Groupe opérant sur un ensemble. Exemples et applications.

101

Cadre : G un groupe, X un ensemble

I] Actions et formule des classes

1. Actions de groupes

Déf. 1 : G opère à gauche sur X s'il existe une application $G\times X \to X$, $(g,x)\mapsto g\cdot x$ telle que
- $g\cdot(h\cdot x) = (gh)\cdot x$ pour tous $g,h\in G$ et $x\in X$;
- $e\cdot x = x$ pour tout $x\in X$.

Rem. 2 : On définit de même une action à droite.

Ex. 3 :
- L'action triviale de G sur X : $g\cdot x = x$.
- Les isométries du plan affine opèrent sur le plan affine.
- S_X opère sur X par $\sigma\cdot x = \sigma(x)$.

Th.Déf. 4 : À une action G sur X correspond le morphisme structurel $\varphi : G \to S_X$, $g\mapsto \sigma_g$ avec $\sigma_g(x) = g\cdot x$.

Ex. 5 : L'action triviale correspond au morphisme trivial $g\mapsto e$.

Déf. 6 : Une action de groupes est dite fidèle si le morphisme structurel associé est injectif.

2. Orbite et stabilisateur

Déf. 7 : On appelle stabilisateur de x l'ensemble $G_x := \{g\in G / g\cdot x = x\}$. L'action est dite libre si $G_x = \{e\}$ pour tout $x\in X$.

Ex. 8 : Dans l'opération de S_n sur $X = \{1,\dots,n\}$, $G_x \simeq S_{n-1}$.

Prop. 9 : Soit $\varphi : G\to S_X$ une action de G sur X. Le noyau de φ est alors $\ker\varphi = \bigcap_{x\in X} G_x$.

Déf. 10 : On appelle orbite de x le sous-ensemble $\Omega_x := \{g\cdot x / g\in G\}$. L'action est dite transitive s'il existe exactement une orbite dans X.

Rem. 11 : Une action est transitive sur chaque orbite.

Prop. 12 : Soit G opérant sur X. La relation $\sim$ définie sur X par $x\sim y \iff x\in\Omega_y$ (ie $\exists g\in G / x = g\cdot y$) est une relation d'équivalence, dont les classes d'équivalence sont les orbites.

Les orbites forment une partition de X. On a alors $|X| = \sum_{i=1}^{r} |\Omega_{x_i}|$.

Th. 13 : Soit G opérant sur X. Alors, pour tous $x,y\in X$, on a $x\sim y \Rightarrow G_x$ et G_y sont conjugués dans $\mathcal{P}(G)$ (les parties de G).

Déf. 14 : Le sous-ensemble des points fixes de X par l'action de G sur X est $X^G := \{x\in X / g\cdot x = x$ pour tout $g\in G\}$.

Rem. 15 :
- $X^G = \{x\in X / G_x = G\} = \{x\in X / \Omega_x = \{x\}\}$.
- Si l'action est transitive, $X^G = \emptyset$.

Ex. 16 : Soit $G\leq S_4$ opérant sur $X = \{1,2,3,4\}$. Alors :
- Si $G = \langle(123)\rangle$, $X^G = \{4\}$.
- Si $G = \langle(12)(34)\rangle$, $X^G = \emptyset$.

3. Formule des classes et conséquences

Th. 17 : Soit G opérant sur X. Pour tout $x\in X$, on a $|\Omega_x| = [G : G_x]$.

Prop. 18 : Un groupe à n éléments ayant 2 classes de conjugaison est d'ordre 2.

Th. 19 : (Formule des classes.) On suppose G et X finis. Soit G opérant sur X. Si $X = \bigsqcup_{i=1}^{r} \Omega_{x_i}$ est la partition de X en orbites, alors
$$|X| = \sum_{i=1}^{r} |\Omega_{x_i}| = \sum_{i=1}^{r} [G : G_{x_i}] = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$$

Cor. 20 : (Formule de Burnside.) Soient $g\in G$, X^g l'ensemble des points fixes de X sous l'action de $\langle g\rangle$. Alors le nombre r des orbites de X sous l'action de G est $r = \frac{1}{|G|}\sum_{g\in G} |X^g|$.

App. 21 : Si G est un sous-groupe fini non trivial de $SO_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$, alors $G \simeq \mathbb{Z}/m\mathbb{Z}$, D_m, A_4, S_4 ou A_5 (pour $m\geq 2$).

App. 22 : Si on dispose de 4 perles magenta, 3 perles cyan et 2 perles kaki, alors on peut faire 76 colliers différents.

4. p-groupes

Déf. 23 : Soit p premier. Un p-groupe est un groupe dont l'ordre de tout élément est une puissance de p.

Ex. 24 :
- $G = \{e\}$ p-groupe $\forall p$ premier.
- D_4 est un 2-groupe fini.

Prop. 25 : Soit G un p-groupe agissant sur X. Alors $|X| \equiv |X^G|$ $[p]$.

App. 26 : (Théorème de Cauchy.) Si G fini avec $p \mid |G|$, alors il existe au moins un élément $g \in G$ d'ordre p.

Csq. 27 : Un p-groupe fini est un groupe fini dont l'ordre est une puissance de p.

Prop. 28 : Soit G un p-groupe fini. Alors $Z(G) \neq \{e\}$.

II] Actions classiques et théorie des groupes

1. Action par translation

Déf. 29 : Un groupe G agit sur lui-même par translation à gauche : $G \times G \to G$, $(g,h) \mapsto g \cdot h = gh$.

Prop. 30 : $G_g = \{e\}$; l'action est fidèle, libre et transitive.

App. 31 : (Théorème de Cayley.) Tout groupe fini d'ordre n est isomorphe à un sous-groupe transitif de S_n.

Ex. 32 : Pour tout $H \leq G$, G opère transitivement à gauche sur G/H.

Ex. 33 : G opère sur $\mathcal{P}(G)$ (l'ensemble des parties de G) par translation.

2. Action par conjugaison

Déf. 34 : Un groupe G opère sur lui-même par conjugaison (ou par automorphisme intérieur) : $G \times G \to G$, $(g,h) \mapsto g \cdot h = ghg^{-1}$.

Déf. 35 : Dans ce cas, les orbites s'appellent les classes de conjugaison et le stabilisateur s'appelle le centralisateur, noté Z_G.

Prop. 36 : $Z_G(e) = G$ donc l'action n'est jamais libre. De plus, elle n'est ni fidèle, ni transitive si $G \neq \{e\}$.

Prop. 37 : $g \in Z_G \iff$ sa classe de conjugaison est $\{g\}$.

Déf. 38 : Deux sous-groupes de G sont conjugués s'ils appartiennent à la même orbite de l'action de G sur l'ensemble de ses sg par conjugaison.

Déf. 39 : Le stabilisateur d'un sg de G s'appelle le normalisateur pour cette action.

Prop. 40 : $H \triangleleft G \iff H$ est un point fixe de G pour cette action.

Prop. 41 : $G^G = Z(G)$ pour l'action de conjugaison.

Déf. 42 : Les classes de conjugaison pour les ensembles de matrices s'appellent les classes de similitude.

Ex. 43 : $GL_n(\mathbb{C})$ agit sur l'ensemble des matrices diagonalisables sur $\mathbb{C}$ par conjugaison. La classe de similitude d'une matrice A est $\Omega_A = \{PAP^{-1} / P \in GL_n(\mathbb{C})\}$.

Déf. 44 : Soit G opérant sur X. On appelle invariant pour cette action une application sur X constante sur chaque orbite. L'invariant est dit total s'il prend deux valeurs différentes sur deux orbites distinctes.

Ex. 45 : Le spectre est un invariant total de similitude pour les matrices diagonalisables. Le polynôme minimal est un invariant, mais pas total.

3. Groupes de Sylow

Déf. 46 : Soit $|G| = n$, $p \mid n$ premier. Si $n = p^\alpha m$, $p \nmid m$, alors on appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Rem. 47 : S est un p-sg de Sylow $\iff$ $[G:S] \wedge p = 1$.

Ex. 48 : Soit $G = GL_n(\mathbb{F}_p)$, $|G| = mp^{\frac{n(n-1)}{2}}$. Alors un p-sg de Sylow de G est l'ensemble des matrices triangulaires supérieures strictes.

Th. 49 : (Théorèmes de Sylow.) • Soit G fini et $p \mid |G|$ premier. Alors G contient au moins un p-sous-groupe de Sylow. DEV 1

• Soit $|G| = n = p^\alpha m$, $p \nmid m$. Alors les p-Sylows sont tous conjugués ; leur nombre k divise n, et $k \equiv 1$ $[p]$ donc $k \mid m$.

Cor. 50 : Si S est un p-Sylow de G, alors $S \triangleleft G \iff S$ est l'unique p-Sylow.

Ex. 51 : Un groupe d'ordre 63 n'est pas simple.

App. 52 : Tout groupe simple d'ordre 60 est isomorphe à A_5.

III] Actions par équivalence et congruence

1. Action par équivalence

$\mathbb{K}$ corps, $G = GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$.

Déf. 53 : G opère sur $M_{m,n}(\mathbb{K})$ par équivalence via l'application $\alpha : G \times M_{m,n}(\mathbb{K}) \to M_{m,n}(\mathbb{K})$, $((P,Q),A) \mapsto (P,Q) \cdot A = PAQ^{-1}$.

Déf. 54 : L'orbite de A est $\Omega_A = \{(P,Q) \cdot A / P, Q \in G\} = \{B \in M_{m,n}(\mathbb{K}) / \operatorname{rg} B = \operatorname{rg} A\}$.
Le stabilisateur de A est $G_A = \{(P,Q) \in G / PAQ^{-1} = A\}$.

Ex.55 : Notons $I_{m,n,r} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}\}m$. Alors le stabilisateur de $I_{m,n,r}$ est $\left\{\left(P = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, Q = \begin{pmatrix} A & 0 \\ C' & D' \end{pmatrix}\right), \text{ où } A \in M_r(\mathbb{K}), (B, C') \in M_{r,m-r}(\mathbb{K}) \times M_{n-r,r}(\mathbb{K}), D', D \in M_{n-r,m-r}(\mathbb{K})\right\}$.

Th.56 : $A, B \in M_{m,n}(\mathbb{K})$ sont dans la même orbite $\Leftrightarrow$ $\mathrm{rg}\, A = \mathrm{rg}\, B$.

Rem.57 : On a $|\Omega_A| = |G|/|G_A| = |Gl_m(\mathbb{K}) \times Gl_n(\mathbb{K})| / |G_A|$.

2. Action par congruence

Déf.58 : $Gl_n(\mathbb{K})$ agit par congruence sur $\mathcal{S}_n(\mathbb{K})$ (matrices symétriques) via l'application $\beta : Gl_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) \to \mathcal{S}_n(\mathbb{K})$, $(P, A) \mapsto P.A = PA{}^tP$.

Th.59 :
- Si $\mathbb{K} = \mathbb{C}$, $\Omega_A = \Omega_{A'} \Leftrightarrow \mathrm{rg}\, A = \mathrm{rg}\, A'$;
- Si $\mathbb{K} = \mathbb{R}$, $\Omega_A = \Omega_{A'} \Leftrightarrow \mathrm{rg}\, A = \mathrm{rg}\, A'$ et A, A' ont même signature ;
- Si $\mathbb{K} = \mathbb{F}_q$, $\Omega_A = \Omega_{A'} \Leftrightarrow A, A'$ ont le même discriminant et même rang.

Ex.60 : $\Omega_{I_n} = \{S \in \mathcal{S}_n(\mathbb{R}) \ / \ \forall x \in \mathbb{R}^n \setminus \{0\}, {}^t x S x > 0\}$.

Ex.61 : $G_{I_n} = \{P \in Gl_n(\mathbb{R}) \ / \ P^tP = I_n\} = O_n(\mathbb{R})$ le groupe orthogonal.

DEV 2 **App.62** : (Loi de réciprocité quadratique.) Soient $p, q > 2$ impairs distincts. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, où $\left(\frac{\cdot}{\cdot}\right)$ est le symbole de Legendre.

IV] Actions sur les espaces vectoriels et affines

1. Représentations linéaires

Soit V un $\mathbb{C}$-ev de dimension finie.

Déf.63 : Une représentation linéaire de G dans V est la donnée d'un morphisme $\rho : G \to GL(V)$.

Déf.64 : Le caractère χ_ρ de ρ est l'application $\chi_\rho : g \in G \mapsto \mathrm{Tr}(\rho(g)) \in \mathbb{C}$.

Ex.65 : La représentation régulière : $\forall s \in G$, $\rho_r(s) : \mathbb{K}[G] \to \mathbb{K}[G]$, $f \mapsto \delta_s * f$.

Déf.66 : Une sous-représentation de ρ est une représentation $\rho' : G \to GL(V')$, où V' est un sev de V $\rho(g)$-stable $\forall g \in G$, et telle que $\rho(g)_{|V'} = \rho'(g)$. Une représentation est irréductible si elle n'admet aucune sous-représentation non triviale.

Prop.67 : Toute représentation peut s'écrire comme somme de représentations irréductibles. (Théorème de Maschke.)

Th.68 : Deux représentations sont isomorphes $\Leftrightarrow$ elles ont le même caractère.

App.69 : Table de caractères de S_4.

2. Isométries

Déf.70 : On appelle espace affine un ensemble $\mathcal{E}$ sur lequel le groupe additif $(E, +)$ d'un ev agit à droite, transitivement et librement.

Déf.71 : Le groupe $Is(X)$ des isométries de $X \subset \mathbb{R}^3$ est le sous groupe des isométries de l'espace affine euclidien $\mathbb{R}^3$ qui stabilisent X.

App.72 : On peut faire agir le groupe $Is(\Delta_4)$ sur l'ensemble $S = \{A, B, C, D\}$ des sommets de Δ_4, où Δ_4 désigne le tétraèdre : $\varphi : Is(\Delta_4) \to S_4$. On a alors le : $g \mapsto g_{|S}$

Th.73 : $Is(\Delta_4) \simeq S_4$ et $Is^+(\Delta_4) \simeq A_4$.

App.74 : On peut faire agir $Is(C_6)$ sur l'ensemble $\{D_1, D_2, D_3, D_4\} = D$ des grandes diagonales de C_6, où C_6 désigne le cube : $\varphi : Is(C_6) \to S_4$. On a alors le : $g \mapsto g_{|D}$

Th.75 : $Is^+(C_6) \simeq S_4$ et $Is(C_6) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$.

	Id 1	Transpositions 6	Double-transpositions 3	3-cycles 8	4-cycles 6
χ_1	1	1	1	1	1
χ_ε	1	-1	1	1	-1
χ_s	3	1	-1	0	-1
χ_4	2	0	2	-1	0
χ_c	3	-1	-1	0	1

Autres dvp possibles mis dans ce plan :

- Isométries
- Sg finis de SO_3
- Collier de perles

Références :

- Calais, Éléments de théorie des groupes
- Ulmer, Théorie des groupes

} I], II]

- Perrin, Cours d'algèbre → Sylow, p-groupes
- Peyré, L'algèbre discrète de la transformée de Fourier → Représentations
- NH2G2 I et II

Actions sur les matrices

Isométries

\+ Combes : collier de perles
déf. de l'espace affine