

## 101. Groupes opérant sur un ensemble. Exemples et applications.

**Introduction :** La notion d'action de groupe a d'abord été introduite en géométrie, avant d'être utilisée pour reformuler et prouver de nombreux résultats algébriques.

### 1 Actions de groupes

#### 1.1 Définitions et premières propriétés

Soit  $(G, \cdot)$  un groupe, soit  $X$  un ensemble.

**Définition 1.** On dit que  $G$  agit sur  $X$  (à gauche) s'il existe une application

$$\begin{cases} G \times X \rightarrow X \\ (g, x) \mapsto g \cdot x \end{cases} \text{ telle que :}$$

- (i).  $\forall g, g' \in G, \forall x \in X, g \cdot (g' \cdot x) = (gg') \cdot x$
- (ii).  $\forall x \in X, e_G \cdot x = x$ .

**Exemple 2.** Un groupe agit sur lui-même par :

- Translation à gauche :  $g \cdot h = gh$ .
- Translation à droite :  $g \cdot h = hg^{-1}$ .
- Conjugaison :  $g \cdot h = ghg^{-1}$ .

**Proposition 3.** Une action de  $G$  sur  $X$  induit un morphisme

$$\Phi \begin{cases} G \rightarrow \mathcal{S}_X \\ g \mapsto (\Phi(g) : x \mapsto g \cdot x) \end{cases} .$$

**Application 4** (Théorème de Cayley). *Tout groupe de cardinal  $n$  est isomorphe à un sous-groupe de  $\mathcal{S}_n$ .*

**Définition 5.** On considère une action de  $G$  sur  $X$ .

- Soit  $x \in X$ , on appelle orbite de  $x$  l'ensemble  $Gx = \{g \cdot x, g \in G\}$ . On appelle stabilisateur de  $x$  l'ensemble  $\text{Stab}(x) = \{g \in G, g \cdot x = x\}$ .
- L'action est dite transitive si elle ne possède qu'une seule orbite.

**Exemple 6.** L'action de translation à gauche d'un groupe est transitive.

**Exemple 7.**  $\mathcal{S}_n$  agit sur  $\llbracket 1, n \rrbracket$  par  $\sigma \cdot k = \sigma(k)$ . Le stabilisateur de  $k \in \llbracket 1, n \rrbracket$  est l'ensemble des permutations qui fixent  $k$ .

**Proposition 8.** Pour tout  $x \in X$ ,  $\text{Stab}(x)$  est un sous-groupe de  $G$ . Les orbites forment une partition de  $X$ .

### 1.2 Actions de groupes finis

**Théorème 9** (Formule des classes). Soit  $G$  groupe fini qui agit sur un ensemble fini  $X$ . On a, pour tout  $x \in X$ ,  $|G| = |Gx| \cdot |\text{Stab}(x)|$ . Ainsi, si  $\Omega$  partie de  $X$  qui rencontre chaque orbite en un seul point,  $|X| = \sum_{x \in \Omega} \frac{|G|}{|\text{Stab}(x)|}$ .

**Application 10** (Lemme de Cauchy). *Si  $p$  est un nombre premier, un  $p$ -groupe possède un élément d'ordre  $p$ .*

**Application 11.** *Si  $p$  est un nombre premier, un  $p$ -groupe a un centre non trivial.*

**Définition 12.** Si  $G$  agit sur  $X$ , pour  $g \in G$ , on appelle fixateur de  $g$  l'ensemble  $\text{Fix}(g) = \{x \in X, g \cdot x = x\}$ .

**Théorème 13** (Formule de Burnside). Si  $G, X$  sont finis, le nombre d'orbites de l'action de  $G$  sur  $X$  est donné par  $N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$ .

**Application 14.** *Si une roue de loterie est découpée en  $n$  secteurs, et qu'on dispose de  $p$  couleurs, le nombre de coloriages possibles est  $\frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) p^d$ .*

### 1.3 Théorèmes de Sylow

**Définition 15.** Soit  $p$  nombre premier, soit  $G$  un groupe d'ordre multiple de  $p$ . On appelle  $p$ -Sylow de  $G$  tout sous-groupe de  $G$  d'ordre égal à  $\max\{k \in \mathbb{N}, p^k \mid |G|\}$ .

**Théorème 16** (Théorèmes de Sylow). Soit  $G$  groupe d'ordre  $p^k m$ ,  $p$  premier,  $m \not\equiv 1 \pmod{p}$ .

- (i).  $G$  possède un  $p$ -Sylow.
- (ii). Tous les  $p$ -Sylow de  $G$  sont conjugués.
- (iii). Si on note  $c_p$  le nombre de  $p$ -Sylow de  $G$ , on a  $c_p \mid m$  et  $c_p \equiv 1 \pmod{p}$ .

**Application 17.** *Il n'existe pas de groupe simple à 30 ou 42 éléments.*

**Application 18.** *Le groupe  $A_n$  est simple pour tout  $n \geq 5$ .*

## 2 Exemples d'actions de groupes

### 2.1 Actions de conjugaison et de congruence

Soit  $\mathbb{K}$  un corps.

**Proposition 19.**  $GL_n(\mathbb{K})$  agit sur  $\mathcal{M}_n(\mathbb{K})$  par conjugaison :  $P \cdot M = PMP^{-1}$ .

**Définition 20.** Deux matrices qui sont dans la même orbite sont dites semblables. Les orbites sont appelées classes de similitude.

La réduction des endomorphismes consiste à déterminer les classes de similitude sous cette action.

**Exemple 21.** Si  $\mathbb{K} = \mathbb{C}$ , l'ensemble des matrices triangulaires supérieures forme un système de représentants des orbites pour cette action.

**Proposition 22.**  $GL_n(\mathbb{K})$  agit sur  $S_n(\mathbb{K})$  par congruence :  $P \cdot S = {}^tPSP$ .

**Théorème 23.** Lorsque  $\mathbb{K} = \mathbb{F}_q$ , il y a  $2n+1$  orbites pour cette action, représentées par les matrices  $\text{diag}(I_r, 0_{n-r})$ ,  $r \leq n$ , et  $\text{diag}(I_{r-1}, \alpha, 0_{n-r})$  où  $\alpha \in \mathbb{F}_q$  n'est pas un carré.

**Application 24** (Réciprocité quadratique). Soient  $p, q$  deux nombres premiers impairs distincts. On a  $\begin{pmatrix} p \\ q \end{pmatrix} \begin{pmatrix} q \\ p \end{pmatrix} = (-1)^{\frac{(p-1)(q-1)}{4}}$ .

## 2.2 Matrices de permutation

**Définition 25.** Pour  $\sigma \in S_n$ , on définit  $P_\sigma = (p_{i,j})_{1 \leq i,j \leq n}$  par  $\forall i, j, p_{i,j} = \delta_{i, \sigma(j)}$ .  $P_\sigma$  est appelée matrice de permutation associée à  $\sigma$ .

**Proposition 26.**  $S_n$  agit sur  $\mathcal{M}_n(\mathbb{K})$  par  $\sigma \cdot M = P_\sigma M$ , et deux matrices sont dans la même orbite si les lignes de l'une se déduisent de celles de l'autre par une permutation.

**Proposition 27** (Décomposition de Bruhat). On note  $T_s$  le sous-groupe de  $GL_n(\mathbb{K})$  formé des matrices triangulaires supérieures. Alors  $G = \bigsqcup_{\sigma \in S_n} T_s P_\sigma T_s$ .

**Proposition 28.** L'ensemble  $\mathcal{D}$  des drapeaux de  $\mathbb{K}^n$  est en bijection avec  $GL_n(\mathbb{K})/T_s$ , et l'ensemble des orbites pour l'action de translation de  $GL_n(\mathbb{K})$  sur  $GL_n(\mathbb{K})/T_s \times GL_n(\mathbb{K})/T_s$  est en bijection avec  $S_n$ .

## 2.3 Actions de groupes en géométrie

**Définition 29.** Un espace affine est la donnée d'un ensemble  $\mathcal{E}$ , d'un  $\mathbb{R}$ -espace vectoriel  $E$  et d'une action transitive de  $(E, +)$  sur  $\mathcal{E}$ , dont les stabilisateurs sont réduits à un point, donnée par  $(v, M) \mapsto M + v$ .

**Proposition 30.**  $S_4$  agit sur les sommets du tétraèdre régulier et sur les grandes diagonales du cube.

**Corollaire 31.**  $S_4$  est isomorphe à  $Isom(T)$  et  $Isom^+(C)$ .

# 3 Représentations linéaires des groupes finis

## 3.1 Définitions et propriétés

**Définition 32.** Soit  $G$  un groupe. On appelle représentation linéaire de  $G$  la donnée d'un  $\mathbb{C}$ -espace vectoriel  $V$  et d'une action de groupe de  $G$  sur  $V$  compatible avec la structure d'espace vectoriel. Cela définit un morphisme de groupes  $\rho : G \rightarrow GL(V)$ . Si  $V$  est de dimension finie, sa dimension est appelée degré de la représentation.

**Exemple 33.**

- Le morphisme constant  $\mathbf{1} : G \rightarrow \mathbb{C}^*$  est une représentation de degré 1.
- Le groupe diédral s'identifie à un sous-groupe de  $GL(\mathbb{R}^2)$  : c'est la représentation standard, de degré 2.

**Définition 34.** On dit qu'un sous-espace  $W$  de  $V$  est stable par la représentation s'il est stable par tous les  $\rho(g)$ ,  $g \in G$ . La représentation est dite irréductible si ses seuls sous-espaces stables sont  $\{0\}$  et  $V$ .

**Définition 35.** Si  $(\rho_1, V_1), (\rho_2, V_2)$  sont des représentations de  $G$ , on définit leur somme directe comme la représentation sur  $V_1 \oplus V_2$  définie par  $(\rho_1 \oplus \rho_2)(g) = \rho_1(g) \oplus \rho_2(g)$ .

**Théorème 36** (Maschke). Toute représentation de degré fini est somme directe de représentations irréductibles.

**Définition 37.**  $(\rho_1, V_1)$  et  $(\rho_2, V_2)$  sont dites équivalentes s'il existe  $f : V_1 \rightarrow V_2$  isomorphisme tel que  $\forall g \in G, \rho_2(g) = f \circ \rho_1(g) \circ f^{-1}$ .

## 3.2 Caractères

**Définition 38.** On appelle caractère d'une représentation  $(\rho, V)$  l'application  $\chi_\rho : g \mapsto \text{tr}(\rho(g))$ .

**Proposition 39.** On a  $\chi_\rho(1) = \text{deg}(\rho)$  et  $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$ .

On munit l'ensemble  $\mathcal{F}(G)$  des fonctions de  $G$  dans  $\mathbb{C}$  du produit scalaire hermitien

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}.$$

**Théorème 40.**

- Deux représentations irréductibles sont équivalentes si et seulement si elles ont même caractère.
- Les caractères des représentations irréductibles forment une base orthonormée de l'espace des fonctions  $G \rightarrow \mathbb{C}$  constantes sur les classes de conjugaison.

**Définition 41.** On appelle table de caractères le tableau donnant la valeur de chaque caractère irréductible sur chaque classe de conjugaison.

**Exemple 42.** Table de caractères de  $\mathcal{S}_4$ .

## Annexe

Table de caractères de  $\mathcal{S}_4$  :

	$Id$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$	$(1\ 2)(3\ 4)$
$\chi_1$	1	1	1	1	1
$\chi_\varepsilon$	1	-1	1	-1	1
$\chi_s$	3	1	0	-1	-1
$\chi'_s$	3	-1	0	1	-1
$\chi_t$	2	0	-1	0	2

## Développements

- Décomposition de Bruhat.
- Loi de réciprocité quadratique.

## Références

- [1] G. Auliac, J. Delcourt, R. Goblot, OBJECTIF LICENCE - ALGÈBRE ET GÉOMÉTRIE, Ediscience.
- [2] J. Delcourt, THÉORIE DES GROUPES, Dunod.
- [3] G. Rauch, LES GROUPES FINIS ET LEURS REPRÉSENTATIONS, Ellipses.
- [4] A. Szpirglas et al., Algèbre L3, Pearson.