Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

1. Généralités

DÉFINITION 1. Soient G un groupe et X un ensemble. Une action de G sur X est une application de $G \times X$ dans X,

$$\begin{array}{rcl} G \times X & \to & X \\ (g,x) & \mapsto & g \cdot x, \end{array}$$

vérifiant pour tout x dans X,

i) $e \cdot x = x$ où e est l'élément neutre de G,

ii) $g \cdot (h \cdot x) = (gh) \cdot x$, pour tout $g, h \in G$.

On dit alors que G agit sur X et on note $G \curvearrowright X$.

REMARQUE 2. Considérer une action de G sur X équivaut à considérer un morphisme $\varphi : G \to \mathfrak{S}(X)$ de G dans le groupe des permutations $\mathfrak{S}(X)$ avec $\varphi(g) : x \mapsto g \cdot x$.

EXEMPLE 3. Le groupe symétrique $\mathfrak{S}_n$ agit naturellement sur $\{1, \ldots, n\}$ en posant $\sigma \cdot i = \sigma(i)$, pour tout $\sigma \in \mathfrak{S}_n$ et tout $i \in \{1, \ldots, n\}$.

Si E est un espace vectoriel, le groupe $GL(E)$ agit naturellement sur E via $u \cdot e = u(e)$, pour tout $u \in GL(E)$ et $e \in E$.

Le groupe diédral $\mathcal{D}_{2n}$ agit naturellement sur le polygône régulier à n côtés.

DÉFINITION 4. Soit G un groupe agissant sur un ensemble X. On appelle orbite d'un élément $x \in X$ le sous-ensemble de X suivant,

$$\mathrm{Orb}_x = \{g \cdot x \mid g \in G\}.$$

Le stabilisateur de x est le sous-ensemble de G,

$$\mathrm{Stab}_x = \{g \in G \mid g \cdot x = x\}.$$

C'est un sous-groupe de G.

EXEMPLE 5. Les orbites de l'action de $GO(E)$ sur E sont les cercles centrés en zéro.

PROPOSITION 6 (Formule des classes). *Pour deux éléments de X, la relation "appartenir à la même orbite", notée $\mathcal{R}_{Orb}$, est une relation d'équivalence. Par conséquent, les orbites forment une partition de X. Si X est fini et que $\{x_1, \ldots, x_n\}$ sont des représentants des orbites de X, alors,*

$$|X| = \sum_{i=1}^{n} |\mathrm{Orb}_{x_i}|.$$

PROPOSITION 7 (Une seconde formule des classes). *Soit $x \in X$ et G/Stab_x l'ensemble des classes à gauche de Stab_x sous G. Alors l'application $\overline{g} \mapsto g \cdot x$ de G/Stab_x dans Orb_x est une bijection. En particulier, si G est fini,*

$$|G| = |\mathrm{Orb}_x| \cdot |\mathrm{Stab}_x|.$$

DÉFINITION 8 (Différents types d'actions). Une action de G sur X est dite

- *transitive*, si elle n'a qu'une seule orbite,
- *fidèle*, si le morphisme $\varphi : G \to \mathfrak{S}(X)$ est injectif,
- *simple*, si pour tout $g \in G$ et tout $x \in X$, $(g \cdot x = x) \implies (g = e)$ où e est l'élément neutre de G.

EXEMPLE 9. Tout groupe G agit sur lui-même par translation à gauche, c'est-à-dire via $g \cdot h = gh$ pour tout $g, h \in G$. Cette action est simple, transitive (on dit simplement transitive) et fidèle.

On en déduit le

THÉORÈME 10. *(Cayley) Tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

EXEMPLE 11. Tout groupe G agit sur lui-même par automorphisme intérieur, $g \cdot h = ghg^{-1}$ pour tout $g, h \in G$. Les orbites de cette action sont appelée *classes de conjugaison*. Le stabilisateur d'un élément $h \in G$ est appelé *centralisateur* de h,

$$\mathrm{Stab}_h = \{g \in G \mid gh = hg\}.$$

EXEMPLE 12. De la même manière, tout groupe G agit sur l'ensemble de ses sous-groupes par conjugaison en posant pour $H < G$ et $g \in G$,

$$g \cdot H = gHg^{-1}.$$

Le stabilisateur de H, noté $N_G(H)$ est appelé *normalisateur* de H. On a $H \triangleleft N_G(H)$ et $N_G(H)$ est le plus grand sous-groupe ayant cette propriété.

Proposition 13. *Si G agit sur X, alors les stabilisateurs des éléments d'une même orbite sont conjugués. Plus précisément, si $x \in X$,*

$$\mathrm{Stab}_{g\cdot x} = g\,\mathrm{Stab}_x\, g^{-1}, \quad \forall g \in G.$$

2. Application au groupe symétrique

Proposition 14. *Soit $n \in \mathbb{N}$. Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en produit de cycles disjoints. Cette décomposition est unique à l'ordre près des facteurs.*

Exemple 15. La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 8 & 7 & 6 & 5 & 1 & 2 & 3 \end{pmatrix}$ se décompose en $\sigma = (1\ 4\ 7)(2\ 9\ 3\ 8)(5\ 6)$.

Proposition 16 (Conjugaison dans le groupe symétrique)**.**

1. *Si $\sigma \in \mathfrak{S}_n$ est un k-cycle, $\sigma = (a_1, \dots, a_k)$, alors pour toute permutation $\tau \in \mathfrak{S}_n$,*
$$\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_k)).$$
2. *Dans $\mathfrak{S}_n$, tout les k-cycles sont conjugués.*
3. *Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

3. Classification dans les espaces de matrices

Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Étant donné une base de E, on identifie $GL(E)$ à $GL_n(\mathbb{K})$ via l'isomorphisme canonique.

Exemple 17. $GL_n(\mathbb{K})$ agit sur lui-même par similitude, c'est-à-dire,

$$P \cdot A = P^{-1}AP, \quad \forall P, A \in GL_n(\mathbb{K}).$$

Deux matrices sont dans la même orbite pour cette action si et seulement si elles sont semblables.

Théorème 18 (Spectral)**.** *Le groupe orthogonal $GO_n(\mathbb{R})$ agit sur $S_n(\mathbb{R})$ par similitude et chaque orbite contient une matrice diagonale. Ces orbites sont caractérisées par les valeurs propres (comptées avec multiplicité) des matrices qui les composent.*

Théorème 19 (Théorème du rang)**.** *Soient m et n deux entiers. $GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$ agit sur $\mathcal{M}_{m\times n}(\mathbb{K})$ par équivalence, c'est-à-dire,*

$$(A, B) \cdot M = A^{-1}MB, \quad A, B \in GL_m(\mathbb{K}) \times GL_n(\mathbb{K}),\ M \in \mathcal{M}_{m\times n}(\mathbb{K}),$$

et chaque orbite pour cette action contient un représentant de la forme,

$$\left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & 0 \end{array}\right).$$

L'entier k est le rang de chaque matrice de l'orbite.

Théorème 20 (Sylvester)**.** *$GL_n(\mathbb{R})$ agit sur $S_n(\mathbb{R})$ par congruence, c'est-à-dire,*

$$P \cdot A = {}^tPAP, \quad \forall P \in GL_n(\mathbb{R}),\ \forall A \in S_n(\mathbb{R}),$$

et chaque orbite contient un représentant de la forme,

$$\begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0_{n-r} \end{pmatrix},$$

où $r = p + q$ est le rang des matrices de cette orbite. Le couple (p, q) est appelé la signature de ces matrices.

4. Application aux corps finis

Dans cette section, q est un nombre premier et n est un entier quelconque.

Proposition 21. *On note $G_{k,n}$ l'ensemble des sous-espaces vectoriels de dimension k de $\mathbb{F}_q^n$. $GL_n(\mathbb{F}_q)$ agit naturellement sur $G_{k,n}$ et l'étude de cette action donne,*

$$|G_{k,n}| = \frac{(q^n - 1)\cdots(q^{n-k+1} - 1)}{(q^k - 1)\cdots(q - 1)}.$$

Proposition 22. *Le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est,*

$$\sum_{n_1+\cdots+n_q=n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}.$$

Théorème 23 (Wedderburn)**.** *Tout corps fini est commutatif.*

5. Application à la combinatoire

Proposition 24 (Formule de Burnside)**.** *Soit G un groupe d'ordre n agissant sur un ensemble X. Pour tout $g \in G$, on note $\mathrm{Fix}(g)$ l'ensemble des points fixes de g,*

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

Le nombre d'orbites de cette action est égal à la moyenne arithmétique du nombre de points fixes de g, g parcourant G,

$$|G/\mathcal{R}_{Orb}| = \frac{1}{n} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Application 25. On dispose d'un fil circulaire, de quatre perles rouges, trois bleues et trois blanches. Il est alors possible de réaliser 76 colliers différents.

6. Application en théorie des groupes

Soit p un nombre premier.

Lemme 26. *Soit G un p-groupe agissant sur X et $\mathrm{Fix}(G)$ l'ensemble des points fixes de X sous G,*

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

Alors $|X| \equiv |\mathrm{Fix}(G)| \mod p$.

Proposition 27. *Le centre d'un p-groupe non trivial est non trivial.*

Corollaire 28. *Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Exemple 29. Le corollaire n'est plus vrai pour les groupes d'ordre p^3. En effet, l'ensemble $T_3(\mathbb{F}_p)$ des matrices triangulaires supérieures de taille 3 avec des 1 sur la diagonale n'est pas abélien.

Théorème 30 (Cauchy)**.** *Soit G un groupe fini et p un diviseur premier de $|G|$. Alors G contient au moins un élément d'ordre p.*

Définition 31. Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. On appelle p-Sylow de G tout sous-groupe d'ordre p^α.

Exemple 32. Soit $n = p^\alpha m$ avec $p \nmid m$. Alors $\mathbb{Z}/n\mathbb{Z}$ a un unique p-Sylow donné par $< m >$.

L'ensemble $T_n(\mathbb{F}_p)$ des matrices triangulaires supérieures de taille n avec des 1 sur la diagonale est un p-Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 33. *Soit G d'ordre $p^\alpha m$, $p \nmid m$, S un p-Sylow de G et H un sous-groupe de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Théorème 34 (Sylow)**.** *Soit G d'ordre $n = p^\alpha m$, $p \nmid m$. Alors,*

1. *G admet un p-Sylow,*
2. *tout sous-groupe H de G qui est un p-groupe est inclu dans un p-Sylow,*
3. *les p-Sylow sont tous conjugués (donc leur nombre k divise n),*
4. *on a $k \equiv 1 \mod p$ (donc k divise m).*

Corollaire 35. *Si S est un p-Sylow de G, alors S est distingué dans G si et seulement si S est l'unique p-Sylow de G.*

Application 36. Les groupes d'ordre 63 et 255 ne sont pas simples.

7. Application aux groupes de symétrie

Dans ce qui suit, $\mathbb{A}_n(\mathbb{R})$ est un espace affine dirigé par $\mathbb{R}^n$.

Définition 37. Soit X une partie de $\mathbb{A}_n(\mathbb{R})$. Le *groupe d'isométries* de X, noté $\mathrm{Is}(X)$, est l'ensemble des transformations affines qui laissent X globalement invariant. Il s'agit bien d'un sous-groupe de $GA_n(\mathbb{R})$. Le sous-groupe des transformations de $\mathrm{Is}(X)$ de déterminant 1, noté $\mathrm{Is}^+(X)$, est appelé le *groupe des déplacements* de X.

Exemple 38. Le groupe diédral $D_n := \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est le groupe d'isométries d'un polygone régulier à n côtés.

Lemme 39. *Le groupe d'isométrie d'un ensemble convexe laisse stable ses points extrémaux.*

Proposition 40. *Le groupe d'isométries du tétraèdre Δ_4 est isomorphe à $\mathfrak{S}_4$. Son groupe des déplacements est $\mathfrak{A}_4$ donc*

$$\mathrm{Is}(\Delta_4) = \mathfrak{S}_4 = \mathfrak{A}_4 \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Proposition 41. *Le groupe des déplacements du cube C_6 est isomorphe à $\mathfrak{S}_4$ et son groupe d'isométries est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.*