101 - Groupe opérant sur un ensemble. Exemples et Applications.

Version élémentaire

1 Généralités sur les actions de groupes

1.1 Définitions et énoncés généraux

Définition 1.1. *Soit G un groupe et X un ensemble. Une action (à gauche) de G sur X est la donnée d'un morphisme de groupes $\rho : G \to \mathfrak{S}(X)$, où $\mathfrak{S}(X)$ désigne le groupe des bijections (permutations) de l'ensemble X.*

Remarque 1.2. Cette définition équivaut à la donnée d'une application $G \times X \to X$ notée $(g, x) \mapsto g \cdot x$, vérifiant
- pour tout $x \in X$, $1 \cdot x = x$.
- pour tout $g, g' \in G$ et $x \in X$, $(gg') \cdot x = g \cdot (g' \cdot x)$.

Exemples :
- Le groupe G agit sur lui-même par translation : $g \cdot x = gx$; par conjugaison : $g \cdot x = gxg^{-1}$.
- Si H est un sous-groupe de G, G agit naturellement sur l'ensemble $X := G/H$ des classes à gauche de H dans G via $g \cdot (g'H) := (gg')H$.
- Le groupe $\mathfrak{S}_n$ agit naturellement sur l'ensemble $\{1, \dots, n\}$.
- Si K est un corps et V un K-espace vectoriel, $\mathrm{GL}(V) \subset \mathfrak{S}(V)$ agit sur V.

On dispose d'une relation d'équivalence naturellement associée à une action de groupe : si $x, x' \in X$, on dit que x et x' sont équivalents s'il existe $g \in G$ tel que $x' = g \cdot x$.

Définition 1.3. *Soit X un ensemble muni d'une action d'un groupe G.*

1. *les orbites pour cette action sont les classes d'équivalence associées. Pour tout $x \in X$, on note $\mathcal{O}(x)$ l'orbite de x sous G. On note X/G l'ensemble des orbites.*
2. *pour tout $x \in X$, $G_x := \{g \in G : g \cdot x = x\}$ est un sous-groupe de G appelé stabilisateur.*
3. *pour tout $g \in G$, on note $\mathrm{Fix}_X(g) := \{x \in X : g \cdot x = x\}$, appelé le fixateur de g.*
4. *l'action est dite fidèle (resp. libre) si le morphisme ρ est injectif (resp. si tous les stabilisateurs sont réduits à $\{1\}$).*
5. *on dit que l'action est transitive si pour tout $(x, y) \in X^2$, il existe $g \in G$ tel que $g \cdot x = y$.*
6. *on note $X^G := \{x \in X : \forall g \in G, g \cdot x = x\}$ l'ensemble des points fixes de G dans X.*

Exemples :
- l'action par translation de G sur lui-même est libre, donc fidèle, et elle est transitive.
- l'action par conjugaison de G sur lui-même est fidèle ssi le centre de G est trivial. Cette action est libre (resp. transitive) ssi $G = \{1\}$. Les orbites sont les classes de conjugaison.
- l'action de $\mathfrak{S}_n$ sur $\{1, \dots, n\}$ est fidèle et transitive.
- l'action de $\mathrm{GL}(V)$ sur V est fidèle. Elle est transitive si et seulement si $V = \{0\}$. Sinon, cette action a exactement deux orbites : $\{0\}$ et $V \setminus \{0\}$.

Proposition 1.4. *Soit X un ensemble muni d'une action d'un groupe G. Alors pour tout $x \in X$ et $g \in G$, $G_{g \cdot x} = gG_xg^{-1}$ et on a une bijection $G/G_x \xrightarrow{\sim} \mathcal{O}(x)$.*

Exemple : On a une bijection $\mathfrak{S}_n/\mathfrak{S}_{n-1} \xrightarrow{\sim} \{1 \dots, n\}$, donnée par l'action de $\mathfrak{S}_n$ sur l'élément n.

1.2 Actions d'un groupe fini sur un ensemble fini

Proposition 1.5. *Soit X un ensemble fini muni d'une action d'un groupe fini G.*

1. *(équation aux classes)* $|X| = \sum_{\omega \in X/G} |\omega| = \sum_{\mathcal{O}(x) \in X/G} \frac{|G|}{|G_x|}$.
2. *(formule de Burnside)* $|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|$.

Remarque 1.6. L'égalité 2 dit que le nombre moyen de points fixes d'un élément de G est le nombre d'orbites. Ainsi une permutation aléatoire de $\mathfrak{S}_n$ a-t-elle en moyenne un point fixe.

Exemple : Si G agit sur lui-même par conjugaison, on obtient la relation

$$|G| = |Z(G)| + \sum_{g \in C_G \setminus Z(G)} \frac{|G|}{|Z_G(g)|},$$

où $C_G \subset G$ est un ensemble de représentants des classes de conjugaison, $Z_G(g)$ est le centralisateur de g et $Z(G)$ est le centre de G.

Une application classique de l'équation aux classes (pour l'action des inversibles d'un corps par conjugaison) :

Théorème 1.7 (*). *(Wedderburn) Une algèbre à division finie est un corps.*

2 Applications à la théorie des groupes

2.1 Groupe symétrique

Proposition 2.1. *(Cayley)*

Soit G un groupe fini. Il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{S}_n$.

En utilisant l'action de $\mathfrak{S}_n$ sur $X = \{1, \dots, n\}$, on montre :

Théorème 2.2. *Tout permutation de $\mathfrak{S}_n$ s'écrit de façon unique (à l'ordre près) comme produit de cycles à supports disjoints.*

Soit K un corps, on définit l'action de $\mathfrak{S}_n$ sur la K-algèbre $K[X_1, \dots, X_n]$ par $\sigma \cdot X_i := X_{\sigma(i)}$. Un polynôme P est dit symétrique si pour tout $\sigma \in \mathfrak{S}_n$, $\sigma \cdot P = P$. On note $\sigma_1, \dots, \sigma_n \in K[X_1, \dots, X_n]$ les polynômes symétriques élémentaires.

Théorème 2.3 (*). *Soit $P \in K[X_1, \dots, X_n]$. Si P est symétrique, il existe un unique $Q \in K[X_1, \dots, X_n]$ tel que $P = Q(\sigma_1, \dots, \sigma_n)$.*

2.2 Structure des groupes finis

Lemme 2.4 (*). *Soit G un groupe de cardinal p^n (un p-groupe), où p est un nombre premier, agissant sur un ensemble fini X. Alors $|X^G| \equiv |X| \pmod p$.*

En considérant une action de $\mathbb{Z}/p\mathbb{Z}$, on montre :

Théorème 2.5 (*). *(Cauchy) Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors G contient un élément d'ordre p.*

En utilisant l'équation aux classes pour l'action de G sur lui-même par conjugaison :

Proposition 2.6 (*). *Soit G un p-groupe, où p est un nombre premier. Alors le centre de G est non trivial. En particulier, le groupe G est nilpotent.*

Proposition 2.7 (*). *Soit G un groupe fini et p le plus petit nombre premier divisant $|G|$. Alors tout sous-groupe de G d'indice p est distingué.*

2.3 Représentations linéaires d'un groupe

Définition 2.8. *Soit G un groupe fini. Une représentation (linéaire) de G est un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie.*

En particulier, une représentation d'un groupe G est une action (linéaire) de G sur V, i.e. un morphisme $\rho' : G \to \mathfrak{S}(V)$.

Définition 2.9. *Soit (V, ρ) une représentation d'un groupe fini G.*
- *Si (V', ρ') est une autre représentation de G, un morphisme de représentation $\varphi : (V, \rho) \to (V', \rho')$ est une application linéaire $\varphi : V \to V'$ telle que pour tout $g \in G$, $\rho'(g) \circ \varphi = \varphi \circ \rho(g)$.*
- *Une sous-représentation de (V, ρ) est un sous-espace vectoriel W de V stable par $\rho(g)$, pour tout $g \in G$.*
- *La représentation (V, ρ) est dite irréductible si elle n'admet pas de sous-représentation non triviale.*
- *Le caractère de la représentation (V, ρ) est la fonction $\chi_V : G \to \mathbb{C}$ définie par $\chi_V(g) := \mathrm{tr}(\rho(g))$.*

Théorème 2.10.
1. *Deux représentations de même caractère sont isomorphes.*
2. *(Maschke) Toute représentation de G est somme directe de sous-représentations irréductibles.*

On dispose également d'un produit scalaire canonique sur l'espace des caractères, et de relations d'orthogonalité pour les caractères de représentations irréductibles. Cela permet de construire la table des caractères irréductibles d'un groupe.

Exemples :
- (*) Tables de caractères des groupes cycliques.
- (**) Table de caractères de $\mathfrak{S}_4$, en lien avec les isométries du tétraèdre.
- (**) Tables de caractères du groupe diédral et du groupe des quaternions (d'ordre 8).

3 Applications à la géométrie

3.1 Géométrie affine

Définition 3.1. *Soit K un corps. Un espace affine sur K est un ensemble $\mathcal{E}$ muni d'une action libre et transitive du groupe additif d'un K-espace vectoriel E.*

Si on note $\mathrm{GA}(\mathcal{E})$ le groupe des transformations affines de $\mathcal{E}$, l'action de $\mathrm{GA}(\mathcal{E})$ sur $\mathcal{E}$ est transitive.

3.2 Géométrie euclidienne

Définition 3.2. *Soit $\mathcal{E}$ un espace affine euclidien de dimension n. Un polyèdre convexe P de $\mathcal{E}$ est dit régulier si le groupe des isométries de P agit transitivement sur les suites $(F_0, \ldots, F_{n-1})$, où F_i est une face de P de dimension i, avec $F_i \subset F_{i+1}$, pour tout i.*

Théorème 3.3. *Soit $\mathcal{E}$ un espace affine euclidien de dimension 3.*
- *(*) Le groupe des isométries (resp. directes) du tétraèdre est isomorphe à $\mathfrak{S}_4$ (resp. $\mathfrak{A}_4$).*
- *(**) Celui du cube ou de l'octaèdre est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathfrak{S}_4$).*

Étudions maintenant les angles et les rotations.

Définition 3.4. *Soit P un plan euclidien. Le groupe $\mathrm{SO}(P)$ agit librement et transitivement sur la sphère unité. Soient $u, v \in P$ de norme 1. La mesure de l'angle (u, v) est l'unique $\theta \in \mathbb{R}/2\pi\mathbb{Z}$ tel que $R_\theta u = v$.*

4 Applications à l'algèbre linéaire

4.1 Bases

Soit K un corps et V un K-espace vectoriel de dimension finie n. On dipose d'une action naturelle de $\mathrm{GL}(V)$ sur l'ensemble $\mathfrak{B}_V$ des bases de V. Cette action est libre et transitive.

Définition 4.1. *Si $K = \mathbb{R}$ et V est euclidien, le sous-groupe $\mathrm{SO}(V) \subset \mathrm{GL}(V)$ agit sur les bases orthonormées de V selon deux orbites, appelées orientations de V.*

4.2 Actions par translation

On peut faire agir $\mathrm{GL}_n(K)$ sur $\mathrm{Mat}_n(K)$ par translation à gauche :

Proposition 4.2 (*). *Soient $A, B \in \mathrm{Mat}_n(K)$. Alors A et B sont dans la même orbite si et seulement si A et B ont même noyau.*

Si on considère l'action par translation à droite, donnée par $P \cdot A := AP^{-1}$, on a :

Proposition 4.3 (*). *Soient $A, B \in \mathrm{Mat}_n(K)$. Alors A et B sont dans la même orbite si et seulement si A et B ont même image.*

4.3 Matrices semblables, matrices équivalentes

On considère l'action de $\mathrm{GL}_n(K)\times\mathrm{GL}_p(K)$ sur $\mathrm{Mat}_{n,p}(K)$ donnée par $(P,Q)\cdot M := PMQ^{-1}$ (équivalence des matrices), et l'action de $\mathrm{GL}_n(K)$ sur $\mathrm{Mat}_n(K)$ donnée par $P\cdot M := PMP^{-1}$ (similitude des matrices).

Théorème 4.4 (**)**.** *Soit K un corps. Alors les classes d'équivalence de matrices dans $\mathrm{Mat}_{n,p}(K)$ sont données par le rang : pour tout $M \in \mathrm{Mat}_{n,p}(K)$, il existe un unique $0 \leq r \leq \min(n,p)$ tel que M est équivalente à la matrice* $\begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$.

Remarque 4.5. Cet énoncé est essentiellement équivalent à l'algorithme du pivot de Gauss pour la résolution des systèmes linéaires.

Remarque 4.6. De même, la classification des formes quadratiques sur un corps K peut s'interpréter comme la description des orbites pour l'action de $\mathrm{GL}_n(K)$ sur les matrices symétriques $\mathrm{Sym}_n(K)$ définie par $A\cdot M := AM{}^tA$.

Exemples :
- Si $K=\mathbb{C}$, l'action de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathrm{Sym}_n(\mathbb{C})$ a exactement $n+1$ orbites données par le rang $0\leq r\leq n$.
- (Sylvester) Si $K=\mathbb{R}$, l'action de $\mathrm{GL}_n(\mathbb{R})$ sur $\mathrm{Sym}_n(\mathbb{R})$ a exactement $\frac{(n+1)(n+2)}{2}$ orbites données par la signature $(p,q)\in\mathbb{N}^2$ avec $p+q\leq n$.

5 Applications en combinatoire

5.1 Colliers de perles

On cherche à dénombrer les colliers à 9 perles dont 4 bleues, 3 blanches et 2 rouges. En utilisant une action du groupe diédral D_9, on trouve qu'il y a exactement 76 tels colliers (*).

5.2 Coloriage de polyèdres

On dénombre les coloriages des faces d'un polyèdre avec n couleurs (à rotation près).

Exemple :(**) Il y a exactement $N = \frac{n^6+3n^4+12n^3+8n^2}{24}$ coloriages des faces du cubes avec (au plus) n couleurs (à rotation près). En particulier, pour $n=3$ couleurs, on trouve $N=57$ coloriages.