101 Groupe opérant sur un ensemble. Exemples et applications

Refs : [Sp] Szpirglas
[Ul] Ulmer
[CalI] Caldero NH2G2 I
[CalII] 〃 〃 II
[Per] Perrin
[Co] Combes

Dvpt : Sylow
Mat diago sur $\mathbb{F}_q$

I - Action de groupe : définition et premiers exemples :

Def 1. On dit qu'un groupe G agit sur un ensemble X si on a une application

$$\varphi : \begin{array}{ccc} G\times X & \longrightarrow & X \\ (g,x) & \longmapsto & g.x \end{array}$$ telle que

$\forall x\in X \quad e.x = x$

$\forall x\in X, \forall (g,h)\in G^2 \quad g.(h.x) = (gh).x$

On note alors $G \circlearrowleft X$ et φ est appelée une action de G sur X.

Prop 2 La définition 1 est équivalente à l'existence d'un morphisme de groupe $\rho : G \longmapsto Bij(X)$

Exemple 3 Soit G un groupe

- $G \circlearrowleft G$ par translation à gauche : $\varphi : \begin{array}{ccc} G\times G & \longrightarrow & G \\ g,h & \longrightarrow & gh \end{array}$
- $G \circlearrowleft G$ par conjugaison $\begin{array}{ccc} G\times G & \longrightarrow & G \\ g\ h & \longrightarrow & ghg^{-1} \end{array}$
- $S_n \circlearrowleft [\![1,n]\!]$ $\quad \begin{array}{ccc} S_n \times [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ \sigma \quad i & \longrightarrow & \sigma(i) \end{array}$
- Si $\mathbb{K}$ est un corps commutatif $GL_n(\mathbb{K}) \circlearrowleft M_{n,1}(\mathbb{K})$: $\begin{array}{ccc} GL_n(\mathbb{K})\times M_{n,1}(\mathbb{K}) & \longrightarrow & M_{n,1}(\mathbb{K}) \\ (M\ ,\ X) & \longrightarrow & MX \end{array}$
- Si on note $Isom(\Delta)$ le groupe des isométries du triangle équilatéral $A_1A_2A_3$, $Isom(\Delta)$ agit sur $\{A_1, A_2, A_3\}$

$$\begin{array}{ccc} Isom(\Delta)\times \{A_1, A_2, A_3\} & \longrightarrow & \{A_1, A_2, A_3\} \\ f \qquad A_i & \longrightarrow & f(A_i) \end{array}$$

[Ul]

Application 4 $Isom(\Delta) \simeq S_3$ et si on note $Isom(\mathcal{C})$ les isométries du cube dans $\mathbb{R}^3$, on a $Isom(\mathcal{C}) \simeq S_4 \times \mathbb{Z}/2\mathbb{Z}$ (en faisant agir cette fois $Isom(\mathcal{C})$ sur D_1, D_2, D_3, D_4 les grandes diagonales du cube)

Def 5 Une action d'un groupe G sur un ensemble X est dite
- fidèle si $(g.x = x\ \forall x\in X) \Rightarrow g = e$
- transitive si $\forall x, y \in X, \exists g\in G \quad g.x = y$

Rq 6 L'action de G sur X est fidèle $\Leftrightarrow$ le morphisme ρ de la prop 2 est injectif

Application 7 (Théorème de Cayley) Tout groupe d'un groupe est isomorphe à un sous groupe de permutations et un groupe fini de cardinal n est isomorphe à un sous-groupe de S_n.

Ex 8 - L'action de S_n sur $[\![1,n]\!]$ est fidèle
- L'action de $Isom(\Delta)$ sur $\{A_1, A_2, A_3\}$ est transitive
- L'action de conjugaison de S_n sur lui-même n'est pas transitive (12) et (123) ne peuvent pas être reliés par cette action

II - Orbites, stabilisateurs, points fixes

Def 9 Soit une action de G sur X. On définit la relation d'équivalence $x\mathcal{R}y \Leftrightarrow \exists g\in G$ tq $x = g.y$. Les classes d'équivalences associées à cette relation sont appelées orbites de l'action. Pour $x\in X$ on note O_x son orbite.

Application 10 Tout $\sigma\in S_n$ s'écrit comme produit $\sigma = \gamma_1 \cdots \gamma_m$ de cycles γ_i de longueur ≥ 2 dont les supports sont 2 à 2 disjoints et correspondant aux orbites de l'action naturelle de $\langle\sigma\rangle$ sur $[\![1,n]\!]$. La décomposition est unique à ordre près

[Cal II]

Application 11 Soit $\sigma \in S_n$, notons $[l_1, \dots l_m]$ la liste des cardinaux des supports des cycles intervenant dans la décomposition à supports disjoints de σ, rangés dans l'ordre croissant : c'est le "type" de σ. Deux permutations σ et σ' sont alors conjuguées dans S_n $\Leftrightarrow$ elles sont de même type. [Ue]

Ex 12 Dans S_n, $n \geq 4$ les doubles transpositions sont conjuguées.

Rq 13 Soit $G \curvearrowright X$, et $x \in X$, l'action de G sur O_x est transitive.

App 14 Soit $G = GL_n(\mathbb{K})$, $S = Sym_n(\mathbb{K})$ $\mathbb{K}$ corps f et f' des formes quadratique sur un $\mathbb{K}$-ev E de dimension n, on note F et F' les matrices de F et F' dans une base de E. Alors f et f' sont équivalentes ssi F et F' sont dans la même orbite sous l'action [Per]

$$\varphi : G \times S \longrightarrow S$$
$$P, B \longrightarrow {}^tPBP$$

Def 14b Soit $G \curvearrowright X$, $x \in X$, le stabilisateur de x, noté $Stab\,x$ est le sous groupe de G défini par $\{g \in G;\ g \cdot x = x\}$. x est appelé point fixe si $Stab\,x = G$ x est alors seul dans son orbite.

Prop 15 Les orbites de l'action de G sur X forment une partition de X et on a une bijection $f_x : G/Stab\,x \to O_x$ (x fixé)

$$\bar{g} \longrightarrow g \cdot x$$

De plus, $\forall \bar{h} \in G/Stab\,x$, $\forall g \in G$ $f_x(g\bar{h}) = g \cdot f_x(\bar{h})$

Corollaire 16 Si G et X sont finis, alors $\forall x \in X$ $\#O_x \mid |G|$ et $|G| = \#O_x \times |Stab\,x|$

App 17 Soit G un groupe fini et p le plus petit diviseur 1er de $|G|$ alors tout sous groupe H de G d'indice p est normal dans G. [Sp exos]

Prop 18 Si $x, y \in X$ sont dans la même orbite, $Stab\,x$ et $Stab\,y$ sont conjugués.

III - Formule de Burnside, équation aux classes

Prop 19 : Si $G \curvearrowright X$ avec G, X finis, on a $\#X = \sum_{x \in E} \#O_x$ où E est un système de représentants des orbites.

Application 20 : $|G| = |Z(G)| + \sum_i \#O_i$ où la somme porte sur les classes de conjugaison de cardinal > 1

Application 21 (Théorème de Wedderburn) Tout corps fini est commutatif. [Per]

Application 22 : Le nombres de matrices diagonalisables sur $\mathbb{F}_q$ le corps à q éléments est égal à

$$\sum_{\substack{n_1 + \dots n_q = n \\ n_i \geq 0}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1} |GL_{n_i}(\mathbb{F}_q)|}$$ [Cal]

Prop 23 Si G et X sont finis, alors si on note N le nombre d'orbites sous l'action de G, on a :

$$N = \frac{1}{|G|} \sum_{g \in G} |Fix(g)| \quad \text{où}$$

$$Fix(g) = \{x \in X \ ; g \cdot x = x\}$$

Application 24 On peut faire exactement 7? colliers différents à 9 perles avec 4 perles bleues, 3 blanches et 2 oranges. [Combes]

IV - Application aux p-groupes

Thm 25 Soit G un p-groupe, on a $|Z(G)| \geq p$

Corollaire 26 Tout groupe d'ordre p^2 est abélien.

Prop 27 Soit G un $p$groupe agissant sur X un ensemble fini. Soit $X^G = \{x \in X,\ \forall g \in G\ g \cdot x = x\}$ on a $|X^G| \equiv |X| \bmod p$

Application 28 (Th de Cauchy) Soit G un groupe fini d'ordre n et soit p un facteur premier de n. Alors il existe dans G au moins un élément d'ordre p [Co]

Corollaire 29 : Soit G un groupe fini et $p \in \mathbb{N}$ premier. G est un p-groupe $\Leftrightarrow$ tout élément de G est d'ordre une puissance de p [Co]

V - Les théorèmes de Sylow

Def 30 : Soit G un groupe fini et p un nombre premier divisant $|G|$. On écrit $|G| = p^\alpha m$ avec $p \nmid m$ et $\alpha \geq 1$. Un p-Sylow de G est un sous groupe de G d'ordre p^α

Rq 31 : Un p-Sylow de G est un p sous-groupe de G tel que $[G:H]$ soit premier avec p. Cela caractérise les p-Sylow

Exemple 20 Soit p premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments. Soit $G = GL_n(\mathbb{F}_p)$. Alors

$$|G| = p^{n(n-1)/2} (p^n - 1) \cdots (p-1)$$

et H l'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale est un sous groupe de G qui est en fait un p-Sylow de G

Lemme 33 : Soit G un groupe fini, p 1er divisant $|G|$ et S un p-Sylow de G. Si H est un sous groupe de G, $\exists g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Thm 34 : Soit G un groupe et p 1er, tq $p \mid |G|$. Alors
- G contient au moins un p-Sylow
- Les p-Sylow de G sont 2 à 2 conjugués
- Si n_p est le nombre de p-Sylow de G on a $n_p \mid |G|$ et $n_p \equiv 1 \mod p$.

Corollaire 35 : Un p-Sylow de G est distingué dans G $\Leftrightarrow$ c'est l'unique p-Sylow de G.

Thm 36 : Soit H un p-sous groupe de G ; $\exists S$ un p-Sylow de G tel que $H \subset S$.

Application 37 : Un groupe d'ordre 63 n'est pas simple.

Application 38 : Tout groupe de cardinal 45 est isomorphe à l'un des produits directs : $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ ou $\mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2$

Prop 39 : Plus généralement, un groupe d'ordre pq, $p<q$, p et q 1ers. Si p ne divise pas $q-1$ le groupe G est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Application 40 : Tout groupe d'ordre 15 est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ie à $\mathbb{Z}/15\mathbb{Z}$.

VI - Action de Steiniz (Cal I)

Dans cette partie on notera $\mathbb{K}$ un corps commutatif et $G = Gl_m(\mathbb{K}) \times Gl_n(\mathbb{K})$ pour $n, m \in \mathbb{N}^*$

Déf 41 L'action de Steiniz est l'opération
$$\alpha : G \times M_{m,n}(\mathbb{K}) \longrightarrow M_{m,n}(\mathbb{K})$$
$$((P,Q), A) \longmapsto PAQ^{-1}$$
Deux matrices dans la même orbite pour cette action sont dites équivalentes.

Thm 42 : Deux matrices A et B de $M_{m,n}(\mathbb{K})$ sont équivalentes $\Leftrightarrow$ elles ont le même rang.

V - Représentations de groupes :

Déf 43 Soit V un $\mathbb{C}$-ev de dim finie et G un groupe. On appelle Représentation linéaire de G sur V toute action de groupe
$$\rho : G \longrightarrow Gl(V)$$
On dit que V est un G-module
La dimension de V est appelée degré de la représentation

Ex 44 • La représentation triviale de G : $\rho \quad \begin{matrix} G \longmapsto Gl_1(\mathbb{C}) \\ g \longmapsto \rho(g) = 1. \end{matrix}$

• Soit X un ensemble fini $X = \{x_1, \dots x_n\}$ et $e_{x_1}, \dots e_{x_n}$ une base de l'espace vectoriel des fonctions de X dans $\mathbb{C}$.* Si G agit sur X, on peut définir la représentation de permutation associée à cette action par

$$\rho : G \longrightarrow Gl(\mathbb{C}_X)$$
$$g \longmapsto g \cdot : \begin{matrix} \mathbb{C}_X \longrightarrow \mathbb{C}_X \\ e_{x_i} \longmapsto e_{g \cdot x_i} \end{matrix}$$

La représentation de permutation associée à l'action de G sur lui-même par translation à gauche est appelée rep. régulière de G.

Ex 45. Une représentation de G de dimension 1 est un morphisme de groupe
$$\rho : G \longmapsto \mathbb{C}^*$$
Ainsi les représentations linéaires de dim 1 de $\mathbb{Z}/2\mathbb{Z}$ sont
$$\rho : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^* \qquad \bar{1} \longrightarrow 1$$
et
$$\rho' : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{C}^* \qquad \bar{1} \longrightarrow -1.$$

Une représentation linéaire de S_n de dim 1 peut être donnée par
$$\rho : S_n \longrightarrow \mathbb{C}^* \qquad \sigma \longmapsto \varepsilon(\sigma)$$

*note $\mathbb{C}_X$