101 | A réécrire |

Groupe opérant sur un ensemble
Exemples et applications

I Généralités

1) Définitions

Déf : Soit $(G,*)$ un groupe et X un ensemble.
Une action à gauche de G sur X est la donnée d'un de ces deux énoncés équivalents :
- d'un morphisme de groupes φ de G dans $\mathfrak{S}(X)$ où $\mathfrak{S}(X)$ est l'ensemble des bijections de X dans X.
- d'une application $\cdot \left(\begin{array}{l} G \times X \to X \\ (g,x) \mapsto g\cdot x \end{array}\right)$ vérifiant : $1_G \cdot x = x$ ($\forall x \in X$) et $g\cdot(g'\cdot x) = (gg')\cdot x$ $\forall x \in X$, $\forall g, g' \in G^2$

Rq : Dans cette leçon, on parlera que d'action à gauche.

Déf : Soit $x \in X$
Le sous-groupe de G $\mathcal{S}(x) := \{g \in G / g\cdot x = x\}$ est appelé le stabilisateur de x.
Le sous-ensemble de X $G(x) := \{g\cdot x / g \in G\}$ est appelé l'orbite de X.

Propé : On définit une relation d'équivalence R sur X par $x R y$ si et ssi $\exists g \in G$ tel que $g\cdot x = y$
Alors la classe d'équivalence de $x \in X$ pour R est $G(x)$
Alors $X = \coprod_{x \in X/R} G(x)$

Déf : Soit une action $\cdot$ de G sur X. Pour $g \in G$, on pose $\varphi_g \left(\begin{array}{l} X \to X \\ x \mapsto g\cdot x \end{array}\right)$ et $\varphi \left(\begin{array}{l} G \to \mathfrak{S}(X) \\ g \mapsto \varphi_g \end{array}\right)$.
L'action est transitive si il existe une seule orbite i.e. $\forall (x,y) \in X^2$, $\exists g \in G$ tel que $g\cdot x = y$
L'action est fidèle si φ est injective i.e. $(\forall x \in X,\ g\cdot x = x) \Rightarrow g = 1_G$ i.e. $\bigcap_{x \in X} \mathcal{S}(x) = \{1_G\}$

2) Cas d'un groupe et d'un ensemble fini

Propo : Soit G un groupe fini et X un ensemble fini. Alors on a les égalités suivantes :

$$\boxed{\begin{array}{l} \bullet\ |X| = \sum_{x \in X/R} |G(x)| = |G| \sum_{x \in X/R} \frac{1}{|\mathcal{S}(x)|} \\ \bullet\ |G| = |G(x)| \cdot |\mathcal{S}(x)| \end{array}}$$

Rq : La 1ère égalité est appelé formule des classes

Déf : On note $Fix(g) = \{x \in X \mid g\cdot x = x\}$ pour $g \in G$
Alors on obtient la formule de Burnside :
$$|X/R| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

3) Exemples et premières applications

1) L'action par translation : G agit sur lui-même par $\forall (g,h) \in G^2$, $g\cdot h = gh$ pour tout $(G,*)$ groupe.
C'est une action transitive et même fidèle.

2) L'action par conjugaison : G agit sur lui-même par $\forall (g,h) \in G^2$. $g\cdot h = ghg^{-1}$ pour tout groupe $(G,*)$.

Appli 1) – Thm de Cayley : Soit G un groupe fini
Alors G est isomorphisme à un sous-groupe de $\mathfrak{S}_{|G|}$

Appli 2) : Classes de conjugaison : Soit G un groupe et $g \in G$
La classe de conjugaison de g est $C(g) = \{hgh^{-1} / h \in G\}$
Elles forment une partition de G.

Appli 3) : Équivalence de matrices : Soit $n \in \mathbb{N}^*$, K un corps.
Deux matrices A et B de $\mathcal{M}_n(K)$ sont semblables, si il existe $P \in GL_n(K)$ telque $A = PBP^{-1}$
"Être semblables" est une relation d'équivalence, ~~et il y a ... orbites, chacune déterminée par le rang des matrices de l'orbite.~~

II Applications en théorie des groupes et aux corps

• **Groupe d'ordre p^α et p-Sylow**

Def : Un groupe fini d'ordre p^α où p premier ($p \in \mathcal{P}$) est un p-groupe.

Lemme de Cauchy : Soit G un groupe fini et p un nombre premier tel que $p \mid |G|$. Alors $\exists a \in G$ tel que p est l'ordre de a.

Prop : Le centre d'un p-groupe est non trivial.

Un p-groupe d'ordre p^α, $\alpha \in \mathbb{N}^*$ admet un sous-groupe d'ordre p^β, $0 \leq \beta \leq \alpha - 1$.

Def : Soit G un groupe fini d'ordre $p^\alpha q$ où $p \nmid q$, $\alpha \in \mathbb{N}$ et $p \in \mathcal{P}$.
Un p-sous-groupe de Sylow de G est un sous-groupe de G d'ordre p^α.

Lemme : $|GL_n(\mathbb{F}_p)| = (p^n - 1) \cdots (p^n - p^{n-2})(p^n - p^{n-1})$

Th : Soit G un groupe fini d'ordre $p^\alpha q$, $p \nmid q$, $\alpha \in \mathbb{N}$ et $p \in \mathcal{P}$.
Alors :
- G admet au moins un p-Sylow
- les p-Sylows sont conjugués et si n_p est leur nombre, alors $n_p \equiv 1 \, [p]$ et $n_p \mid q$.

De plus, si $n_p = 1$, le p-Sylow de G est alors distingué.

Rq : Fournit un critère de non-simplicité.

Prop : Soit G un groupe infini et $H < G$ tq $H \neq G$ et d'indice fini. Alors G n'est pas simple.

• **Autres applications et exemples**

Def : Soient H et K deux groupes tel que K agit sur H via le morphisme $\varphi : K \to \mathcal{S}(H)$ tel que $\varphi(k)$ morphisme $\forall k$.
On peut munir $G = H \times K$ d'une loi $\times$ définie par $(h,k) \times (h',k') = (h\varphi_k(h'), kk')$ pour tout h, h', k, k'.
Alors $(G, \times)$ est un groupe appelé produit semi-direct associé à l'action de K sur H noté $H \rtimes_\varphi K$

Ex : $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

DEV 1 — Théorème de Wedderburn —

$\boxed{\text{Tout anneau dans lequel tout élément non nul est inversible qui est fini est commutatif}}$

Lemme : $X^n - 1 \mid X^m - 1 \iff n \mid m$

(• **Action de $\mathcal{S}_n$ sur les polynômes**) A éviter peut-être

Def : Soit K un corps et $X_1, \ldots, X_n$ n indéterminées.
Alors on définit l'action $\left(\begin{array}{l} \mathcal{S}_n \times K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n] \\ (\sigma, P(X_1, \ldots, X_n)) \mapsto P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \end{array} \right)$
Un polynôme est symétrique si $\forall \sigma \in \mathcal{S}_n$, $\sigma \cdot P = P$

Ex : XY ou $X+Y+Z$ sont symétriques

Def : Les polynômes symétriques sont (σ_i), $1 \leq i \leq n$ où
$\sigma_i = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}$

Th : Pour $P \in K[X_1, \ldots, X_n]$ symétrique, $\exists ! \, Q \in K[X_1, \ldots, X_n]$ tel que $P(X_1, \ldots, X_n) = Q(\sigma_1, \ldots, \sigma_n)$.

III Autres exemples et applications

1) En géométrie

→ On a vu que les isométries laissant invariants les polygones réguliers à n côtés (le groupe D_n) peuvent être construits via le produit semi-direct.

Prop : Soit un tétraèdre régulier $A_1A_2A_3A_4$, $X = \{A_1, A_2, A_3, A_4\}$ et G le groupe des isométries préservant $A_1A_2A_3A_4$.
Soit $\varphi \left(\begin{array}{l} G \to \mathcal{S}_4 \\ f \mapsto (A_i \mapsto f(A_i)) \end{array} \right)$.
Alors φ est un isomorphisme : $G \simeq \mathcal{S}_4$

Prop : Grâce aux actions de groupes, on trouve que :
- le groupe des isométries directes laissant le tétraèdre régulier invariant est A_4
- le groupe des isométries directes laissant le cube invariant est $\mathcal{S}_4$.

(3) Rq : Puisque le cube et l'octaèdre sont duaux, le groupe des isométries directes préservant l'octaèdre est aussi isomorphe à S_4.

Th : A conjugaison près, il y a cinq types de sous-groupes finis dans $SO_3(\mathbb{R})$:

- les groupes cycliques
- les groupes diédraux
- les groupes de déplacements des polyèdres réguliers : A_4, S_4 et A_5

2) En algèbre linéaire

→ On a déjà vu la relation "être semblable" via l'action de $GL_n(K)$ sur $M_n(K)$ définie par conjugaison.

Def : On définit une action de $GL_n(K) \times GL_n(K) = G$ sur $M_n(K)$ par $G, X \longrightarrow X$, $((P,Q), M) \longmapsto PMQ^{-1}$)

Deux matrices dans la même orbite pour cette action sont dites équivalentes.

Prop : Les orbites de cette action sont caractérisées par le rang des matrices de l'orbite.

En particulier, il y a $n+1$ orbites pour cette action.

Def : On définit une action de $G_n(K)$ sur $M_n(K)$ par $\left(\begin{array}{l} G(K) \times M_n(K) \longrightarrow M_n(K) \\ (P, M) \longmapsto {}^*PMP \end{array}\right)$ où ${}^*P = {}^t\overline{P}$

Deux matrices dans la même orbite pour cette action sont dites congruentes.

Appli : classification des formes quadratiques sur K (à mettre plus ?)

Def : Soit V un $\mathbb{C}$-espace vectoriel de dimension finie n et G un groupe fini.

Une représentation de G dans V est la donnée d'une action de G dans V $\rho : G \longrightarrow GL_n(V)$

Ex : Soit V le $\mathbb{C}$-espace vectoriel de base $(e_g)_{g \in G}$ (de dim $|G|$) où $e_g(h) = \begin{cases} 1 & g = h \\ 0 & \text{sinon} \end{cases}$

La représentation régulière est définie par $\rho(g)(e_h) = \delta_{gh}$

C'est une action fidèle.

Ex : Soit V un $\mathbb{C}$-espace vectoriel de dimension n de base (e_i)

On définit la représentation par permutation comme la représentation de S_n sur V définie par $\rho(\sigma)(e_i) = e_{\sigma(i)}$

(à mettre avant)

Def : Le caractère d'une représentation ρ de G sur V est χ, la trace de ρ : $\chi(g) = Tr(\rho(g))$.

Ex : $\chi(\rho_1) = \begin{cases} 1 & \\ 0 & \text{sinon} \end{cases}$ et $\chi(\rho_p) =$ Nombre de pts fixes

DEV 2 - Décomposition de Burnside

3) En combinatoire

Pb : Coloriage du cube

Avec m couleurs, combien y-a-t-il de coloriages distincts ?

Si $C = \{c_1, \dots, c_m\}$ les couleurs et $F = \{f_1, \dots, f_6\}$ les 6 faces, un coloriage est la donnée de $\varphi : (1,6) \to C$ ~~qu'on peut ... par ... le cube~~.

Une telle symétrie est caractérisée par la position des faces dont le groupe est isomorphe à $G < S_6$ $G, X \to X$

On considère l'action de G sur $X = C^F$ par $(\sigma, f \mapsto f \circ \sigma)$

alors un coloriage est alors la donnée d'une orbite.

$$|X/R| = x = \frac{1}{|G|} \sum_{\sigma \in G} m^{\omega(\sigma)}$$ où $\omega(\sigma)$ nombre d'orbites.

Rq : On peut généraliser l'idée pour le polyèdre à n côtés

Ex : si $m=2$, $x=10$ et $m=3$, $x=57$

Rq : On peut faire un raisonnement avec les colliers : n perles, en colliers à n perles $\sim$ polyèdre régulier où on a $G \sim D_n$

Ex : cf Colliers

) Expliquer l'équivalence

) Th de Cayley + $S_n \hookrightarrow GL_n(\mathbb{F}_p)$
via ⟶ M

)

Milieu des faces du cube
=
sont de l'octaèdre

Les isométries préservent les milieux.

Réciproque en faisant l'inverse

Rq : Faire suivre
groupes - représentations - algèbres

Références

COMBES
PERRIN
PEYRE
COGNET