

101 Groupe opérant sur un ensemble. Exemples et applications.

Soit G un groupe.

I - Actions de groupe

Soit $X \neq \emptyset$ un ensemble.

1. Cas général

Définition 1. On appelle **action** (à gauche) de G sur X toute application

$$\begin{aligned} G \times X &\rightarrow X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

satisfaisant les conditions suivantes :

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

[ULM21]
p. 29

Remarque 2. On peut de même définir une action à droite de G sur X .

Exemple 3. — Le groupe S_X des bijections de X dans X opère naturellement sur X par la relation $\sigma \cdot x = \sigma(x)$ pour tout $\sigma \in S_X$ et pour tout $x \in X$.
— Pour un espace vectoriel V , le groupe $GL(V)$ opère sur V .

On supposera par la suite que G agit sur X à gauche via l'action \cdot .

Théorème 4. On a une correspondance bijective entre les actions de G sur X et les morphismes de G dans S_X . En effet, si \cdot désigne une action de G sur X , on peut y faire correspondre le morphisme

$$\varphi : \begin{aligned} G &\rightarrow S_X \\ g &\mapsto (x \mapsto g \cdot x) \end{aligned}$$

Définition 5. On définit pour tout $x \in X$:

- $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$ l'**orbite** de x .
- $\text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\} < G$ le **stabilisateur** de x .

On dit que l'action de G sur X est :

- **Libre** si $\text{Stab}_G(x) = \{e_G\}$ pour tout $x \in X$.

— **Transitive** si G n'admet qu'une seule orbite.

Exemple 6. L'action du groupe diédral \mathcal{D}_3 sur les sommets d'un triangle équilatéral est transitive mais n'est pas libre.

Proposition 7. La relation \sim définie sur X par

$$x \sim y \iff x \in G \cdot y$$

est une relation d'équivalence dont les classes d'équivalence sont les orbites des éléments de X sous l'action de G .

Application 8. Toute permutation $\sigma \in S_n$ s'écrit comme produit

$$\sigma = \gamma_1 \cdots \gamma_m$$

de cycles γ_i de longueur ≥ 2 dont les supports sont deux-à-deux disjoints. Cette décomposition est unique à l'ordre près.

[PER]
p. 57

Définition 9. Une action $\varphi : G \rightarrow S_X$ une action de G sur X est dite **fidèle** si $\text{Ker}(\varphi) = \{e_G\}$.

[ULM21]
p. 33

Proposition 10. Soit $\varphi : G \rightarrow S_X$ une action de G sur X . Alors,

$$\text{Ker}(\varphi) = \bigcap_{x \in X} \text{Stab}_G(x)$$

Corollaire 11. Une action libre est fidèle.

Proposition 12. Soit $x \in X$. L'application

$$f : \begin{array}{ccc} G / \text{Stab}_G(x) & \rightarrow & G \cdot x \\ g \text{Stab}_G(x) & \mapsto & g \cdot x \end{array}$$

est une bijection.

p. 71

Remarque 13. Attention cependant, $G / \text{Stab}_G(x)$ n'est pas un groupe en général.

2. Cas fini

On suppose ici que G et X sont finis.

Proposition 14. Soit $x \in X$. Alors :

- $|G \cdot x| = (G : \text{Stab}_G(x))$.
- $|G| = |\text{Stab}_G(x)| |G \cdot x|$.
- $|G \cdot x| = \frac{|G|}{|\text{Stab}_G(x)|}$

Théorème 15 (Formule des classes). Soit Ω un système de représentants associé à la relation \sim de la Proposition 7. Alors,

$$|X| = \sum_{\omega \in \Omega} |G \cdot \omega| = \sum_{\omega \in \Omega} (G : \text{Stab}_G(\omega)) = \sum_{\omega \in \Omega} \frac{|G|}{|\text{Stab}_G(\omega)|}$$

Définition 16. On définit :

- $X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$ l'ensemble des points de X laissés fixes par tous les éléments de G .
- $X^g = \{x \in X \mid g \cdot x = x\}$ l'ensemble des points de X laissés fixes par $g \in G$.

Corollaire 17 (Formule de Burnside). Le nombre r d'orbites de X sous l'action de G est donné par

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Corollaire 18. Soit p un nombre premier. Si G est un p -groupe (ie. l'ordre de G est une puissance de p), alors,

$$|X^G| \equiv |X| \pmod{p}$$

Corollaire 19. Soit p un nombre premier. Le centre d'un p -groupe non trivial est non trivial.

Corollaire 20. Soit p un nombre premier. Un groupe d'ordre p^2 est toujours abélien.

Application 21 (Théorème de Cauchy). On suppose G non trivial et fini. Soit p un premier divisant l'ordre de G . Alors il existe un élément d'ordre p dans G .

Application 22 (Premier théorème de Sylow). On suppose G fini d'ordre np^α avec $n, \alpha \in \mathbb{N}$ et p premier tel que $p \nmid n$. Alors, il existe un sous-groupe de G d'ordre p^α .

II - Action d'un groupe sur un groupe

1. Action par translation

Proposition 23. G agit sur lui-même par translation (à gauche) via l'action

[ULM21]
p. 34

$$(g, h) \mapsto g \cdot h = gh$$

De plus, cette action est fidèle et transitive.

Application 24 (Théorème de Cayley). Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n .

Proposition 25. Soit $H < G$. Alors G agit sur G/H via l'action

$$(g, hH) \mapsto g \cdot hH = (gh)H$$

De plus, cette action est transitive.

Proposition 26. Soit $H < G$. Soit $\varphi : G \rightarrow S_{G/H}$ le morphisme de l'action par translation de G sur G/H . Alors,

$$\text{Ker}(\varphi) = \bigcap_{g \in G} gHg^{-1}$$

Application 27. On suppose que G est de cardinal infini et que G possède un sous-groupe d'indice fini distinct de G . Alors G n'est pas simple.

[PER]
p. 17

2. Action par conjugaison

Proposition 28. G agit sur lui-même par conjugaison via l'action

[ULM21]
p. 36

$$(g, h) \mapsto g \cdot h = ghg^{-1}$$

Définition 29. — L'orbite de $g \in G$ sous l'action par conjugaison de G sur lui-même s'appelle la **classe de conjugaison** de g .

- Le stabilisateur de $g \in G$ sous l'action par conjugaison de G sur lui-même s'appelle le **centralisateur** de g .
- Deux éléments de G qui appartiennent à la même classe de conjugaison sont dits **conjugués**.

Exemple 30. — Si $\sigma = (a_1 \dots a_p) \in S_n$ est un p -cycle, et si $\tau \in S_n$, alors

$$\tau \sigma \tau^{-1} = (\tau(a_1) \dots \tau(a_p))$$

— Par conséquent, dans S_n , les p -cycles sont conjugués.

— Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n .

[PER]
p. 15

Proposition 31. Soit $g \in G$. Alors g appartient au centre de G (noté $Z(G)$) si et seulement si sa classe de conjugaison est réduite à un seul élément.

[ULM21]
p. 36

Corollaire 32. $Z(G)$ est l'union des classes de conjugaison de taille 1.

Proposition 33. Soit Ω un système de représentants associé à la relation \sim de la Proposition 7 pour l'action par conjugaison. On note $\Omega' = Z(G) \setminus \Omega$. Alors,

[GOU21]
p. 24

$$|G| = |Z(G)| + \sum_{\omega \in \Omega'} \frac{|G|}{|\text{Stab}_G(\omega)|}$$

[DEV]

Application 34 (Théorème de Wedderburn). Tout corps fini est commutatif.

p. 100

Proposition 35. G agit sur ses sous-groupes par conjugaison via l'action

[ULM21]
p. 38

$$(g, H) \mapsto g \cdot H = gHg^{-1}$$

Proposition 36. Soit $H < G$. Alors H est distingué dans G si et seulement si H est un point fixe pour l'action de la Proposition 35.

III - Action d'un groupe sur un espace vectoriel

1. Action par conjugaison sur les espaces de matrices

Soit E un espace vectoriel de dimension finie n sur un corps \mathbb{K} .

Proposition 37. L'application

[ROM21]
p. 199

$$\begin{aligned} \text{GL}_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) &\rightarrow \mathcal{M}_n(\mathbb{K}) \\ (P, A) &\mapsto PAP^{-1} \end{aligned}$$

définit une action de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Définition 38. Deux matrices qui sont dans la même orbite pour cette action sont dites **semblables**.

Remarque 39. Deux matrices semblables représentent la même application linéaire dans deux bases de \mathbb{K}^n .

[GOU21]
p. 127

C'est cette remarque qui justifie que l'on va étudier l'action par conjugaison de $\mathrm{GL}_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Théorème 40. Soient A et B deux matrices semblables. Alors :

[ROM21]
p. 199

- $\mathrm{trace}(A) = \mathrm{trace}(B)$.
- $\det(A) = \det(B)$.
- $\mathrm{rang}(A) = \mathrm{rang}(B)$.
- $\chi_A = \chi_B$.
- $\pi_A = \pi_B$.

Contre-exemple 41. Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont la même trace, le même déterminant, le même polynôme caractéristique, mais ne sont pas semblables.

[D-L]
p. 137

Théorème 42. Soient \mathbb{L} une extension de \mathbb{K} et $A, B \in \mathcal{M}_n(\mathbb{K})$. On suppose \mathbb{K} infini et A, B semblables sur \mathbb{L} . Alors A et B sont semblables sur \mathbb{K} .

[GOU21]
p. 167

Notation 43. Soient $f \in \mathcal{L}(E)$ et $x \in E$. On note $P_{f,x}$ le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et $E_{f,x} = \{P(f)(x) \mid P \in \mathbb{K}[X]\}$.

p. 397

Lemme 44. Soit $f \in \mathcal{L}(E)$.

- (i) Si $k = \deg(\pi_f)$, alors $\mathbb{K}[f]$ est un sous-espace vectoriel de $\mathcal{L}(E)$ de dimension k , dont une base est $(f^i)_{i \in [0, k-1]}$.
- (ii) Soit $x \in E$. Si $l = \deg(P_{f,x})$, alors E_x est un sous-espace vectoriel de E de dimension l , dont une base est $(f^i(x))_{i \in [0, l-1]}$.

Lemme 45. Soit $f \in \mathcal{L}(E)$. Il existe $x \in E$ tel que $P_{f,x} = \pi_f$.

Théorème 46 (Frobenius). Soit $f \in \mathcal{L}(E)$. Il existe des sous-espaces vectoriels F_1, \dots, F_r de E tous stables par f tels que :

(i) $E = \bigoplus_{i=1}^r F_i.$

(ii) $\forall i \in \llbracket 1, r \rrbracket$, la restriction $f_i = f|_{F_i}$ est un endomorphisme cyclique de F_i .

(iii) Si $P_i = \pi_{f_i}$ est le polynôme minimal de f_i , on a $P_{i+1} \mid P_i \forall i \in \llbracket 1, r-1 \rrbracket$.

La suite $(P_i)_{i \in \llbracket 1, r \rrbracket}$ ne dépend que de f et non du choix de la décomposition (elle est donc unique). On l'appelle **suite des invariants de f** .

Corollaire 47. Deux endomorphismes sont semblables si et seulement s'ils ont les mêmes invariants de similitude.

2. Représentations linéaires et caractères

Dans cette partie, on suppose que G est d'ordre fini.

[ULM21]
p. 144

Définition 48. — Une **représentation linéaire** ρ est un morphisme de G dans $\mathrm{GL}(V)$ où V désigne un espace-vectoriel de dimension finie n sur \mathbb{C} .

— On dit que n est le **degré** de ρ .

— On dit que ρ est **irréductible** si $V \neq \{0\}$ et si aucun sous-espace vectoriel de V n'est stable par $\rho(g)$ pour tout $g \in G$, hormis $\{0\}$ et V .

Exemple 49. Soit $\varphi : G \rightarrow S_n$ le morphisme structurel d'une action de G sur un ensemble de cardinal n . On obtient une représentation de G sur $\mathbb{C}^n = \{e_1, \dots, e_n\}$ en posant

$$\rho(g)(e_i) = e_{\varphi(g)(i)}$$

c'est la représentation par permutations de G associée à l'action. Elle est de degré n .

Définition 50. La représentation par permutations de G associée à l'action par translation à gauche de G sur lui-même est la **représentation régulière** de G , on la note ρ_G .

Définition 51. On peut associer à toute représentation linéaire ρ , son **caractère** $\chi = \mathrm{trace} \circ \rho$. On dit que χ est **irréductible** si ρ est irréductible.

p. 150

Proposition 52. (i) Les caractères sont des fonctions constantes sur les classes de conjugaison.

(ii) Il y a autant de caractères irréductibles que de classes de conjugaisons.

Définition 53. Soit $\rho : G \rightarrow \text{GL}(V)$ une représentation linéaire de G . On suppose $V = W \oplus W_0$ avec W et W_0 stables par $\rho(g)$ pour tout $g \in G$. On dit alors que ρ est **somme directe** de ρ_W et de ρ_{W_0} .

Théorème 54 (Maschke). Toute représentation linéaire de G est somme directe de représentations irréductibles.

Théorème 55. Les sous-groupes distingués de G sont exactement les

$$\bigcap_{i \in I} \text{Ker}(\rho_i) \text{ où } I \in \mathcal{P}(\llbracket 1, r \rrbracket)$$

[PEY]
p. 231

Corollaire 56. G est simple si et seulement si $\forall i \neq 1, \forall g \neq e_G, \chi_i(g) \neq \chi_i(e_G)$.

Bibliographie

Leçons pour l'agrégation de mathématiques

[D-L]

Maximilien DREVETON et Joachim LHABOUZ. *Leçons pour l'agrégation de mathématiques. Préparation à l'oral*. Ellipses, 28 mai 2019.

<https://www.editions-ellipses.fr/accueil/3543-13866-lecons-pour-lagregation-de-mathematiques-preparation-a-loral-9782340030183.html>.

Les maths en tête

[GOU21]

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3^e éd. Ellipses, 13 juill. 2021.

<https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html>.

Cours d'algèbre

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

L'algèbre discrète de la transformée de Fourier

[PEY]

Gabriel PEYRÉ. *L'algèbre discrète de la transformée de Fourier. Niveau M1*. Ellipses, 15 jan. 2004.

<https://adtf-livre.github.io>.

Mathématiques pour l'agrégation

[ROM21]

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2^e éd. De Boeck Supérieur, 20 avr. 2021.

<https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie>.

Théorie des groupes

[ULM21]

Felix ULMER. *Théorie des groupes. Cours et exercices*. 2^e éd. Ellipses, 3 août 2021.

<https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html>.