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

Version ambitieuse

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 $g \cdot (g'H) := (gg')H$.
- Pour tout ensemble X, le groupe $\mathfrak{S}(X)$ agit naturellement sur X, via $\sigma \cdot x := \sigma(x)$.
- 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. *soit $n \geq 1$. On dit que l'action est n-transitive si pour tout $(x_1, \dots x_n, y_1, \dots, y_n) \in X^{2n}$ tels que $x_i \neq x_j$ et $y_i \neq y_j$ pour tout $i \neq j$, il existe $g \in G$ tel que $g \cdot x_i = y_i$ pour tout i.*
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 $\mathfrak{S}(X)$ sur X 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 $g \in G$, $G_{g \cdot x} = gG_x g^{-1}$ et on a une bijection G-équivariante $G/G_x \xrightarrow{\sim} \mathcal{O}(x)$.*

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 les relations suivantes :
- $|G| = |Z(G)| + \sum_{g \in C_G \setminus Z(G)} \frac{|G|}{|Z_G(g)|}$, 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.
- $|C_G| = \frac{1}{|G|} \sum_{g \in G} |Z_G(g)|$.

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. *Soit G un groupe fini.*

1. *(Cayley) Il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{S}_n$ (avec $n \leq |G|$).*
2. *Pour tout corps K, il existe n tel que G soit un sous-groupe de $\mathrm{GL}_n(K)$.*

Conséquence : Un groupe d'ordre $2m$, avec m impair, n'est pas un groupe simple.

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.*

Proposition 2.3 (**). *Soit $H \subset \mathfrak{S}_n$ un sous-groupe d'indice $2 \leq k \leq n$. Alors soit $k = 2$ et $H = \mathfrak{A}_n$, soit $k = n$ et H est isomorphe à $\mathfrak{S}_{n-1}$.*

Soit A un anneau commutatif, on définit l'action de $\mathfrak{S}_n$ sur la A-algèbre $A[X_1, \dots, X_n]$ 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 $\sigma_1, \dots, \sigma_n \in A[X_1, \dots, X_n]$ les polynômes symétriques élémentaires.

Théorème 2.4 (**). *Le morphisme de A-algèbres $A[Y_1, \dots, Y_n] \to A[X_1, \dots X_n]$ défini par $Y_i \mapsto \sigma_i(X_1, \dots X_n)$ est injectif d'image $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$: tout polynôme symétrique s'écrit de façon unique comme un polynôme en les polynômes symétriques élémentaires.*

2.2 Résultats simples de structure des groupes finis

Lemme 2.5. *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 2.6 (*). *(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 2.7. *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 2.8 (*). *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 Théorèmes de Sylow

En utilisant le théorème de Cayley et l'action de G par conjugaison, on montre :

Théorème 2.9 (***). *Soit G un groupe fini de cardinal $n = p^\alpha m$, avec $(m, p) = 1$.*

1. *Il existe un sous-groupe de G de cardinal p^α, appelé un p-sous-groupe de Sylow de G.*
2. *Tout p-sous-groupe de G est contenu dans un p-Sylow de G.*
3. *Si S et T sont deux p-Sylow de G, alors il existe $g \in G$ tel que $T = gSg^{-1}$.*
4. *Si n_p désigne le nombre de p-Sylow de G, alors n_p divise m et $n_p \equiv 1 \pmod p$.*

Conséquences :
- Un groupe d'ordre < 60 n'est pas simple.
- (**) $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60.
- (***) Si G est un groupe fini simple non cyclique, alors soit son cardinal est divisible par 12, soit le plus petit facteur premier de son cardinal apparaît au moins au cube dans la décomposition en facteurs premiers.
- Un groupe d'ordre $60 < . < 168$ n'est pas simple.
- (***) $\mathrm{SL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ est l'unique groupe simple d'ordre 168.

2.4 Produit semi-direct

Définition 2.10. *Soit N, H deux groupes, et $\rho : H \to \mathrm{Aut}(N)$ un morphisme de groupes. On définit $G := N \rtimes_\rho H$ comme l'ensemble $N \times H$ muni de la loi de composition interne $(n, h) \cdot (n', h') := (n\rho(h)(n'), hh')$. Alors G est un groupe, le produit semi-direct de H par N.*

Exemples : Le groupe diédral D_n des isométries du polygone régulier à n côtés est isomorphe à $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Le groupe $\mathfrak{S}_3$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.
Conséquences :
- (***) classification des groupes d'ordre ≤ 15.
- (***) classification des groupes d'ordre pq, p^3, avec p et q premiers.
- description du groupe affine d'un espace affine.

2.5 Représentations linéaires d'un groupe

Par définition, une représentation linéaire d'un groupe G dans un K-espace vectoriel V est une action (linéaire) de G sur V, i.e. un morphisme $\rho : G \to \mathrm{GL}(V)$.
Exemples :
- Toute représentation complexe est somme directe de représentations irréductibles.
- (**/***) Table de caractères de $\mathfrak{S}_4$ (resp. $\mathfrak{A}_5$) en lien avec les isométries du tétraèdre (resp. du dodécaèdre).
- (***) Tout groupe fini d'ordre $p^\alpha q^\beta$, avec p et q premiers, est résoluble (Burnside).
- (**) Tout sous-groupe compact maximal de $\mathrm{GL}_n(\mathbb{R})$ est conjugué à $\mathcal{O}_n(\mathbb{R})$.

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. Le choix d'un point de $\mathcal{E}$ induit un isomorphisme $\mathrm{GA}(\mathcal{E}) \cong E \rtimes \mathrm{GL}(E)$.

3.2 Géométrie projective

Si K est un corps et V un K-espace vectoriel, on a l'action naturelle de $\mathrm{PGL}(V)$ sur $\mathbb{P}(V)$.

Théorème 3.2 (**). *On note $n := \dim(V)$.*
L'action de $\mathrm{PGL}(V)$ sur $\mathbb{P}(V)$ est libre et n-transitive. Elle n'est pas $(n+1)$-transitive.
Si $n = 2$, on a une bijection naturelle (appelée birapport) entre l'ensemble des orbites de $\mathrm{PGL}(V)$ dans l'ensemble des quadruplets de points distincts de $\mathbb{P}(V)$ et $K \setminus \{0; 1\}$.

En utilisant la 2-transitivité de cette action, on montre (méthode d'Iwasawa) :

Théorème 3.3 (**). *Le groupe $\mathrm{PSL}(V)$ est simple, sauf si $\dim(V) = 2$ et $|K| = 2$ ou 3.*

Théorème 3.4 (**). *(Isomorphismes exceptionnels) On a des isomorphismes canoniques de groupes : $\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$, $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$, $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$, $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.*

3.3 Géométrie euclidienne

Définition 3.5. *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 $(F_0, \dots, F_{n-1})$, où F_i est une face de P de dimension i, avec $F_i \subset F_{i+1}$, pour tout i.*

Théorème 3.6. *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. $\mathfrak{S}_4$).*
- *(***) Celui du dodécaèdre ou de l'icosaèdre est isomorphe à $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathfrak{A}_5$).*

Réciproquement, on dispose de la classification des sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$:

Théorème 3.7 (**). *Soit $\mathcal{E}$ un espace affine euclidien de dimension 3. Soit $G \subset \mathrm{Isom}^+(\mathcal{E})$ un sous-groupe fini. Alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, D_n, $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$.*

Définition 3.8. *Soit $\mathcal{E}$ un espace affine euclidien. Un pavage de $\mathcal{E}$ est un couple $(\mathcal{P}, G)$, où $\mathcal{P} \subset \mathcal{E}$ est compact connexe d'intérieur non vide et $G \subset \mathrm{Isom}^+(\mathcal{E})$ est un sous-groupe tel que*

1. *$\mathcal{E} = \bigcup_{g \in G} g(\mathcal{P})$.*
2. *pour tous $g, h \in G$, $g(\mathcal{P}) \cap h(\mathcal{P}) \neq \emptyset \implies g = h$.*

Proposition 3.9 (**). *À conjugaison près dans $\mathrm{GA}(\mathcal{E})$, il y a exactement cinq tels sous-groupes G. Si on remplace $\mathrm{Isom}^+(E)$ par $\mathrm{Isom}(\mathcal{E})$, on trouve 17 sous-groupes convenables.*

Étudions maintenant les angles et les rotations.

Définition 3.10. *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 $R_\theta u = v$.*

L'action du groupe $\mathbb{U}$ des nombres complexes de module 1 sur $\mathbb{R}^2$ permet d'identifier $\mathbb{U} \cong \mathrm{SO}_2(\mathbb{R})$. On note $\mathbb{H}$ la $\mathbb{R}$-algèbre des quaternions et $G \subset \mathbb{H}^\times$ le groupe des quaternions de norme 1. Alors, en considérant l'action de $\mathbb{H}^\times$ sur $\mathbb{H}$ par conjugaison, on obtient :

Théorème 3.11 (**). *On a des isomorphismes canoniques : $G/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}_3(\mathbb{R})$ et $(G \times G)/\{\pm(1,1)\} \xrightarrow{\sim} \mathrm{SO}_4(\mathbb{R})$.*

3.4 Géométrie hyperbolique

On note $\mathcal{H} := \{z \in \mathbb{C} : \mathfrak{Im}(z) > 0\}$. On dispose d'une action transitive de $\mathrm{PSL}_2(\mathbb{R})$ sur $\mathcal{H}$ par homographies, via la formule $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}$; on en déduit $\mathcal{H} \cong \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$.

Théorème 3.12 (**). *L'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathcal{H}$ admet pour domaine fondamental l'ensemble $\mathcal{D} := \{z \in \mathbb{C} : |z| \geq 1 \text{ et } |\mathfrak{Re}(z)| \leq \frac{1}{2}\}$.*

Remarque 3.13. Le quotient $\mathcal{H}/\mathrm{PSL}_2(\mathbb{Z})$ (et donc le domaine fondamental $\mathcal{D}$) est lié également à la classification des réseaux de $\mathbb{R}^2$.

Corollaire 3.14 (**). $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*

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

Le groupe $\mathrm{GL}(V)$ (resp. $\mathrm{GL}(U)$) agit sur $\mathrm{Hom}_K(U, V)$ par translation à gauche (resp. à droite). Les orbites sont caractérisées par le noyau (resp. l'image) des applications linéaires.

4.3 Matrices semblables, matrices équivalentes

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

Théorème 4.2. *Soit A un anneau principal. On note $r := \min(n, p)$.*

Alors les classes d'équivalence de matrices dans $\mathrm{Mat}_{n,p}(A)$ sont données par les facteurs invariants : pour tout $M \in \mathrm{Mat}_n(A)$, il existe $d_1, \ldots, d_r \in A$ (uniques modulo $A^\times$) tels que $d_i | d_{i+1}$ pour tout i et M est équivalente à $\mathrm{diag}(d_1, \ldots, d_r)$.

Remarque 4.3. En particulier, si A est un corps, les classes d'équivalence sont caractérisées par le rang des matrices (il y en a donc exactement $n + 1$).

Théorème 4.4. *Soit K un corps. Alors les classes de similitudes de matrices dans $\mathrm{Mat}_n(K)$ sont données par les invariants de similitude : pour tout $M \in \mathrm{Mat}_n(K)$, il existe des polynômes unitaires (uniques) $P_1, \ldots, P_r \in K[X]$ tels que $P_i | P_{i+1}$ pour tout i et M soit semblable à $\mathrm{diag}(C(P_1), \ldots, C(P_r))$ (où $C(P)$ désigne la matrice compagnon de P).*

Remarque 4.5. 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 $A \cdot M := AM^tA$.

4.4 Décomposition de Bruhat et action sur les drapeaux

Si K est un corps, $\mathrm{GL}_n(K)$ agit transitivement sur l'ensemble $\mathcal{D}$ des drapeaux de K^n.

Théorème 4.6 (**). *(Bruhat) Soit K un corps. Notons T (resp. U) le sous-groupe de $\mathrm{GL}_n(K)$ formé des matrices triangulaires supérieures (resp. unipotentes supérieures). Alors*

$$\mathrm{GL}_n(K) = \bigsqcup_{\sigma \in \mathfrak{S}_n} UP_\sigma T\,.$$

Décrivons les orbites de l'action de $\mathrm{GL}_n(K)$ sur les paires de drapeaux :

Corollaire 4.7 (**). *On a une bijection canonique $(\mathcal{D} \times \mathcal{D})/\mathrm{GL}_n(K) \xrightarrow{\sim} \mathfrak{S}_n$. En particulier, cette action a exactement $n!$ orbites.*

5 Applications en combinatoire et en arithmétique

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).

Théorème 5.1 (**). *Soit X un ensemble fini muni d'une action d'un groupe fini G. Soit $C = \{1, \ldots, n\}$ l'ensemble des couleurs. Un coloriage de X (avec au plus n couleurs) est un élément de C^X.*
Alors le nombre de coloriages de X (modulo G) est exactement $N = \frac{1}{|G|} \sum_{\sigma \in G} n^{\lambda(\sigma)}$, où $\lambda(\sigma)$ est le nombre de cycles de σ vu comme permutation de X.

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).

Remarque 5.2. Ce théorème est un cas particulier du théorème de Polyà.

5.3 Théorème des deux carrés

Soit p un nombre premier, $p \equiv 1 \pmod 4$. En munissant $X := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ d'une action de $\mathbb{Z}/2\mathbb{Z}$, on montre facilement que p est somme de deux carrés d'entiers.