Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

RM
2022-2023

On considère pour la suite sauf mention contraire un groupe G multiplicatif et un ensemble E non vide. Soit $n \in \mathbb{N}^*$.

1 Actions de groupe

1.1 Action d'un groupe sur un ensemble

Définition 1 : On dit que le groupe G opère à gauche sur l'ensemble E si on a une application $(g,x) \in G \times E \mapsto g.x \in E$ telle que pour tout x de E et g, g' de G, alors $1.x = x$ et $g.(g'.x) = (gg').x$.
Cela revient au même que de définir un morphisme de groupe $\varphi : G \to \mathcal{S}(E)$ avec $\varphi(g)(x) = g.x$.

Exemple 2 : Le groupe $\mathcal{S}_n$ agit naturellement sur l'ensemble $\{1,...,n\}$ avec $\forall \sigma \in \mathcal{S}_n$ et $k \in [\![1\,;n]\!]$, $\sigma.k = \sigma(k)$.

Définition 3 : On dit que l'action de G sur E est transitive (ou simplement transitive) si pour tout $x, y \in E$, il existe $g \in G$ tel que $y = g.x$ (g est unique si c'est simplement transitif).
Une action est dite n-fois transitive si pour tout $(x_i)_{1\leq i\leq n}, (y_i)_{1\leq i\leq n} \in E^n \times E^n$, il existe $g \in G$ tel que pour tout $i \in [\![1\,;n]\!]$, $g.x_i = y_i$.

Exemple 4 : • L'action d'un espace vectoriel V sur un espace affine est une action simplement transitive.
• L'action de $\mathcal{S}_n$ sur $\{1,...,n\}$ est k-transitive pour tout $k \in [\![1\,;n]\!]$.

Remarque 5 : Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

Définition 6 : On dit que l'action de G sur E est fidèle si le morphisme de groupe φ est injectif, ce qui signifie que si $g \in G$ et pour tout $x \in E$, $g.x = x$ si et seulement si $g = 1$.

Exemple 7 : $\mathcal{S}_n$ agit fidèlement sur $\{1,...,n\}$.

1.2 Orbites, Stabilisateurs et équations aux classes

Définition 8 : Si G opère sur E, on appelle pour tout x dans E l'orbite de x sous l'action de G le sous ensemble $O_x = \{g.x | g \in G\}$.

Remarque 9 : On a que la relation $x \sim y$ si et seulement si il existe $g \in G$ tel que $y = g.x$ est une relation d'équivalence sur E. Il en résulte que les orbites forment une partition de E.

Définition 10 : Si G opère sur E, pour tout x dans E, on appelle le sous-ensemble $G_x = \{g \in G | g.x = x =\}$ le stabilisateur de x sous l'action de G.

Proposition 11 : Les stabilisateurs G_x sont des sous-groupes de G.

Exemple 12 : Le stabilisateur de $k \in [\![1\,;n]\!]$ pour l'action de $\mathcal{S}_n$ sur $\{1,...,n\}$ noté $Stab_k$ est isomorphe à $\mathcal{S}_{n-1}$.

Théorème (Équations aux classes) 13 : Si G est un groupe fini opérant sur E, on a :
i) En prenant $x_1,...,x_r$ un système de représantant des orbites, on a $|E| = \sum_{i=1}^{r} |O_{x_i}|$.
ii) On a $|G| = |O_x||G_x|$ pour tout x dans E.

1.3 Application aux p-groupes et au dénombrement

Définition 14 : Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où α est un entier naturel non nul.

Proposition 15 : Soit G un p-groupe opérant sur un ensemble fini E. Alors on a $|E^G| \equiv |E| \pmod p$ avec $E^G = \{x \in E, |O_x| = 1\}$.

Corollaire 16 : Si G opère sur lui même par conjugaison, on a $G^G = Z(G)$ et donc on a $|Z(G)| \equiv |E| \pmod p$.

Corollaire 17 : Le centre d'un p-groupe non trivial est non trivial.

Théorème 18 : Tout groupe d'ordre p^2 avec p premier est abélien.

Application 19 : Soit p un nombre premier. A isomorphisme près, les groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Théorème (de Cauchy) 20 : Soit G un groupe fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n, il existe dans G un élément d'ordre p.

Lemme (Formule de Burnside) 21 : Soit G un groupe agissant sur un ensemble E. On note r le nombre d'orbites. Alors

$$r = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|.$$

où $Fix(g) = \{x \in E | g.x = x\}$.

Développement 22 : Le nombre de colorations distinctes du cube avec c couleurs est

$$\frac{c^2}{24}(c^4 + 3^2 + 12c + 8)$$

Dev 1

2 Action de groupe sur un groupe

2.1 Action par translation à gauche

Définition 23 : On a que G agit sur lui même par translation à gauche avec $(g, h) \in G \times G \mapsto g.h = gh \in G$.

Proposition 24 : Cette action est fidèle et transitive.

Remarque 25 : En faisant agir un sous-groupe H sur G par translation à gauche, on peut retrouver le théorème de Lagrange grâce à l'équation aux classes.

Application (Théorème de Cayley) 26 : Comme φ est injectif, on en déduit que l'image de G par φ est un sous groupe de $\mathcal{S}(G)$ et donc que G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.

Proposition 27 : Soit H un sous-groupe de G. Alors G agit sur G/H les classes à gauche par translation à gauche avec $g'.gH = (g'g).H$. Cette action est transitive.

2.2 Action par conjugaison

Définition 28 : On appelle alors action par conjugaison une action de G sur lui même avec pour g, h dans G, $g.h = ghg^{-1}$. Le morphisme φ est alors noté Int. On appelle $Int(G)$ l'ensemble des automorphismes intérieurs de G. les orbites $O_x = \{g.x | g \in G\}$ pour $x \in G$ sont appelées classes de conjugaison. On dit que deux éléments de G sont conjugués si ils appartiennent à la même classe de conjugaison.

Exemple 29 : Dans $\mathfrak{S}_n$, tous les cycles d'ordre p sont conjugués.

Remarque 30 : Si le groupe G est abélien, alors tous les automorphismes intérieurs sont triviales. C'est donc utilisé dans des groupes non abéliens.

Remarque 31 : On a alors que H est distingué si H est stable par automorphisme intérieur.

2.3 Simplicité et applications aux théorèmes de Sylow

Définition 32 : Un groupe G non trivial est dit simple si et seulement si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Exemple 33 : • $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est premier.
• $\mathcal{A}_n$ est simple pour $n \geq 5$.

Remarque 34 : Il n'est donc pas possible de "factoriser" les groupes simples. Leur étude est donc particulière. La classification des groupes simples finis à été achevée en 1981.

Définition 35 : Soit G un groupe de cardinal $n = p^\alpha m$ avec $\alpha \geq 1$ et $p \not| m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Exemple 36 : Soit $G = Gl_n(\mathbb{F}_p)$. Alors l'ensemble $P = \{A = (a_{i,j}) | a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1\}$ est un p-sous-groupe de Sylow de G.

Théorème (de Sylow) 37 : Soit G un groupe fini et p un diviseur (premier) de $|G|$, alors G contient au moins un p-sous-groupe de Sylow.

Corollaire 38 : Si $|G| = p^\alpha m, p \not| m$, G contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.

Théorème (de Sylow 2) 39 : Soit G un groupe de cardinal $|G| = p^\alpha m, p \not| m$.
i) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S, avec $H \subset S$.
ii) Les p-Sylow sont tous conjugués.
iii) On a $S_p \equiv 1 \pmod p$ et $S_p | m$.

Corollaire 40 : Si S est un p-Sylow de G, on a que S est distingué dans G si et seulement si $S_p = 1$ si et seulement si S est l'unique p-Sylow de G.

Application 41 : • Un groupe d'ordre 63 n'est pas simple.

Développement 42 : Tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$. **Dev 2**

3 Actions de groupes sur des espaces de matrices

On se place sur un corps $\mathbb{K}$ commutatif avec $n, m \in \mathbb{N}^*$.

3.1 Action de $GL_n(\mathbb{K})$ sur $M_{n,m}(\mathbb{K})$ par translation

Définition 43 : L'application $(P, A) \in GL_n(\mathbb{K}) \times M_{n,m}(\mathbb{K}) \mapsto P.A = PA \in M_{n,m}(\mathbb{K})$ définit une action de $Gl_n(\mathbb{K})$ sur $M_{n,m}(\mathbb{K})$ (action de translation à gauche) et deux matrices sont dans la même orbites si et seulement si elles ont le même noyau.

Remarque 44 : On peut définir de même la translation à droite avec $P.A = AP^{-1}$.

Définition 45 : Pour $\lambda \in \mathbb{K}$ et $i, j \in [\![1\,;n]\!]$ avec $i \neq j$, on appelle matrice de transvection une matrice carré de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ et matrice de dilatation une matrice carré de la forme $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i}$.

Proposition 46 : • La multiplication à gauche par une matrice de dilatation $D_i(\lambda)$ a pour effet de multiplier la ligne i par λ.

• La multiplication à gauche par une matrice de transvection $T_{i,j}(\lambda)$ a pour effet de remplacer la ligne L_i par $L_i + \lambda L_j$.

• La multiplication à droite par une matrice de dilatation $D_j(\lambda)$ a pour effet de multiplier la colonne j par λ.

• La multiplication à droite par une matrice de transvection $T_{i,j}(\lambda)$ a pour effet de remplacer la colonne C_j par $C_j + \lambda C_i$.

Ces opérations sont appelés opérations élémentaires sur les lignes ou les colonnes.

Théorème 47 : Soit $A \in M_{n,m}(\mathbb{K})$. Il existe une matrice $P \in GL_n(\mathbb{K})$ produit de matrices de permutation et de transvection telle que la matrice PA soit échelonnée en lignes. Cette matrice PA est donc dans l'orbite de A pour l'action par translation à gauche.

Théorème 48 : Une opération sur un système élémentaire sur les lignes d'un système linéaire $AX = b$ le transforme en un système équivalent.

Remarque 49 : On vient donc ici de revoir la méthode pour un résoudre un système linéaire et l'existence la matrice échelonnée, l'algorithme trouvant cette matrice est appelé pivot de Gauss et est en $O(n^3)$.

3.2 Action de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$ par conjugaison

Théorème 50 : L'application $(P, A) \in GL_n(\mathbb{K}) \times M_n(\mathbb{K}) \mapsto P.A = PAP^{-1} \in M_n(\mathbb{K})$ définit une action de $GL_n(\mathbb{K})$ sur $M_n(\mathbb{K})$. Deux matrices qui sont dans la même orbite pour cette action sont dites semblables.

Théorème 51 : Pour $\mathbb{K}$ algébriquement clos, deux matrices A, B dans $M_n(\mathbb{K})$ sont semblables si et seulement si pour tout $\lambda \in \mathbb{K}$ et $k \in \mathbb{N}^*$ les matrices $(A - \lambda I_n)^k$ et $(B - \lambda I_n)^k$ sont équivalentes.

Théorème 52 : Pour $\mathbb{K}$ algébriquement clos, toute matrice $A \in M_n(\mathbb{K})$ est semblable à sa transposée.

Remarque 53 : Quand on essaye de diagonaliser une matrice, cela revient à chercher un matrice diagonale dans son orbite.

3.3 Action de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$ par congruence

Théorème 54 : L'application $(P, A) \in GL_n(\mathbb{K}) \times S_n(\mathbb{K}) \mapsto P.A = PA^tP \in S_n(\mathbb{K})$ définit une action de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$. Deux matrices qui sont dans la même orbite pour cette action sont dites congruentes.

Remarque 55 : Deux matrices congruentes représentent la même forme quadratique dans deux bases (en générale différente) de $\mathbb{K}^n$.

Théorème 56 : Si φ est une forme quadratique sur $\mathbb{K}^n$, il existe alors une base $(f_i)_{1 \leq i \leq n}$ de $\mathbb{K}^n$ dans la laquelle la matrice de φ est de la forme $diag(\lambda_1, ..., \lambda_n)$ (si r est le rang de q, alors les r premiers λ_i sont non nuls et les suivants sont nuls.

Théorème 57 : *i)* Pour $\mathbb{K} = \mathbb{C}$ deux matrices symétriques A, B sont congruentes si et seulement si elles ont même rang. Donc les orbites sont les ensembles $\mathcal{O}_r = \{A \in S_n(\mathbb{C}) | rg(A) = r\}$, où r est compris entre 0 et n.

ii) Pour $\mathbb{K} = \mathbb{R}$, deux matrices symétriques A, B sont congruentes si et seulement si elles ont même signature. Donc les orbites sont les ensembles $\mathcal{O}_{s,t} = \{A \in S_n(\mathbb{R}) | sign(\varphi) = (s, t)\}$ où φ est la forme quadratique associé à la matrice A, $s = \max dim(F)$ ou F tel que $\varphi_{|F} \in S^+ + (F)$ et $t = r - s$ avec r le rang de A.

Références :

1. Algèbre Gourdon
2. Algèbre et géométrie Rombaldi
3. Cours d'algèbre Perrin
4. Théorie des groupes Ulmer
5. isenmann (rip)