe une base orthonormée pour q si et seulement si $rg(q) = n$ ie q non dégénérée
3. Théorème : Si E un $\mathbb{R}$-espace vectoriel, alors il existe une base e de E tel que $q(x) = x_1^2 + ... + x_p^2 - x_{p+1}^2 - ... - x_r^2$, ie $Mat_e(q) = diag(I_p, I_{r-p}, I_{n-r})$
4. Définition : Dans ce cas le couple $sign(q) = (p, r-p)$ est appelé signature de q
5. Corollaire : Dans ce cas q est définie négative si et seulement si $sign(q) = (n, 0)$ si et seulement il existe une base orthonormée pour q, définie négative si et seulement si $sign(q) = (0, n)$, et non dégénéré si et seulement si $sign(q) = (p, n-p)$
6. Exemple : Si $q(x) = x_1^2 + 2x_2^2 + 15x_3^2 - 4x_1x_2 + 6x_1x_3 - 8x_2x_3$ alors $sign(q) = (2, 1)$

4.4 Congruence avec un corps fini et loi de réciprocité quadratique

(Chapitres 15.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi et V.C de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

On considère p nombre premier impair, $q = p^n$, $K = \mathbb{F}_q$, $q \in Q(E)$ et φ sa forme polaire.

1. Lemme : Il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$
2. Lemme : Soit $a, b, c \in \mathbb{F}_q^*$, alors $ax^2 + by^2 = c$ admet un solution dans $\mathbb{F}_q \times \mathbb{F}_q$
3. Théorème : Si $rg(q) = r$, soit $\alpha \in \mathbb{F}_q \backslash \mathbb{F}_q^2$, alors il existe une base b de E telle que $Mat_b(q) = diag(I_{r-1}, \delta, 0_{n-r})$ avec $\delta \in \{1, r\}$
4. Corollaire : Deux formes quadratiques non dégénérées sont congruentes si et seulement si elles dans toute base b de E, $\frac{det(}{}$
5. Définition : Soit $a \in \mathbb{F}_p^*$, alors $\left(\frac{a}{p}\right) := 1$ si a est un carré et $\left(\frac{a}{p}\right) := -1$ sinon

6. Exemple : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, si p impair alors $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
7. Proposition : $a \longmapsto \left(\frac{a}{p}\right)$ est multiplicatif
8. Lemme : Soit $a \in \mathbb{Z}^*$ et q premier impair, alors $|\{x \in \mathbb{F}_q, ax^2 = 1\}| = 1 + \left(\frac{a}{q}\right)$
9. Théorème : Soit $(p, q) \in (\mathcal{P}\backslash\{2\})^2$ distincts, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
10. Exemple : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383