101 : Groupe opérant sur un ensemble. Exemples et applications

Pandou

2 mai 2022

1 Définitions et propriétés

1.1 Vocabulaire des actions

Définition 1. *Une action de G sur un ensemble X est une application $G \times X \longrightarrow X$ telle que*

1. $\forall g, h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.
2. $\forall x \in X, 1 \cdot x = x$.

Proposition 2. *Toute action définit un morphisme de groupes $G \longrightarrow \mathfrak{S}(X)$. Réciproquement, tout morphisme $G \longrightarrow \mathfrak{S}(X)$ définit une action.*

Définition 3. *On définit une relation d'équivalence sur X en posant*

$$x \sim y \Longleftrightarrow \exists g \in G, y = g \cdot x$$

La classe d'équivalence de x, notée $G \cdot x$ est appelée une orbite.

Remarque 4 : En particulier, les orbites sous l'action de G forment une partition de X.

Définition 5. *Le stabilisateur de $x \in X$ est le sous-groupe de G défini par $G_x = \{g \in G, g \cdot x = x\}$.*

Définition 6. *On dit qu'une action est :*

- *transitive s'il n'y a qu'une seule orbite.*
- *p-transitive si pour tout $(y_1, ..., y_p), (x_1, ..., x_p) \in X$ tous distincts, il existe $g \in G$ tel que $y_i = g \cdot x_i$.*
- *fidèle si le morphisme $\rho : G \longrightarrow \mathfrak{S}(X)$ est injectif.*
- *libre si tout élément différent du neutre agit sans point fixe.*
- *librement transitive si elle est transitive et libre : $\forall x, y \in X, \exists g \in G, y = g \cdot x$.*

Exemples 7 :

- L'action naturelle de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est n-fois transitive.
- L'action de $\mathrm{Diff}(\mathbb{R})$ sur $\mathbb{R}$ n'est pas 3-transitive.
- L'action de $GL_n(\mathbb{R})$ sur l'ensemble des droites vectorielles de $\mathbb{R}^n$ n'est pas fidèle, mais l'action de $PGL_n(\mathbb{R})$ l'est.
- Si $\vec{E}$ est un espace affine, l'action de E sur $\vec{E}$ est librement transitive.

Proposition 8. *Si $\rho : G \longrightarrow \mathfrak{S}(X)$ définit une action de groupe, alors $\widetilde{\rho} : G/\mathrm{Ker}(\rho) \longrightarrow \mathfrak{S}(X)$ définit une action appelée fidélisation de ρ.*

1.2 Combinatoire

On suppose ici que G et X sont finis.

Proposition 9. *On suppose que G est fini, alors on a une bijection naturelle entre G/G_x et $G \cdot x$.*

Remarque 10 : En particulier, cette proposition donne des informations combinatoires quand l'action est transitive. Par exemple, $GL_n(\mathbb{F}_q)$ agit transitivement sur $\mathbb{F}_q^n \setminus \{0\}$, avec par exemple $x = e_1$, on trouve :

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

Corollaire 11. *Soit $\mathcal{X}$ un système de représentant des orbites de l'action de G, alors*

$$\mathrm{Card}(X) = \sum_{x \in \mathcal{X}} \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)}$$

Application 12 : Il existe une famille finie de sous-groupes stricts de G telle que

$$\mathrm{Card}(G) = \mathrm{Card}\big(Z(G)\big) + \sum_{i \in I} \frac{\mathrm{Card}(G)}{\mathrm{Card}(H_i)}$$

Proposition 13 (Formule de Burnside)**.** *Le nombre d'orbites k se calcule via*

$$k = \frac{1}{|G|} \sum_{g \in G} \mathrm{Card}\big(\mathrm{Fix}(g)\big)$$

avec $\mathrm{Fix}(g) = \{x \in X, g \cdot x = x\}$.

Théorème 14 (Cauchy)**.** *Soit G un groupe fini et p premier qui divise l'ordre de G, alors G admet un élément d'ordre p.*

2 Actions sur un groupe et groupe symétrique

2.1 Translation à gauche

Proposition 15. *L'action de G sur lui-même par translation à gauche, ie $g \cdot h = gh$ est librement transitive.*

Corollaire 16 (Théorème de Cayley)**.** *Si G est un groupe d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Application 17 : Tout groupe d'ordre n se plonge dans un $GL_n(K)$.

Définition 18. *Soit H un sous-groupe de G, G agit sur G/H par translation à gauche.*
- *Le stabilisateur de xH est xHx^{-1}.*
- *Le noyau de l'action est $\bigcap_{x \in G} xHx^{-1}$.*

Proposition 19. *Si G est infini et H un sous-groupe propre de G d'indice fini, alors G n'est pas simple.*

2.2 Conjugaison sur G

Définition 20. *Pour l'action de G sur lui-même par conjugaison, ie $g \cdot h = ghg^{-1}$.*
- *Une orbite pour cette action est appelée classe de conjugaison.*
- *Le stabilisateur de g est appelé commutant de g, ou centralisateur.*
- *Le noyau du morphisme $G \longrightarrow \mathfrak{S}(G)$ est appelé centre de G, noté $Z(G)$.*

Proposition 21. *Soit $\sigma \in \mathfrak{S}_n$ et $\begin{pmatrix} a_1 & \dots & a_p \end{pmatrix}$ un p-cycle, alors*

$$\sigma \begin{pmatrix} a_1 & \dots & a_p \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_p) \end{pmatrix}$$

Corollaire 22. *Deux permutations sont conjugués dans $\mathfrak{S}_n$ si, et seulement si, ils ont le même nombre de cycles de même longueur.*

DEVELOPPEMENT 1

Lemme 23. *Si $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$ transforme une transposition en une transposition, alors φ est intérieur.*

Théorème 24. *Si $n \neq 6$, tous les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs.*

Remarque 25 : Pour $n = 6$, $\mathfrak{S}_6$ admet un sous-groupe d'indice 6 qui agit transitivement sur $[\![1, 6]\!]$, donc il existe un automorphisme qui n'est pas intérieur.

2.3 p-groupes

Définition 26. *Un p-groupe est un groupe dont l'ordre est une puissance de p.*

Proposition 27. *Soit G un p-groupe agissant sur un ensemble fini X, on note $X^G = \{x \in X, \forall g \in G, g \cdot x = x\}$, alors*

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) \mod (p)$$

Corollaire 28. *Le centre d'un p-groupe n'est jamais trivial.*

Application 29 : Un groupe d'ordre p^2 est abélien.

2.4 Conjugaison sur $\mathcal{P}(G)$

Définition 30. *G agit sur $\mathcal{P}(G)$ par conjugaison via $g \cdot S = gSg^{-1}$.*
- *Une orbite pour cette action est appelée classe de conjugaison.*
- *Le stabilisateur de S pour cette action est appelée normalisateur de S dans G.*

Définition 31. *Soit G un groupe d'ordre $n = p^\alpha m$ avec $p \wedge m = 1$. Un p-Sylow de G est un sous-groupe de cardinal p^α.*

Exemple 32 : Le groupe des matrices unitriangulaires supérieures de $GL_n(\mathbb{F}_p)$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 33. *Soit G un groupe, H un sous-groupe de G et S un p-Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

Théorème 34 (Sylow)**.** *Soit G un groupe d'ordre $n = p^\alpha m$, $p \wedge m = 1$. Alors,*
1. *G admet un p-Sylow.*
2. *Les p-Sylow sont conjugués.*
3. *Si n_p est le nombre de p-Sylow, alors $n_p = 1 \mod (p)$ et n_p divise m.*

Application 35 : Un groupe d'ordre 63 n'est pas simple.

3 Algèbre (bi)linéaire

3.1 Translation et équivalence

Définition 36. *$GL_m(K)$ agit sur $M_{m,n}(K)$ via $P \cdot M = PM$. De même, $GL_n(K)$ agit sur $M_{m,n}(K)$ via $Q \cdot M = MQ^{-1}$.*

Théorème 37. *Deux matrices sont dans la même orbite pour l'action de $GL_m(K)$ si, et seulement si, elles ont même noyau. Deux matrices sont dans la même orbite pour l'action de $GL_n(K)$ si, et seulement si, elles ont même image.*

Définition 38. *$GL_m(K) \times GL_n(K)$ agit sur $M_{m,n}(K)$ via $(P, Q) \cdot M = PMQ^{-1}$. Deux matrices dans la même orbite sont dites équivalentes.*

Théorème 39. *Deux matrices sont équivalentes si, et seulement si, elles ont même rang.*

3.2 Similtiude

Définition 40. *$GL_n(K)$ agit sur $M_n(K)$ via $P\cdot M = PMP^{-1}$. Deux matrices dans la même orbites sont dites semblables.*
Une matrice semblable à une matrice diagonale (resp. triangulaire) est dite diagonalisable (resp. trigonalisable).

Proposition 41. *Deux matrices semblables ont même trace, même rang, même déterminant, même polynôme caractéristique et même polynôme minimal.*

Remarque 42 : Ces invariants ne sont pas totaux : $\begin{pmatrix}0&1&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&0\end{pmatrix}$ et $\begin{pmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$ ne sont pas semblables mais ont même trace, rang, déterminant, polynôme caractéristique et polynôme minimal.

Proposition 43. *Une matrice est trigonalisable si, et seulement si, son polynôme caractéristique est scindé.*

Corollaire 44. *Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.*

Théorème 45 (Lemme des noyaux)**.** *Soit $M\in M_n(K)$ et $P=P_1...P_k\in K[X]$ avec P_i premiers entre eux deux à deux. Alors,*

$$\mathrm{Ker}\big(P(M)\big)=\bigoplus_{i=1}^{k}\mathrm{Ker}\big(P_i(M)\big)$$

Corollaire 46. *Une matrice est diagonalisable si, et seulement si, elle est annulée par un polynôme scindé à racines simples.*

Corollaire 47. *Soit $A\in M_n(K)$ telle que χ_A est scindé sur $K[X]$. Alors, il existe un unique couple (D,N) tel que*

1. *$A=D+N$.*
2. *$[D,N]=0$.*
3. *D est diagonalisable et N nilpotente.*

Application 48 : Calcul d'exponentielles de matrices.

Théorème 49 (Réduction de Jordan)**.** *Soit $A\in M_n(\mathbb{C})$ une matrice nilpotente. Alors, il existe une unique partition $n_1\geqslant ...\geqslant n_p$ de n telle que A est semblable à* $\mathrm{diag}(J_{n_1},...,J_{n_p})$ *où $J_p=\begin{pmatrix}0&1&\dots&0\\0&\ddots&\ddots&\\&\ddots&\ddots&1\\0&&0&0\end{pmatrix}\in M_p(\mathbb{C})$.*

Corollaire 50 (Réduction de Jordan v2)**.** *On note $J_n(\lambda)=\begin{pmatrix}\lambda&1&\dots&0\\0&\ddots&\ddots&\\&\ddots&\ddots&1\\0&&0&\lambda\end{pmatrix}$. Si $A\in M_n(\mathbb{C})$ de spectre $\{\lambda_1,...,\lambda_k\}$, alors A est semblable à* $\mathrm{diag}(J_{n_1}(\lambda_1),...,J_{n_k}(\lambda_k))$.

3.3 Congruence

Définition 51. *$GL_n(K)$ agit sur $S_n(K)$ via $P\cdot S=PSP^T$. Deux matrices dans la même orbite sont dites congruentes.*

Proposition 52. *Toute matrice symétrique est congruente à une matrice diagonale.*

Remarque 53 : On appelle une telle matrice diagonale grâce à l'algorithme de Gauss.

Théorème 54 (Classification dans $\mathbb{C}$)**.** *Deux matrices de $S_n(\mathbb{C})$ sont congruentes si, et seulement si, elles ont même rang.*

Théorème 55 (Classification dans $\mathbb{R}$)**.** *Toute matrice symétrique réelle est congruente à une unique matrice de la forme* $\mathrm{diag}(I_p,-I_q,0)$*. Le couple (p,q) est appelée signature.*
Deux matrices symétriques réelles sont congruentes si, et seulement si, elles ont même signature.

Théorème 56 (Classification dans $\mathbb{F}_q$)**.** *Soit ζ un élément non carré de $\mathbb{F}_q$, alors toute matrice symétrique inversible sur $\mathbb{F}_q^n$ est congruente soit à I_n, soit à* $\mathrm{diag}(I_{n-1},\zeta)$.

4 Applications en géométrie

Dans cette partie, G est un sous-groupe de $GL_n(\mathbb{C})$.

4.1 Action continue et théorème d'homéomorphisme

Définition 57. *Soit G un groupe matriciel et X un espace topologique, on dit que l'action de G sur X est continue si $G\times X\longrightarrow X$ est une application continue.*

Proposition 58. *L'adhérence d'une orbite de G est une réunion d'orbites de G.*

Théorème 59. *Si G agit continûment et transitivement sur X, alors on a un homéomorphisme $G/G_x\simeq G\cdot x$.*

Application 60 : $SO(n)/SO(n-1)\simeq\mathbb{S}^{n-1}$ et $SU(n)/SU(n-1)\simeq\mathbb{S}^{2n-1}$.

4.2 Un isomorphisme quaternionique

Définition 61. *On note $\mathbb{H}$ la $\mathbb{R}$-algèbre de dimension 4 engendrée par $(1, i, j, k)$ telle que*

$$i^2 = j^2 = k^2 = ijk = -1$$

On note $\mathbb{R} = \mathrm{Vect}(1)$ et $\mathbb{I} = \mathrm{Vect}(i, j, k)$.

Proposition 62. *On note $\langle h_1, h_2\rangle = \frac{1}{2}\big(h_1\overline{h_2} + h_2\overline{h_1}\big)$ et $N(h) = \langle h, h\rangle$, ce qui munit $\mathbb{H}$ d'une structure d'espace euclidien.*

Théorème 63. *$\mathbb{H}$ est un corps non commutatif, dont le centre est $\mathbb{R}$. De plus, $N(hh') = N(h)N(h')$.*

Proposition 64. *On a les homéomorphismes suivants*

$$\{h \in \mathbb{H}, N(h) = 1\} \simeq \mathbb{S}^3 \simeq SU(2)$$

Lemme 65 (Admis)**.** *Les retournements engendrent $SO(3)$.*

DEVELOPPEMENT 2

Théorème 66.

$$PSU(2) \simeq SO(3) \qquad et \qquad SO(3) \times SO(3) \simeq PSO(4)$$

Remarque 67 : On observe que $PSO(4)$ n'est pas simple : c'est un cas exceptionnel !

4.3 Actions d'algèbres de Lie

Définition 68. *Un groupe de Lie matriciel est un sous-groupe de $GL_n(\mathbb{R})$ muni d'une structure de variété différentiable, on note $\mathfrak{g}$ le plan tangent en l'identité : c'est l'algèbre de Lie associée à G.*

Théorème 69. *Soit G un groupe de Lie matriciel.*

1. *L'application exponentielle envoie $\mathfrak{g}$ dans G et induit un $\mathcal{C}^\infty$-difféomorphisme entre un voisinage de 0 de $\mathfrak{g}$ et un voisinage de I_n dans G.*
2. *$\mathfrak{g}$ est stable par crochet de Lie : $[X, Y] = XY - YX$.*
3. *Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes de Lie matriciels, alors $T\varphi : \mathfrak{g} \longrightarrow \mathfrak{g}'$ est un morphisme d'algèbre de Lie (ie préserve le crochet des matrices) et de plus*

$$\forall X \in \mathfrak{g}, \varphi(e^X) = \exp\big(T\varphi(X)\big)$$

Définition 70. *Si (ρ, V) est une représentation de G, alors on définit un morphisme d'algèbres de Lie $T\rho : \mathfrak{g} \longrightarrow \mathfrak{gl}(V)$, appelée représentation d'algèbres de Lie sur V.*

Proposition 71.

$$\forall X \in \mathfrak{g}, T\rho(X) = \frac{\mathrm{d}}{\mathrm{d}t}\rho\big(e^{tX}\big)_{|t=0}$$

Remarque 72 : L'étude des représentations d'algèbres de Lie donne un point de vue purement algébrique sur la théorie des représentations des groupes de Lie.

Références :

- Arnaudiès, Fraysse, Cours de mathématiques - Algèbre.
- Calais, Éléments de théorie des groupes.
- Caldero, Germoni, H2G2.
- Mneimé, Testard, Introduction à la théorie des groupes de Lie classique.
- Mneimé, Éléments de géométrie, actions de groupes.
- Perrin, Cours d'algèbre.