150 EXEMPLES D'ACTIONS DE GROUPES SUR LES ESPACES DE MATRICES.

Soit $\mathbb{K}$ un corps commutatif. Soient n, p des entiers non nuls.

I. Action par translations et pivot de Gauss [CG13, ChIV, p127]

I. A. Généralités

Définition 1. [Action par translation]
On définit les actions par translation/multiplication à gauche et à droite :

$$\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & PM \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathcal{GL}_p(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ (P, M) & \longmapsto & MP^{-1} \end{array}$$

Définition 2. [Matrices de dilatation, transvection, permutation élémentaire]
Une matrice de dilatation est une matrice $D_{i,\alpha} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\alpha \in \mathbb{K}^*$. Une matrice de transvection est une matrice $T_{i,j,\beta} = I_n + \beta E_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $\beta \in \mathbb{K}^*$ et $i \neq j$. Une matrice de permutation élémentaire est une matrice $P_{i,j} \in \mathcal{GL}_n(\mathbb{K})$ pour un $i < j$.

$$D_{i,\alpha} = \begin{pmatrix} I_{i-1} & & \\ & \alpha & \\ & & I_{n-i} \end{pmatrix} \qquad P_{i,j} = \begin{pmatrix} I_{i-1} & & & & \\ & 0 & & 1 & \\ & & I_{j-i-1} & & \\ & 1 & & 0 & \\ & & & & I_{n-j} \end{pmatrix}$$

Proposition 3. *Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$. Les opérations élémentaires sur les lignes (resp. colonnes) de M sont obtenues par multiplication à gauche (resp. à droite) par les matrices précédemment introduites :*

Matrice	$D_{i,\alpha}M$	$T_{i,j,\beta}M$	$P_{i,j}M$	$MD_{i,\alpha}$	$\dots$
Opération	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow \alpha L_j$	$C_i \leftarrow \alpha C_i$	$\dots$

I. B. Caractérisation des orbites et pivot de Gauss [CG13, ChI, p2]

Définition 4. On appelle :
- pivot d'une ligne son coefficient non nul le plus à gauche.
- matrice échelonnée en lignes une matrice telle que dès qu'une ligne est nulle, les suivantes sont nulles, et pour les lignes non nulles le pivot d'une ligne est strictement à droite du pivot de la ligne précédente. On dit qu'une matrice échelonnée est réduite si ses pivots valent 1.

On a la définition similaire de matrice échelonnée (resp. réduite) en colonnes.

Exemple 5. $\begin{pmatrix} 1 & 2 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ est réduite en lignes, $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 3 & 0 \\ 2 & 4 & 0 \end{pmatrix}$ est échelonnée en colonnes.

Théorème 6. [Orbites de l'action par multiplication à gauche]
Pour l'action par multiplication à gauche :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\ker(A) = \ker(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en lignes.*

Théorème 7. [Orbites de l'action par multiplication à droite]
Pour l'action par multiplication à droite :
- *deux matrices A et A' sont dans la même orbite si et seulement si $\mathrm{Im}(A) = \mathrm{Im}(A')$,*
- *toute matrice est dans l'orbite d'une unique matrice réduite en colonnes.*

Théorème 8. *$\mathcal{SL}_n(\mathbb{K})$ est engendré par les transvections, $\mathcal{GL}_n(\mathbb{K})$ est engendré par les transvections et les dilatations.*

Application 9. [Algorithme du pivot de Gauss]
L'algorithme du pivot de Gauss permet de se ramener à la matrice réduite associée à une matrice via des opérations élémentaires sur les lignes.

Exemple 10. $\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{pmatrix}$ a pour matrice réduite associée $\begin{pmatrix} 1 & 2 & 1/2 \\ 0 & 1 & -1/2 \\ 0 & 0 & 1 \end{pmatrix}$.

I. C. Application à la décomposition polaire
[CG13, ChVI, p201] [Rom17, Ch22, p697]

On se place sur $\mathbb{K} = \mathbb{R}$, $n = p$ et on considère l'action à gauche restreinte à $\mathcal{O}_n(\mathbb{R})$.

Théorème 11. [Décomposition polaire]
L'application $\mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) \longrightarrow \mathcal{GL}_n(\mathbb{R}), (O, S) \longmapsto OS$ est un homéomorphisme.

Théorème 12. *L'orbite de toute matrice M contient une matrice symétrique positive. Si M est inversible, l'orbite contient une matrice symétrique définie positive.*

Application 13. $\mathcal{O}_n(\mathbb{R})$ est le seul sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ contenant $\mathcal{O}_n(\mathbb{R})$.

Application 14. Pour $A \in \mathcal{M}_n(\mathbb{R})$, on a $\|A\|_2 = \sqrt{\rho(A^\top A)}$.

II. Action de Steinitz

[CG13, CHI, p2]

Définition 15. [Action de Steinitz]
On appelle action de Steinitz l'action $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{GL}_p(\mathbb{K}) \times \mathcal{M}_{n,p}(\mathbb{K}) & \longrightarrow & \mathcal{M}_{n,p}(\mathbb{K}) \\ ((P,Q),M) & \longmapsto & PMQ^{-1} \end{array}$.
Les orbites pour cette action sont appelées classes d'équivalence.

Théorème 16. *Si M est de rang r, M est équivalente à $J_r = \begin{pmatrix} I_r & \\ & 0_{n-r,p-r} \end{pmatrix}$.*

Remarque 17. L'algorithme du pivot total permet d'obtenir J_r.

Corollaire 18. *Deux matrices sont équivalentes si et seulement si elles ont même rang. Ainsi $\mathcal{O} = \{O_r \mid 0 \leq r \leq \min(m,n)\}$ où $O_r = \{M \in \mathcal{M}_{n,p}(\mathbb{K}) \mid \mathrm{rg}(M) = r\}$.*

Exemple 19. $\begin{pmatrix} 2 & 4 & 1 \\ 1 & 3 & 0 \\ 0 & 5 & 2 \end{pmatrix}$ est équivalente à I_3.

Corollaire 20. $\mathrm{rg}(M^\top) = \mathrm{rg}(M)$.

Proposition 21. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. Alors $\overline{O_r} = \bigsqcup_{0 \leq k \leq r} O_k$.*

Corollaire 22. *Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. L'unique orbite fermée est $O_0 = \{0\}$ et l'unique orbite ouverte est $O_{\min(n,p)}$. Si $n = p$, $O_n = \mathcal{GL}_n(\mathbb{K})$ est un ouvert dense de $\mathcal{M}_n(\mathbb{K})$.*

III. Action par conjugaison

[CG13, ChIII, p83]

III. A. Généralités

Définition 23. [Action par conjugaison]
On considère l'action par conjugaison $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K}) \\ (P,M) & \longmapsto & PMP^{-1} \end{array}$.
Deux matrices d'une même orbite sont dites semblables.

Remarque 24. On considère un $\mathbb{K}$-espace vectoriel E de dimension finie n, et $u \in \mathcal{L}(E)$. Soient $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, P la matrice de passage de $\mathcal{B}$ vers $\mathcal{B}'$. Alors si $A = M_{\mathcal{B}}(u)$ et $A' = M_{\mathcal{B}'}(u)$, on a $A' = PAP^{-1}$.

Proposition 25. *Deux matrices semblables ont même rang, déterminant, trace, valeurs propres, polynôme minimal, polynôme caractéristique.*

Remarque 26. Dans aucun des cas il ne s'agit d'une caractérisation. Par exemple pour le polynôme minimal considérer $\mathrm{diag}(1,1,2)$ et $\mathrm{diag}(1,2,2)$ et pour le polynôme caractéristique, considérer I_2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

III. B. Applications à la trigonalisabilité/diagonalisabilité

[MM16]

Définition 27. Une matrice est trigonalisable (resp. diagonalisable) si elle est dans l'orbite d'une matrice triangulaire (resp. diagonale).

Théorème 28. *Une matrice est trigonalisable (resp. diagonalisable) si et seulement si son polynôme minimal est scindé (resp. scindé à racines simples).*

Proposition 29. *Dans $\mathbb{K} = \mathbb{C}$, $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si sa classe de similitude est fermée dans $\mathcal{M}_n(\mathbb{K})$.*

Application 30. [Cardinal de $\mathcal{D}_n(\mathbb{F}_q)$] [Rom17, §5.6, p148–151]
Soit $n \in \mathbb{N}$, $q = p^r$ où p premier, $r \neq 0$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{n_1+\cdots+n_q=n} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

III. C. Action de $\mathcal{O}_n(\mathbb{R})$ et de $\mathcal{U}_n(\mathbb{C})$

[CG13, ChV, p149] [Rom17, Ch22]

Si $\mathbb{K} = \mathbb{R}$ (resp. $\mathbb{C}$), restreignons l'action par conjugaison à $\mathcal{O}_n(\mathbb{R})$ (resp. $\mathcal{U}_n(\mathbb{C})$).

Remarque 31. Avec le contexte de la remarque précédente, l'action de $\mathcal{O}_n(\mathbb{R})$ (resp. $\mathcal{U}_n(\mathbb{C})$) équivaut à un changement de base orthonormée pour E euclidien (resp. hermitien).

Fixons donc un endormorphisme $u \in \mathcal{L}(E)$ euclidien. On suppose u normal, c'est-à-dire que sa matrice M dans une base orthonormée fixée vérifie :

Définition 32. $M \in \mathcal{M}_n(\mathbb{K})$ est dite normale si $M^*M = MM^*$ où $M^* = \overline{M^\top}$.

Proposition 33. *Les valeurs propres (complexes) de M normale sont des racines de l'unité.*

Lemme 34.
- *Si F est un sous-espace vectoriel stable par u, alors $F^\perp$ est stable par u,*
- *Il existe un sous-espace vectoriel stable par u de dimension 1 ou 2.*

Théorème 35. [Réduction des endomorphismes normaux]
Il existe une base orthonormée $\mathcal{B}$ de E telle que

$$M_{\mathcal{B}}(u) = \begin{pmatrix} \mathrm{diag}(\lambda_1, \dots, \lambda_p) & & & \\ & R_1 & & \\ & & \ddots & \\ & & & R_r \end{pmatrix}$$

où $p + 2r = n$, $(\lambda_i)_{1 \leq i \leq p} \in \mathbb{R}^p$ et pour $1 \leq k \leq r$, $R_k = \begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ avec $b_k \neq 0$.

Application 36. [Réduction d'un endomorphisme antisymétrique]
Supposons u antisymétrique. Alors il existe une base orthonormée $\mathcal{B}$ de E telle que $M_{\mathcal{B}}(u)$ est de la forme précédente, avec $\lambda_1 = \cdots = \lambda_p = 0$, $2r \leq n$ et $R_k = \begin{pmatrix} 0 & -b_k \\ b_k & 0 \end{pmatrix}$.

IV. Action par congruence

[Rom17, Ch15, p463]

IV. A. Généralités

On suppose dans cette section que $\mathrm{car}(\mathbb{K}) \neq 2$.

Définition 37. [Action par congruence]
On appelle action par congruence l'action sur $\mathcal{S}_n(\mathbb{K})$: $\begin{array}{ccc} \mathcal{GL}_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) & \longrightarrow & \mathcal{S}_n(\mathbb{K}) \\ (P, S) & \longmapsto & PSP^\top \end{array}$.
Deux matrices d'une même orbite sont dites congruentes.

Remarque 38. On considère un $\mathbb{K}$-espace vectoriel E de dimension finie n, q une forme bilinéaire symétrique sur E, $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, P la matrice de passage de $\mathcal{B}$ vers $\mathcal{B}'$. Alors si $S = M_{\mathcal{B}}(q) \in \mathcal{S}_n(\mathbb{K})$ et $S' = M_{\mathcal{B}'}(q) \in \mathcal{S}_n(\mathbb{K})$, on a $S' = PSP^\top$.

Définition 39. [Discriminant]
On définit le discriminant de $S \in \mathcal{S}_n(\mathbb{K})$ par $\overline{\det(S)} \in \mathbb{K}^*/(\mathbb{K}^*)^2$ si S est inversible, 0 sinon.

Proposition 40. *Deux matrices congruentes ont même discriminant.*

IV. B. Classification des formes quadratiques

[CG13, ChV.B, p179]

Théorème 41. [Classification sur $\mathbb{K} = \mathbb{C}$]
Soit $S \in \mathcal{S}(\mathbb{C})$. Alors S est congruente à J_r où $r = \mathrm{rg}(S)$.
Deux matrices de $\mathcal{S}_n(\mathbb{C})$ sont congruentes si et seulement si elles ont même rang.

Théorème 42. [Classification sur $\mathbb{K} = \mathbb{R}$]
Soit $S \in \mathcal{S}(\mathbb{R})$. Il existe $(s,t) \in \mathbb{N}^2$ tels que S soit congruente à $\begin{pmatrix} I_s & & \\ & -I_t & \\ & & 0_{n-s-t} \end{pmatrix}$.

Proposition 43. *On a $s = \max(\{\dim(F) \mid F$ sev de E sur lequel q est définie positive$\})$ et $t = \max(\{\dim(F) \mid F$ sev de E sur lequel q est définie négative$\})$.*

Corollaire 44. *Deux matrices de $\mathcal{S}_n(\mathbb{R})$ sont congruentes si et seulement si elles ont même signature.*

On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 45. *$\mathbb{F}_p^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^*$.*

Application 46. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

Théorème 47. [Classification sur $\mathbb{K} = \mathbb{F}_q$]
Soit $\alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$. Alors toute matrice $S \in \mathcal{S}_n(\mathbb{F}_q)$ est congruente à $\begin{pmatrix} I_{r-1} & & \\ & \delta & \\ & & 0_{n-r} \end{pmatrix}$ où $\delta \in \{1, \alpha\}$ et $r = \mathrm{rg}(S)$.

Application 48. [Loi de réciprocité quadratique]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Exemple 49. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

SPEECH

Les matrices sont des objets mathématiques assez anciens, dont la structure a été formalisée par son lien avec l'algèbre linéaire (opérations sur les lignes et colonnes, endomorphismes, formes quadratiques). Les actions de groupes permettent de synthétiser tout cela.
Dans un premier temps, on regarde les multiplications de matrices qui nous mènent au pivot de GAUSS et aux décompositions LU et polaire.
Ensuite on étudie l'action de STEINITZ et la caractérisation des orbites par le rang.
Enfin la troisième partie s'intéresse à l'action par conjugaison, qui correspond à la notion de matrices représentant un même endomorphisme et donne un grand nombre d'invariants par similitude. On applique cela à la diagonalisabilité et à la réduction de FROBENIUS.
Enfin on parle de l'action par congruence qui correspond à la relation de représentation d'une même forme quadratique. Sur $\mathbb{C}$ on a une caractérisation simple des orbites, sur $\mathbb{R}$ on utilise la signature. Enfin on donne la classification sur $\mathbb{F}_q$ avec application à la loi de réciprocité quadratique.

QUESTIONS

Q Montrer le premier point du Théorème 15.

R Voir [CG13, §IV.2, p131].

Q Soit $S \in \mathcal{S}_n(\mathbb{C})$ telle que $\det(S+X) = \det(X)$ pour tout $X \in \mathcal{S}_n(\mathbb{C})$. Que dire de S ?

R On a $0 = \det(S-S) = \det(-S) = (-1)^n \det(S)$ dons S est non inversible.
Pour tout $P \in \mathcal{GL}_n(\mathbb{C})$, on a $\det(PSP^\top + PXP^\top) = \det(P)^2 \det(S+X) = \det(P)^2 \det(X) = \det(PXP^\top)$. On peut donc remplacer S par sa forme réduite. Quand X décrit $\mathcal{S}_n(\mathbb{C})$, $PXP^\top$ décrit $\mathcal{S}_n(\mathbb{C})$ donc le problème se réécrit : $\det(S'+X') = \det(X')$ pour $X' \in \mathcal{S}_n(\mathbb{C})$, où $S' = J_r$. Prenant alors $X' = \mathrm{Id}$, on obtient $\det(S'+X') = \det(X')$, ce qui n'est possible que si $\mathrm{rg}(S') = 0$, c'est-à-dire $S' = 0$, ou encore $S = 0$.

BIBLIOGRAPHIE

[CG13] P. CALDERO et J. GERMONI : *Histoires hédonistes de groupes et de géométries - Tome 1*. Calvage et Mounet, 2013.

[MM16] R. MANSUY et R. MNEIMNÉ : *Algèbre linéaire : Réduction des endomorphismes*. De Boeck, 2 ème édition, 2016.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.