101 - Groupe opérant sur un ensemble. Exemples et applications

Cadre : on suppose connus l'ensemble$\mathbb{C}$ et l'exponentielle complexe.

1. Rapport du jury. — 2017 : *Dans cette leçon, il faut bien dominer les deux approches de l'action de groupe : l'approche naturelle et l'approche via le morphisme du groupe agissant vers le groupe des permutations de l'ensemble sur lequel il agit. La formule des classes et ses applications immédiates sont incontournables. Des exemples de natures différentes doivent être présentés : actions sur un ensemble fini, sur un espace vectoriel (en particulier les représentations), sur un ensemble de matrices, sur des groupes ou des anneaux. Les exemples issus de la géométrie ne manquent pas (groupes d'isométries d'un solide). S'ils le désirent, les candidats peuvent aller plus loin en décrivant les actions naturelles de PGL(2,Fq) sur la droite projective qui donnent des injections intéressantes pour q=2,3 et peuvent plus généralement en petit cardinal donner lieu à des isomorphismes de groupes. En notant que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations, ils pourront en déterminer le caractère.*

2. Généralités. —

1. *Définition et exemples.* —

- Def : action à gauche. Un groupe multiplicatif G d'élément neutre e agit/opère à gauche sur un ensemble X au travers d'une application $\Phi : G \times X \to X$ vérifiant :
  - $\forall x \in X$, $\Phi(e, x) = x$
  - $\forall g_1, g_2 \in G$ et $\forall x \in X$, $\Phi(g_1 g_2, x) = \Phi(g_1, \Phi(g_2, x))$
  - soit, en notant $\Phi(g, x) = g \cdot x$, $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
- Def : On définit de manière similaire les groupes opérant à droite.
- Exe : Les rotations dans l'espace qui préservent le cube unitaire opèrent sur le Rubik's cube.
- Exe : $\mathfrak{S}(X)$ opère sur X par $f \cdot x = f(x)$
- Exe : $GL(E)$ agit sur les droites de l'esp-vect E, en associant à f et à D, la droite $f(D)$.
- Exe : $GL_n(\mathbb{R})$ agit par application sur $\mathbb{R}^n$ et par conjugaison sur $M_n(\mathbb{R}^n)$.
- Pro : Il est équivalent de se donner un homomorphisme $\varphi : G \to \mathfrak{S}(X)$ en posant $g \cdot x = \varphi(g)(x)$
- Exe : G opère sur lui même :
  - Def : par translation à gauche. $s \cdot x = sx$
  - Def : par conjugaison. $g_1 \cdot g_2 = g_1 g_2 (g_1)^{-1}$
  - Def : action sur les classes modulo un sous-groupe (même non normal/distingué) : $(g_1, g_2 \cdot H) \mapsto (g_1 g_2) \cdot H$

2. *Définitions associées.* —

- Def : Soit $x \in X$. On définit le stabilisateur de x : $H_x = Stab(x) := g \in G \,:\, g \cdot x = x$. C'est un sous-groupe de G.
- Exe : Si G opère sur lui-même par translation, le stabilisateur de tout élément sera le singleton $\{e\}$. Si G opère par conjugaison, le stabilisateur d'un élément g sera fait du sous-groupe de G des éléments commutant avec g, c'est à dire le "Centralisateur" de g.
- Pro : Pour toute action de G sur X nous avons : $Stab(g \cdot x) = gStab(x)g^{-1}$
- *Orbite* :
  - Def : Orbite de $x \in X$, $\mathscr{O}_x = \{y \in X \,:\, \exists g \in G g \cdot x = y\}$. Il s'agit d'une classe d'équivalence pour la relation $[x \sim y] \iff [\exists g \in G, g \cdot x = y] \iff [\mathscr{O}_x = \mathscr{O}_y]$.
  - Notation équivalente : $\mathscr{O}_x = Gx$.
  - Rem : $\forall g \in G$, $\forall x \in X$, $\mathscr{O}_{\{}gx\} = \mathscr{O}_{\{}x\}$
  - Pro : $G/H_x \equiv \mathscr{O}_x$.
  - Exe : lorsque G agit sur lui-même par conjugaison, les orbites sont les classes de conjugaison.
  - Exe : Les orbites de $\mathbb{R}^n$ sous l'action naturelle de $O_n(\mathbb{R})$ sont les sphères de centre l'origine.
  - App : Décomposition d'une permutation σ en produit de cycles à supports disjoints : on construit les supports disjoints comme les orbites par l'action du groupe $< \sigma >$.
- *Opération transitive* :
  - Def : G opère "transitivement" sur X ssi $\mathscr{O}_x = X$.
  - Si G opère transitivement sur X et si $x, y \in X$ tel que $g \cdot x = y$, alors $H_y = gH_x g^{-1}$.
  - A l'inverse, si H est une sous-groupe de G, G agit transitivement sur G/H par $g \cdot xH = (gx)H$ et $Stab(eH) = H_{eH} = H$
  - Ainsi, de donner une ensemble X sur lequel G opère transitivement c'est se donner un sous-groupe de G dont lui et ses conjugués seront les Stabilisateurs.
  - Exe : le groupe des similitudes affines ($\{x \mapsto ax + b \,:\, a \neq 0\}$) agit sur une droite affine et le stabilisateur d'un point x est le sous-groupe des homothéties affines de centre x.
- *Opération fidèle* :
  - Def : G opère "fidèlement" lorsque $\forall x \in X$, $(g \cdot x = x) \iff (g = e)$. Cela équivaut à dire que φ est injective et que le seul antécédent de l'identité est e.
  - $G/Ker(\varphi)$ opère fidèlement sur X.
  - G opère transitivement sur $\mathscr{O}_x$.
  - Pro : Si $Card(X) \in \mathbb{N}$, alors transitif $\implies$ fidèle.
- Exe : une action par translation d'un groupe sur lui-même est simplement transitive. A fortiori elle est donc fidèle et le morphisme Φ est injectif sur $\mathfrak{S}(X)$.
- App : (théorème de Cayley) - Si G est fini, $(G, .)$ est isomorphe à un sous-groupe de $\mathfrak{S}(X)$
- Def : Une action est libre ssi pour tout $g \in G - \{e\}$, $\varphi(g)$ est sans points fixes.
- Pro : Si $Card(X) \in_N$, alors libre $\implies$ fidèle.
- Développement : Théorème de Cauchy par action circulaire de $\mathbb{Z}/p\mathbb{Z}$

3. *Quelques propriétés.* —

– Pro : Pour chaque $x \in X$, l'application de $G\ Stab(x) \to \mathscr{O}_x$ qui à $\dot{g}$ associe $g \cdot x$ est bijective (et bien définie). Et donc si G est fini, $Card(\mathscr{O}_x) = Card(G)/Card(Stab(x))$.
– Cor : *Formule des classes* - Si X et G sont finis, si $(x_i)_{i\in I}$ est l'ensemble des orbites sous l'action de G, $Card(X) = \Sigma_{i\in I} Card(G)/Card(Stab(x_i))$.
– Def : le "Fixé" par $g \in G$ est le sous-ensemble des $x \in X$ qui sont fixés par g, ie tels que $g \cdot x = x$. On le note $fix(g)$.
– Def : On peut aussi définir le fixateur d'une partie A de G ou de G lui-même.
– Cor : *Formule de Burnside* - Si X et G sont finis, le nombre r d'orbites différentes de X sous l'action de G est donné par : $r = \frac{1}{Card(G)} \Sigma_{g\in G} Card(fix(g))$
– Exe : YYYY Nombre de colliers de perles.
–

3. Applications. —

1. *Groupes finis.* —

– Def : un p-groupe est un groupe fini dont le cardinal est la puissance d'un nombre premier p.
– Pro : Le centre d'un p-groupe distinct de $\{1\}$ n'est pas réduit à $\{1\}$.
– Pro : Tout groupe d'ordre p^2 est abélien.
– Développement 1 : *théorèmes de Sylow*
  • Déf : On dit que G est un p-groupe si l'ordre de G est une puissance de $p \in \mathbb{P}$. Si G est d'ordre $p^n m$ avec $m \wedge p = 1$, on dit qu'un sous-groupe H de G est un p-Sylow de G si H est d'ordre p^n .
  • Rem 1 : Soit S un sous-groupe de G ; S est un p-Sylow de G si et seulement si S est un p-groupe et $(G : S)$ est premier à p.
  • Rem 2 : Tout conjugué d'un p-Sylow de G est un p-Sylow de G.
  • The 1 : Tout groupe fini possède au moins un p-Sylow.
  • Lem : Soit H un sous-groupe de G et soit S un p-Sylow de G. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ soit un p-Sylow de H.
  • Cor : Si G a des p-Sylow et si H est un sous-groupe de G, alors H a aussi des p-Sylow.
  • Soit G un groupe fini d'ordre n. On peut plonger G dans le groupe symétrique $\mathfrak{S}_n$ d'après Cayley. D'autre part, $\mathfrak{S}_n$ se plonge dans $GL_n(\mathbb{K})$ (où $\mathbb{K}$ est un corps fini de caractéristique p) : si $\sigma \in \mathfrak{S}_n$ et si $(e_i)_{1lei\leq n}$ est une base de $\mathbb{K}^n$, on associe à σ la transformation linéaire f définie par $f(e_i) = e_{\sigma(i)}$. Donc G se plonge dans $GL_n(\mathbb{K})$.
  • Il reste à montrer que $GL_n(\mathbb{K})$ a un p-Sylow. Pour cela considérons le groupe P constitué des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. C'est un sous-groupe de $GL_n(\mathbb{K})$ d'ordre $|P| = qn(n-1)/2 = pfn(n-1)/2$. Donc P est un p-Sylow de $GL_n(\mathbb{K})$.
  • The 2: Soit G un groupe de cardinal $n = p^\alpha m$ avec $p \wedge m = 1$.
    ∗ Si H est un p-groupe de G il est inclus dans un p-Sylow de G.
    ∗ Tous les p-Sylow sont conjugués entre eux.
    ∗ Le nombre de p-Sylow divise n et aussi il est congru à 1 modulo p.
  • App : quelques applications des théorèmes de Sylow
    ∗ Exo : des groupes d'ordre 63 ou 255 ne sont pas simples.
    ∗ Cor : (Cauchy comme corollaire) Si p divise l'ordre de G, alors G contient un élément d'ordre p.
    ∗ Cor : un p-Sylow est normal/distingué ssi il est le seul (puisque les autres lui sont conjugués).
    ∗ Cor : Soit p le plus petit nombre premier divisant $Card(G)$. Tout sous-groupe d'indice p est distingué.
    ∗ Exe : Il n'existe qu'un seul groupe (à isomorphisme près) tel que $Card(G) = pq$ ($p, q \in \mathbb{P}$, $p \neq q$ et $p \wedge (q-1) = 1$): $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. (En effet $\mathbb{Z}/p\mathbb{Z}$ est distingué/normal).
    ∗ Rem : Si on analyse $\mathfrak{S}_3$ dont le cardinal est 2×3 et où 2 divise $(3-1)$ nous n'avons pas la structure $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
– Développement 2 : *théorème de Wedderburn*
  • The : soit $\mathbb{K}$ un corps fini, alors $\mathbb{K}$ est commutatif.
  • La preuve découle d'abord d'envisager $\mathbb{K}$ comme un Z-espace vectoriel sur le Centre de $\mathbb{K}$ (qui est un corps commutatif) puis d'utiliser la formule des classes pour une action par conjugaison.
– Isométries
– Groupes Projectifs
– Topologie et géométrie

2. *Développements.* —

– Théorème de Cauchy
– Théorèmes de Sylow
– Théorème de Wedderburn

3. *Sources.* —

– Perrin
– J-P Serre
– Francinou et Gianella, tome 1 Algèbre

May 19, 2018
Bruno Nitrosso, EPP et candidat libre