106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

Pandou

27 mai 2022

On fixe E un K-espace vectoriel de dimension n.

1 Le groupe linéaire : étude algébrique

1.1 Généralités, groupe spécial

Théorème-Définition 1. *Soit $u \in \mathcal{L}(E)$, on a équivalence entre :*

1. *u est injective.*
2. *u est surjective.*
3. *u est inversible.*
4. $\det(u) \neq 0$.

On note $GL(E)$ l'ensemble des endomorphismes de E qui sont inversibles. On note $GL_n(K)$ l'ensemble des matrices $n \times n$ inversibles.

Définition 2. *On définit $SL(E)$ comme le noyau du morphisme $\det : GL(E) \longrightarrow K^*$. Il s'agit en particulier d'un sous-groupe distingué de $GL(E)$.*

Proposition 3.

$$Z\big(GL(E)\big) = K^*\mathrm{Id} \qquad et \qquad Z\big(SL(E)\big) = \mu_n(K)\mathrm{Id}$$

où $\mu_n(K) = \{\lambda \in K, \lambda^n = 1\}$.

Définition 4. *On pose $PGL(E) = GL(E)/Z\big(GL(E)\big)$ et $PSL(E) = SL(E)/Z\big(SL(E)\big)$ le groupe projectif (spécial) linéaire. On notera $PGL_n(K)$ et $PSL_n(K)$ leurs équivalents matriciels.*

Proposition 5. *Soit p un nombre premier, $\alpha \in \mathbb{N}^*$ et $q = p^\alpha$.*

$\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big) = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$.

$\mathrm{Card}\big(PGL_n(\mathbb{F}_q)\big) = \mathrm{Card}\big(SL_n(\mathbb{F}_q)\big) = \dfrac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{q-1}$.

$\mathrm{Card}\big(PSL_n(\mathbb{F}_q)\big) = \dfrac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{d(q-1)}$ *avec* $d = \mathrm{pgcd}(n, q-1)$.

1.2 Générateurs

Théorème-Définition 6. *Soit H un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = \mathrm{Id}_H$. On a équivalence entre :*

1. $\det(u) := \lambda \neq 1$, *ie* $u \notin SL(E)$.
2. *u admet une valeur propre $\lambda \neq 1$ et u est diagonalisable. On note D la droite propre de u pour λ.*
3. $\mathrm{Im}(u - \mathrm{Id}) \not\subset H$.
4. *Il existe une base dans laquelle la matrice de u est $(1, ..., 1, \lambda)$.*

On dit alors que u est une dilatation d'hyperplan H, de droite D et de rapport λ et alors,

$$D = \mathrm{Im}(u - \mathrm{Id}) \qquad et \qquad H = \mathrm{Ker}(u - \mathrm{Id})$$

Théorème-Définition 7. *Soit $H = \mathrm{Ker}(f)$ un hyperplan de E et $u \in GL(E)$ tel que $u_{|H} = \mathrm{Id}_H$ et $u \neq \mathrm{Id}$. On a équivalence entre :*

1. $\det(u) := \lambda = 1$, *ie* $u \in SL(E)$.
2. *u n'est pas diagonalisable.*
3. $D := \mathrm{Im}(u - \mathrm{Id}) \subset H$.
4. *$\overline{u} : E/H \longrightarrow E/H$ est l'identité.*
5. *Il existe $a \in H \setminus \{0\}$ tel que*
$$\forall x \in E, u(x) = x + f(x)a$$
6. *Il existe une base dans laquelle la matrice de u est* $\mathrm{diag}\left(1, ..., 1, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$.

On dit alors que u est une transvection d'hyperplan H et de droite D et on a $D = \mathrm{Vect}(a) \subset H$.

Corollaire 8. *Soit $u \in GL(E)$ tel que $u \neq \mathrm{Id}$. On a équivalence entre :*

1. *u est une transvection de droite D.*
2. $u_{|D} = \mathrm{Id}$ *et* $\overline{u} : E/D \longrightarrow E/D$ *est l'identité.*

Proposition 9. *Soit u une transvection de droite D et d'hyperplan H. Soit $f \in GL(E)$, alors $f \circ u \circ f^{-1}$ est une transvection de droite $f(D)$ et d'hyperplan $f(H)$.*

Lemme 10. *Soit $x, y \in E \setminus \{0\}$. Il existe une transvection ou un produit de deux transvections qui envoie x sur y.*

Théorème 11. *Les transvections engendrent $SL(E)$.*

Corollaire 12. *Les transvections et les dilatations engendrent $GL(E)$.*

1.3 Une famille de groupes simples

Proposition 13. *Si $n \geqslant 3$, les transvections sont conjuguées dans $SL(E)$.*

Proposition 14.
1. *Dans $SL_2(K)$, toute transvection est conjuguée dans $SL(E)$ à une matrice $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, $\lambda \in K^*$.*
2. *Deux matrices $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $SL(E)$ si, et seulement si, $\dfrac{\lambda}{\mu}$ est un carré de K.*

Théorème 15. *$PSL_n(K)$ est simple sauf si, $n = 2$ et $K = \mathbb{F}_2$ ou $n = 2$ et $K = \mathbb{F}_3$.*

Théorème 16. *On a les isomorphismes exceptionnels suivants :*
1. *$GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ (qui n'est pas simple).*
2. *$PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$ (qui n'est pas simple).*
3. *$PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$.*
4. *$PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.*

2 Actions du groupe linéaire

2.1 Pivot de Gauss

Définition 17. *On définit une action de $GL_n(K)$ sur $M_{n,m}(K)$ via $P \cdot A = PA$ et de $GL_m(K)$ sur $M_{n,m}(K)$ via $Q \cdot A = AQ^{-1}$.*

Théorème 18.
1. *Deux matrices sont dans la même orbite pour l'action de translation à gauche si, et seulement si, elles ont même noyau.*
2. *Deux matrices sont dans la même orbite pour l'action de translation à droite si, et seulement si, elles ont même image.*

Remarque 19 : L'action par multiplication à gauche ne change pas les solutions d'un système linéaire. Cela justifie bien la méthode du pivot de Gauss pour la résolution d'un système linéaire.

2.2 Action par équivalence

Définition 20. *On définit une action de $GL_n(K) \times GL_m(K)$ sur $M_{n,m}(K)$ via $(P,Q) \cdot A = PAQ^{-1}$. Deux matrices dans la même orbite sont dites équivalentes.*

Théorème 21. *Deux matrices sont équivalentes si, et seulement si, elles ont même rang.*

Corollaire 22. *Toute matrice $M \in M_{n,m}(K)$ de rang $r \in [\![0, \min(n,m)]\!]$ est équivalente à la matrice J_r.*

Application 23 : Tout hyperplan de $M_n(K)$ rencontre $GL_n(K)$.

2.3 Action par similitude

Définition 24. *On définit une action de $GL_n(K)$ sur $M_n(K)$ via $P \cdot A = PAP^{-1}$. Deux matrices dans la même orbite sont dites semblables.*
On dit que A est diagonalisable si elle est semblable à une matrice diagonale.

Remarque 25 : Deux matrices semblables représentent la même application linéaire dans deux bases différentes.

Théorème 26. *Soit $A \in M_n(K)$. On a équivalence entre :*
1. *A est diagonalisable.*
2. *Le polynôme minimal de A est scindé à racines simples.*
3. *A est annulé par un polynôme annulateur scindé à racines simples.*
4. *$K^n = \bigoplus_{\lambda} \mathrm{Ker}(A - \lambda I_n)$.*

Corollaire 27. *On note $\mathcal{D}_n(K)$ l'ensemble des matrices diagonalisables de $M_n(K)$. On a une bijection*

$$\mathcal{D}_n(K)/GL_n(K) \simeq K^n/\mathfrak{S}_n$$

2.4 Action par congruence

Définition 28. *On définit une action de $GL_n(K)$ sur $S_n(K)$ via $P \cdot A = PAP^T$. Deux matrices dans la même orbite sont dites congruentes.*

Remarque 29 : Deux matrices congruentes représentent la même forme quadratique dans deux bases différentes.

Théorème 30 (Réduction de Gauss). *Toute matrice symétrique est congruente à une matrice diagonale.*

Remarque 31 : Cette matrice diagonale n'est pas unique, même à réordonnement de la diagonale près.

Théorème 32 (Classification dans $\mathbb{C}$)**.** *Soit $A, B \in S_n(\mathbb{C})$, alors A et B sont congruentes si, et seulement si, elles ont même rang.*

Théorème 33 (Classification dans $\mathbb{R}$)**.** *Soit $A \in S_n(\mathbb{R})$ de rang r, alors il existe un unique couple d'entiers (p, q) tel que $p + q = r$ et $P \in GL_n(\mathbb{R})$ tel que $P^T AP = \operatorname{diag}(I_p, -I_q, 0)$. Le couple (p, q) est appelé la signature de A.*

Proposition 34. *p (resp. q) est la dimension du plus grand sous-espace F pour lequel la restriction de A à F est définie positive (resp. définie négative).*

Théorème 35 (Spectral)**.** *Soit $A \in S_n(\mathbb{R})$, il existe $P \in O_n(\mathbb{R})$ tel que $P^{-1}AP$ est diagonale.*

Théorème 36 (Classification dans $\mathbb{F}_q$)**.** *Soit p un nombre premier impair et $q = p^n$ une puissance de p. On fixe $\delta \in \mathbb{F}_q^*$ qui n'est pas un carré. Alors, toute matrice symétrique inversible de $S_n(\mathbb{F}_q)$ est congruente à l'une des deux matrices :*

$$I_n \qquad ou \qquad \operatorname{diag}(1, ..., 1, \delta)$$

3 Les groupes de Lie classiques

Ici, $K = \mathbb{R}$ ou $\mathbb{C}$.

3.1 Éléments de topologie

Proposition 37. *$GL_n(K)$ est dense dans $M_n(K)$.*

Application 38 : Si $A, B \in M_n(K)$, $\chi_{AB} = \chi_{BA}$.

Proposition 39.
1. *$GL_n(\mathbb{C})$ est connexe (par arcs).*
2. *$GL_n(\mathbb{R})$ a deux composantes connexes (par arcs) homéomorphes : $GL_n^+(\mathbb{R}) = \{A \in GL_n(\mathbb{R}), \det(A) > 0\}$ et $GL_n^-(\mathbb{R}) = \{A \in GL_n(\mathbb{R}), \det(A) < 0\}$.*

Application 40 : L'ensemble des projecteurs de rang p est connexe (par arcs).

Lemme 41. *$O_n(\mathbb{R})$ est compact.*

Théorème 42 (Décomposition polaire)**.** *On a les homéomorphismes suivants donné par le produit matriciel*

$$O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \simeq GL_n(\mathbb{R}) \qquad et \qquad U_n(\mathbb{C}) \times H_n^{++}(\mathbb{C}) \simeq GL_n(\mathbb{C})$$

Remarque 43 : Par densité, on a encore une décomposition polaire pour $M_n(K)$, mais on n'a plus d'unicité de $O \in O_n(\mathbb{R})$ et $S \in S_n^{++}(\mathbb{R})$ tels que $M = OS$.

Application 44 : Soit $A, B \in M_n(\mathbb{R})$ telles qu'il existe $U \in U_n(\mathbb{C})$ tel que $B = UAU^*$, alors il existe $O \in O_n(\mathbb{R})$ tel que $B = OAO^T$.

Application 45 : On a un homéomorphisme

$$O_n(\mathbb{C}) \simeq O_n(\mathbb{R}) \times \mathbb{R}^{\frac{n(n-1)}{2}}$$

3.2 Sous-groupes de Lie

Théorème 46 (Admis)**.** *Soit G un sous-groupe de $GL_n(K)$ qui agit continûment et transitivement sur X localement compact, alors on a un homéomorphisme naturel*

$$G/G_x \simeq X$$

où $G_x = \{g \in G, g \cdot x = x\}$ est le stabilisateur de $x \in X$.

Application 47 :
- $SO(n)$ agit transitivement sur $\mathbb{S}^{n-1}$ ce qui donne un homéomorphisme
$$SO(n)/SO(n-1) \simeq \mathbb{S}^{n-1}$$
En particulier, $SO(n)$ est connexe.
- De même, on a un homéomorphisme
$$SU(n)/SU(n-1) \simeq \mathbb{S}^{2n-1}$$
En particulier, $SU(n)$ est connexe.

Théorème 48. *L'exponentielle réalise un difféomorphisme entre un voisinage de 0 dans $M_n(K)$ avec un voisinage de I_n dans $GL_n(K)$.*

Application 49 : $GL_n(K)$ n'a pas de sous-groupes arbitrairement petits : il existe V un voisinage de I_n dans $GL_n(K)$ tel que le seul sous-groupe de $GL_n(K)$ contenu dans V est trivial.

Lemme 50. *Soit $X, Y \in M_n(K)$, on a*

$$\lim_{n\to+\infty} \left[\exp\left(\frac{X}{n}\right)\exp\left(\frac{Y}{n}\right)\right]^n = \exp(X+Y)$$

et,

$$\lim_{n\to+\infty} \left[\exp\left(\frac{X}{n}\right)\exp\left(\frac{Y}{n}\right)\exp\left(-\frac{X}{n}\right)\exp\left(-\frac{Y}{n}\right)\right]^n = \exp\left([X,Y]\right)$$

Théorème-Définition 51. *Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$, on note*

$$\mathfrak{g} = \left\{X \in M_n(\mathbb{R}), \forall t \in \mathbb{R}, e^{tX} \in G\right\}$$

Alors, $\mathfrak{g}$ est un sous-espace vectoriel de $M_n(\mathbb{R})$ stable par $(X, Y) \longmapsto [X, Y]$.

DEVELOPPEMENT 1

Lemme 52. *Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$ non discret et connexe. Soit (h_n) une suite d'éléments de G tendant vers Id tel que $h_n \neq \mathrm{Id}$. Si h est une valeur d'adhérence de la suite* $\left(\frac{\mathrm{Log}(h_n)}{\|\mathrm{Log}(h_n)\|}\right)_n$, *alors $h \in \mathfrak{g}$.*

Théorème 53 (Cartan-Von Neumann). *Soit G un sous-groupe fermé de $GL_n(\mathbb{R})$, il existe un voisinage V de 0 dans $\mathfrak{g}$ et un voisinage W de I_n dans G tel que $\exp$ réalise un homéomorphisme entre V et W.*

Corollaire 54. *Tout sous-groupe fermé G de $GL_n(\mathbb{R})$ est une variété différentielle réelle et $\mathfrak{g}$ est le plan tangent de G en l'identité.*

Remarque 55 : En général, $\exp : \mathfrak{g} \longrightarrow G$ n'est pas surjective (par exemple $G = SL_2(\mathbb{R})$), mais $\exp(\mathfrak{g})$ engendre G.

Exemples 56 :

- $SL_n(\mathbb{R})$ est une sous-variété de dimension $n^2 - 1$ et $\mathfrak{sl}_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}), \mathrm{Tr}(X) = 0\}$.
- $SO_n(\mathbb{R})$ est une sous-variété de dimension $\frac{n(n-1)}{2}$ et $\mathfrak{so}_n(\mathbb{R}) = \left\{X \in M_n(\mathbb{R}), X^T + X = 0\right\}$.
- $SO_0(p,q)$ $(p+q=n)$ est une sous-variété de dimension $\frac{n(n-1)}{2}$ est $\mathfrak{so}(p,q) = \left\{X \in M_n(\mathbb{R}), X^T I_{p,q} + I_{p,q} X = 0, \mathrm{Tr}(X) = 0\right\}$.

3.3 Isomorphismes exceptionnels

DEVELOPPEMENT 1

Lemme 57. 1. *Soit $A \in GL_n(\mathbb{C})$ telle que $\forall H \in H_n(\mathbb{C}), AHA^* = H$, alors A est une homothétie.*

2. *Soit $M \in M_n(\mathbb{C})$ telle que $\forall H \in H_n(\mathbb{C}), MH + HM^* = 0$, alors $M = 0$.*

Théorème 58.

$$PSL_2(\mathbb{C}) \simeq SO_0(3,1)$$

Théorème 59 (Autres isomorphismes exceptionnels). 1. *En faisant agir $SL_2(\mathbb{C})$ sur $\mathfrak{sl}_2(\mathbb{C})$ par similitude, on trouve*

$$PSL_2(\mathbb{C}) \simeq SO_3(\mathbb{C})$$

2. *En faisant agir $SL_2(\mathbb{R})$ sur $\mathfrak{sl}_2(\mathbb{R})$ par similitude, on trouve*

$$PSL_2(\mathbb{R}) \simeq SO_0(2,1)$$

3. *En faisant agir $SU_2(\mathbb{C})$ sur $H_2(\mathbb{C}) \cap \mathfrak{sl}_2(\mathbb{C})$ par congruence hermitienne, on trouve*

$$PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$$

4. *En faisant agir $SU_2(\mathbb{C})^2$ sur l'algèbre des quaternions via $(h,k) \cdot u = huk^{-1}$, on trouve*

$$PSO(4) \simeq SO(3) \times SO(3)$$

Références :

- Caldero, Germoni, H2G2.
- Mneimé, Testard, Introduction à la théorie des groupes de Lie classiques.
- Perrin, Cours d'algèbre.
- Rombaldi, Algèbre et géométrie.