

Leçon 101 Groupes opérants sur un ensemble. Exemples et applications.

Dans cette leçon on considère G un groupe noté multiplicativement de neutre e et X un ensemble.

1 Actions de groupes

1.1 Définitions et exemples

Définition 1. On appelle action à gauche de G sur X toute application $G \times X \rightarrow X ; (g, x) \mapsto g \cdot x$ vérifiant les conditions suivantes :

1. $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ pour tout $g, h \in G$ et tout $x \in X$.
2. $e \cdot x = x$ pour tout $x \in X$.

Un ensemble X sur laquelle opère G est appelé G -ensemble. Lorsque le cadre est clair on abrège $g \cdot x$ en gx .

Exemple 2. — Le groupe $\mathcal{S}(X)$ des bijections de X opère naturellement sur X par la relation $\sigma \cdot x = \sigma(x)$ pour tout $\sigma \in \mathcal{S}(X)$ et tout $x \in X$.

- L'action triviale de G sur X est donnée par $g \cdot x = x$ pour tout $g \in G$ et tout $x \in X$.
- G agit sur lui même par translation en posant $g \cdot h = gh$.
- Si H sous groupe de G , alors G agit par translation sur G/H avec $g_1 \cdot g_2 H = (g_1 g_2) H$.
- G agit sur lui même par conjugaison en posant $g \cdot h = ghg^{-1}$.
- G agit sur l'ensemble de ses sous-groupes par conjugaison avec $g \cdot H = gHg^{-1}$.

Définition 3. On dit que $x \in X$ est point fixe sous l'action de G lorsque $gx = x$ pour tous $g \in G$.

On dit que $Y \subset X$ est une partie stable sous l'action de G lorsque $g(Y) \subset Y$ pour tout $g \in G$.

Théorème 4. On définit une correspondance bijective entre les opérations de G sur X et les morphismes $\gamma : G \rightarrow \mathcal{S}(X)$ de la

manière suivante : à une action de G sur X correspond le morphisme $\varphi : G \rightarrow \mathcal{S}(X) ; g \mapsto \sigma_g$ avec $\sigma_g(x) = g \cdot x$. On dit que φ est le morphisme structural de l'action de G sur X .

Proposition 5. Soit φ une action de G sur X .

1. Si $\psi : \Gamma \rightarrow G$ est un morphisme, alors X est aussi un Γ -ensemble pour l'action $\gamma \odot x = \psi(\gamma) \cdot x = \varphi(\psi(\gamma))(x)$ pour tout $x \in X$ et $\gamma \in \Gamma$.
2. Si $Y \subset X$ est stable sous l'action de G alors Y est un G -ensemble.

Corollaire 6. Si X est fini à n éléments, alors à toute numérotation des éléments de X correspond une bijection entre les opérations de G sur X et les morphismes $\varphi : G \rightarrow \mathcal{S}_n$.

Définition 7. Soit X un G -ensemble et $x \in X$. On appelle **orbite** de x sous G le sous ensemble $\Omega_G(x) := \{g \cdot x | g \in G\}$. On appelle **stabilisateur** de x dans G le sous groupe $Stab_G(x) := \{g \in G | g \cdot x = x\}$. On dit que G opère **librement** sur X lorsque tous les stabilisateurs sont triviaux, c'est-à-dire $g \cdot x = x \iff g = e$ pour tout $x \in X$. On dit que G opère **transitivement** sur X lorsqu'il existe exactement une orbite dans X .

Proposition 8. Soit X un G -ensemble. La relation $\sim$ définie sur X par $x \sim y$ lorsque $x \in \Omega_G(y)$ est une relation d'équivalence sur X dont les classes d'équivalences sont les orbites des éléments sous l'action. Autrement dit les orbites des éléments de X forment une partition de X . On note G/X l'ensemble quotient $X / \sim$.

Exemple 9. Le groupe des isométries du plan opère sur le plan donc D_n son sous groupe qui laisse fixe les n sommets d'un polygone. En restreignant l'action de D_n à ces n points on obtient une action $D_n \rightarrow \mathcal{S}_n$, cette action est transitive (l'orbite d'un sommet contient tous les sommets). Cette action n'est pas libre pour $n \geq 3$ car la symétrie axiale passant par un sommet le laisse fixe.

Proposition 10. Soit $\varphi : G \rightarrow \mathcal{S}(X)$ une action de G sur X , alors le noyau de φ est $\ker(\varphi) = \bigcap_{x \in X} \text{Stab}_G(x)$.

Définition 11. Une action $\varphi : G \rightarrow \mathcal{S}(X)$ de G sur X est dit **fidèle** lorsque $\ker(\varphi) = \{e\}$. C'est-à-dire que le seul stabilisateur commun à tous les éléments de X est le neutre e .

1.2 Principaux théorèmes

Théorème 12. (Cayley) Tout groupe fini G d'ordre $n \in \mathbb{N}$ est isomorphe à un sous groupe transitif de $\mathcal{S}_n$.

Proposition 13. L'opération de translation à gauche de G sur G/H est une action transitive dont le morphisme structurel est de la forme $\varphi : G \mapsto \mathcal{S}_{[G:H]}$

Lemme 14. Soit G groupe fini d'ordre n et $H \subset G$ un sous groupe d'indice k tel que n ne divise pas $k!$. Alors il existe $N \triangleleft G$ distinct de $\{e\}$ inclus dans H .

Définition 15. L'orbite d'un élément $g \in G$ par l'action de conjugaison est appelé classe de conjugaison, deux éléments dans la même classe de conjugaison sont dit conjugués. Le stabilisateur d'un élément $g \in G$ est appelé centralisateur de g dans G et noté $Z_G(g)$.

Proposition 16. Un sous groupe H de G est distingué si et seulement si H est point fixe de l'action de G sur ses sous groupes par conjugaison.

Théorème 17. Soit X un G -ensemble, pour tout $x \in X$ l'application $\varphi_x : G/\text{Stab}_G(x) \rightarrow \Omega_G(x)$; $\bar{g} = g\text{Stab}_G(x) \mapsto g \cdot x$ est bien définie et bijective. Dans le cas où G est fini on a de plus, $|\Omega_G(x)| = [G : \text{Stab}_G(x)] = \frac{|G|}{|\text{Stab}_G(x)|}$.

Théorème 18. (Équation aux classes) Soit G un groupe fini opérant sur un ensemble fini X . En notant $\Omega(x_1), \dots, \Omega(x_r)$ toutes les orbites 2 à 2 distinctes on a :

$$|X| = \sum_{k=1}^r |\Omega(x_k)| = \sum_{k=1}^r \frac{|G|}{|\text{Stab}_G(x_k)|}$$

1.3 Applications aux p-groupes

Définition 19. Si $p \geq 2$ est un nombre premier, on appelle p -groupe tout groupe de cardinal p^α où $\alpha \in \mathbb{N}^*$.

Remarque 20. Pour X un G -ensemble, on note $X^G = \{x \in X | \Omega(x) = \{x\}\}$ l'ensemble des éléments dont l'orbite est réduite à un point.

Corollaire 21. Si $p \geq 2$ premier et G un p -groupe opérant sur un ensemble X fini, alors $|X^G| \equiv |X| \pmod{p}$

Corollaire 22. Soit G un groupe fini qui opère sur lui même par conjugaison, en notant $\Omega(x_1), \dots, \Omega(x_r)$ toutes les orbites 2 à 2 distinctes, on a :

$$|G| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)| \geq 2}}^r |\Omega(x_i)| = |Z(G)| + \sum_{\substack{i=1 \\ |\Omega(x_i)| \geq 2}}^r \frac{|G|}{|\text{Stab}(x_i)|}$$

Théorème 23. Pour tout nombre premier p , le centre d'un p -groupe n'est pas réduit à $\{1\}$.

Théorème 24. Tout groupe d'ordre p^2 avec p premier est commutatif. Il est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

2 Actions sur les espaces de matrice

2.1 Action par translation

Lemme 25. Soient E, F des $\mathbb{K}$ espaces vectoriels et $u, v \in \mathcal{L}(E, F)$.

1. Pour tous supplémentaires H de $\ker(u)$ dans E , la restriction $u|_H$ est un isomorphisme de H sur $\text{Im}(u)$.
2. On a $\ker(u) \subset \ker(v)$ si et seulement si il existe $w : \text{Im}(u) \rightarrow \text{Im}(v)$ telle que $v(x) = w(u(x))$ pour tout $x \in E$.
3. Soient H et G supplémentaires respectifs de $\ker(u)$ et $\ker(v)$ dans E , on a $\text{Im}(v) \subset \text{Im}(u)$ si et seulement si il existe $w : G \rightarrow H$ linéaire telle que $v(x) = w(u(x))$ pour tout $x \in G$.

Théorème 26. L'application $GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \rightarrow \mathcal{M}_n(\mathbb{K})$; $(P, A) \mapsto P \cdot A = PA$ définit une action de translation de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Théorème 27. (Décomposition polaire) Toute matrice $A \in \mathcal{M}_n(\mathbb{R})$ (resp $A \in \mathcal{M}_n(\mathbb{C})$) peut s'écrire $A = \Omega S$ où Ω est une matrice orthogonale (resp unitaire) et S une matrice symétrique (resp hermitienne) positive. Donc ils existe dans l'orbite de A , pour l'action de $\mathcal{O}_n(\mathbb{R})$ (resp $\mathcal{U}_n(\mathbb{C})$) sur $\mathcal{M}_n(\mathbb{R})$ (resp $\mathcal{M}_n(\mathbb{C})$) par translation, un représentant symétrique (resp hermitien) positif.

Théorème 28. L'application $GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \rightarrow \mathcal{M}_n(\mathbb{K})$; $(P, A) \mapsto PA$ définit une action par translation à gauche et deux matrices ont la même orbite si et seulement si elles ont le même noyau.

Théorème 29. — La multiplication à gauche d'une matrice par une matrice de dilatation $D_i(\lambda)$ a pour effet de multiplier sa i -ième ligne par λ .

— La multiplication à gauche d'une matrice par une matrice de transvection $T_{ij}(\lambda)$ a pour effet de remplacer sa i -ième ligne L_i par $L_i + \lambda L_j$.

— La multiplication à droite d'une matrice par une matrice de dilatation $D_j(\lambda)$ a pour effet de multiplier sa j -ième colonne par λ .

— La multiplication à gauche d'une matrice par une matrice de transvection $T_{ij}(\lambda)$ a pour effet de remplacer sa j -ième colonne C_j par $C_j + \lambda C_i$.

Théorème 30. Soit $A \in \mathcal{M}_n(\mathbb{K})$, il existe une matrice $P \in GL_n(\mathbb{K})$ produit de matrice de permutation et de transvection telle que PA soit échelonnée en ligne. Elle est dans l'orbite de A .

Remarque 31. Les opérations lors d'un Pivote de Gauss reviennent à multiplier A par une matrice de transvection ou de dilatation.

2.2 Action par conjugaison

Théorème 32. L'application $GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \rightarrow \mathcal{M}_n(\mathbb{K})$; $(P, A) \mapsto PAP^{-1}$ définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$.

Définition 33. Deux matrices ayant la même orbite pour cette action sont dites semblables.

On considère à présent E un $\mathbb{F}_q$ espace vectoriel de dimension $n \geq 2$. On note $DL(E)$ l'ensemble des automorphismes diagonalisables de E et on note $\mathbb{F}_q = \{\lambda_1, \dots, \lambda_{q-1}\}$

Lemme 34. On a $DL(E) = \{u \in GL(E) | u^{q-1} = Id\}$.

Lemme 35. Pour tout $u \in DL(E)$ on a $E = \bigoplus_{k=1}^{q-1} \ker(u - \lambda_k Id)$

On note $\mathcal{F} = \{(E_1, \dots, E_{q-1}) | E = \bigoplus_{k=1}^{q-1} E_k\}$.

Lemme 36. L'application $\varphi : DL(E) \rightarrow \mathcal{F}$; $u \mapsto (\ker(u - \lambda_k Id))_{1 \leq k \leq q-1}$ est bijective.

Pour $(n_1, \dots, n_{q-1})$ tels que $n_1 + \dots + n_{q-1} = n$ on note $\mathcal{F}_{(n_1, \dots, n_{q-1})} = \{(E_k)_{1 \leq k \leq q-1} \in \mathcal{F} | \dim(E_k) = n_k, 1 \leq k \leq q-1\}$.

Lemme 37. Pour $(n_1, \dots, n_{q-1})$ tels que $n_1 + \dots + n_{q-1} = n$ fixés, l'application :

$$GL(E) \times \mathcal{F}_{(n_1, \dots, n_{q-1})} \rightarrow \mathcal{F}_{(n_1, \dots, n_{q-1})}$$

$$(u, (E_1, \dots, E_{q-1})) \mapsto (u(E_1), \dots, u(E_{q-1}))$$

définit une action transitive de $GL(E)$ sur $\mathcal{F}_{(n_1, \dots, n_{q-1})}$.

Lemme 38. Pour $(n_1, \dots, n_{q-1})$ tels que $n_1 + \dots + n_{q-1} = n$ et $(E_k)_{1 \leq k \leq q-1}$ fixés dans $\mathcal{F}_{(n_1, \dots, n_{q-1})}$, on note $Stab(E_1, \dots, E_{q-1}) = \{u \in GL(E) | u(E_k) = E_k, 1 \leq k \leq q-1\}$

et on a $|Stab(E_1, \dots, E_{q-1})| = \prod_{k=1}^{q-1} |GL(E_k)|$ et $|\mathcal{F}_{(n_1, \dots, n_{q-1})}| =$

$$\frac{|GL(E)|}{\prod_{k=1}^{q-1} |GL(E_k)|}$$

Théorème 39. On a : $|DL(E)| = \sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)| \dots |GL_{n_{q-1}}(\mathbb{F}_q)|}$ avec la convention de $|GL_0(\mathbb{F}_q)| = 1$

Dev 1 : Classification des groupes d'ordre p^2 21, 22, 23 et 24
Dev 2 : Dénombrement des matrices diagonalisables de $\mathbb{F}_q$ 35, 36, 37, 38 et 39

Références

- [ROM17] Jean-Étienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.
- [ULM12] Félix ULMER : Théorie des groupes. Ellipses, 2012.

RAPPORT DU JURY :

Le matériel théorique en accord avec le programme doit être présenté, accompagné d'illustrations pertinentes. Il faut pouvoir dégager l'intérêt des notions introduites avec des exemples d'actions bien choisies pour obtenir des informations soit sur un ensemble X donné, soit sur un groupe G donné et faire apparaître des sous-groupes intéressants de G comme stabilisateurs. Par ailleurs, la présentation doit illustrer comment l'étude des orbites de certaines actions revient à classifier certains objets, soit en trouvant un représentant simple de chaque orbite, soit en dégageant des invariants caractérisant les orbites. Les actions de groupes interviennent aussi efficacement dans des problèmes de dénombrements, notamment via la formule de Burnside. Les exemples peuvent être internes à la théorie des groupes (action naturelle de S_n sur $t_1, \dots, t_n$, action par translation ou par conjugaison, représentations de groupes, etc). Mais il est souhaitable d'emprunter aussi à d'autres domaines (action sur des anneaux, des espaces de matrices ou des espaces de polynômes, groupes d'isométries, etc). La géométrie fournit aussi de nombreux exemples pertinents (groupes d'isométries d'un polygone dans le plan ou d'un solide ou d'un polygone régulier dans l'espace). Pour aller plus loin, on peut aborder l'action de $PGL_2(\mathbb{K})$ sur la droite projective menant au birapport ou celle de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré ou les preuves par actions de groupes des théorèmes de Sylow ou encore d'autres actions donnant lieu à des isomorphismes exceptionnels. Il est aussi possible de s'intéresser aux aspects topologiques ou différentiels liés à certaines actions.