

101: Groupe agissant sur un ensemble. Exemples et applications

On note $(G, \cdot)$ un groupe, E un ensemble non vide, action de G sur E .

I. Action de groupe

a) Définitions et premières propriétés

Def. 1: Une action à gauche de G sur E est une application

$$G \times E \rightarrow E \quad \text{telle que : (i) pour tout } x \in E, 1_G \cdot x = x$$

$$(g, x) \mapsto g \cdot x \quad \text{(ii) pour } g, g' \in G \text{ et } x \in E, g \cdot (g' \cdot x) = (gg') \cdot x$$

Rmq. 2: Supposons que G agisse sur E . Alors pour tout $g \in G, x \in E$

$$\text{On a } g \cdot (g^{-1} \cdot x) = g^{-1} \cdot (g \cdot x) = x. \text{ Ainsi l'application}$$

$$\gamma_g: E \rightarrow E \quad \text{est bijective d'inverse } \gamma_{g^{-1}}. \text{ Ainsi,}$$

$$\varphi: G \rightarrow S(E) \quad \text{est un morphisme de groupe. De plus si } \psi: G \rightarrow S(E)$$

$g \mapsto \gamma_g$ est un morphisme de groupe. On vérifie que $G \times E \rightarrow E$ est une action. On vérifie que les 2 constructions sont inverses l'une de l'autre. Ainsi se donner une action de G sur E , c'est se donner un morphisme de groupe de G dans $S(E)$.

Def. 3: On dit que G agit fidèlement sur E si pour tout $g \in G$ on a: $g \cdot x = x$ pour tout x alors $g = 1_G$. Autrement dit G agit fidèlement sur E si le morphisme associé à l'action est injectif.

On dit que G agit transitivement sur E si pour tout $x, x' \in E$ il existe $g \in G$ tel que $x' = g \cdot x$.

Rmq. 4: Soit H un sous groupe de G . Toute action de G sur E induit par restriction de H sur E .

b) Orbites et stabilisateurs

Def. 5: L'ensemble $\text{stab}_G(x) = \{g \in G \mid g \cdot x = x\}$ est appelé stabilisateur de x . C'est un sous groupe de G .

Lemme 6: La relation $\sim$ définit par $x \sim y$ si il existe $g \in G$ tel que $y = g \cdot x$ est une relation d'équivalence.

Def. 7: Soit $x \in E$, l'ensemble $\text{orb}_G(x) = \{g \cdot x \mid g \in G\}$ est appelé orbite de x sous l'action de G (c'est la classe d'équivalence de x pour $\sim$).

On dit que $x \in E$ est un point fixe sous l'action de G si pour tout $g \in G, g \cdot x = x$. On note E^G l'ensemble des points fixes.

Prop. 8: Soit $x \in E$. Les ASSE:

- (i) $x \in E^G$
- (ii) $|\text{Orb}(x)| = 1$
- (iii) $\text{orb}(x) = \{x\}$
- (iv) $\text{stab}_G(x) = G$

Prop. 9: Les ASSE:

- (i) G agit transitivement sur E
- (ii) il existe x_0 tel que $\text{orb}(x_0) = E$
- (iii) Pour tout $x \in E, \text{orb}(x) = E$
- (iv) E n'admet qu'une seule G -orbite ($= E$).

Prop. 10: (Equation aux classes) Les orbites de E sous l'action de G forment une partition de E . Si de plus E est fini alors

$$|E| = \sum_{x \in \mathcal{R}} |\text{orb}(x)| \quad \text{où } \mathcal{R} \text{ est l'ensemble des orbites de } E.$$

Prop. 11: Pour tout $x \in E$, l'application $f: G \rightarrow \text{orb}(x)$ induit par quotient une bijection $\bar{f}: G/\text{stab}_G(x) \rightarrow \text{orb}(x)$

$$\text{Si } G \text{ est fini on a } |\text{orb}(x)| = \frac{|G|}{|\text{stab}_G(x)|} = \frac{|G|}{|\text{stab}_G(x)|} \cdot |G|$$

Def. 12: Pour tout $g \in G, x \in E$ la G -orbite de x est l'orbite de x sous l'action de $\langle g \rangle$.

Lemme 13: Soit $g \in G$ et w la g -orbite d'un $x \in E$. w est finie si et seulement si il existe $k \in \mathbb{Z}$ tel que $g^k \cdot x = x$.

Dans ce cas, $w = \{x, g \cdot x, \dots, g^{p-1} \cdot x\}$ où p est le plus petit entier différent de 0 tel que $g^p \cdot x = x$.

Prop. 14: (Formule de Burnside) G fini, E fini. $\mathcal{R}$ l'ensemble des orbites de E sous l'action de G . On a:

$$|\mathcal{R}| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

II. Exemples d'actions de groupes

a) Groupe symétrique: l'action de S_n sur $\{1, \dots, n\}$ $n \in \mathbb{N}^*, g \in S_n$

Prop. 15: S_n agit sur $\{1, \dots, n\}$ par $S_n \times \{1, \dots, n\} \rightarrow \{1, \dots, n\}$.

Cette action est fidèle et transitive. $(\sigma, x) \mapsto \sigma(x)$

Rmq. 16: $G \in S_n$. L'action de S_n sur $\{1, \dots, n\}$ se restreint en une action de $\langle \sigma \rangle$ sur $\{1, \dots, n\}$. Une orbite de $\{1, \dots, n\}$ sous cette action s'appelle σ -orbite.

Prop. 17: Soit $x \in \{1, \dots, n\}$ $\text{orb}_G(x) = \{\sigma^m(x) \mid m \in \mathbb{Z}\}$

$\text{orb}_G(x)$ est un singleton si x est un point fixe de σ .

Prop. 18: La réunion des σ -orbites non réduites à un singleton

[BES]
p. 169
170

[BES]
p. 172
176

[BES]
p. 171

sont le support de σ .

Lemme 19: Soit w une σ -orbite à p éléments, soit $a \in w$. Alors p est le plus petit entier strictement positif tq $\sigma^p(a) = a$ et on a $w = \{a, \sigma(a), \dots, \sigma^{p-1}(a)\}$

Def. 20: On dit que σ est un cycle s'il n'existe qu'une seule σ -orbite non réduite à un singleton (nécessairement égal à son support).

Si $p = |\text{supp}(\sigma)|$ on dit que σ est un p -cycle.

Lemme 21: Soit w une orbite non réduite à un élément. Alors, σ_w est un cycle de support w et pour tout $a \in w$, on a:

$$\sigma_w = (a \ \sigma(a) \ \dots \ \sigma^{p-1}(a)) \text{ où } p = |w|$$

De plus, tout p -cycle de S_n est de cette forme.

Thm. 22: σ se décompose en produit de cycles à support disjoint et cette décomposition à l'ordre des facteurs près. Cette décomposition est:

$$\sigma = \pi \sigma_w \text{ où } \pi^* \text{ est l'ensemble des orbites non réduites à un singleton.}$$

b) Action par translation

Def. 23: On appelle translation à gauche l'action de G sur G

$$(G \times G) \rightarrow G$$

$$(g, a) \mapsto ga$$

Prop. 24: L'action de translation à gauche est simplement transitive (i.e. $\forall a, b \in G, \exists! g \in G, g.a = b$) et fidèle (on a $\varphi: G \rightarrow S(G)$ injectif).

Cor. 25: Si G est fini de cardinal n , G est isomorphe à un sous groupe de S_n .

Def. 26: Soit H un sous groupe de G (pas nécessairement distingué). G agit sur G/H par translation avec l'action:

$$(G, G/H) \rightarrow G/H$$

$$g, aH \mapsto (ga)H$$

Prop. 27: Cette action est transitive, le stabilisateur de aH est aHa^{-1}

Prop. 28: Si G est infini et H un sous groupe de G distinct de G et d'indice fini alors G n'est pas simple

c) Action par conjugaison

Def. 29: On appelle action par conjugaison l'action de G sur G par

$$(G \times G) \rightarrow G$$

$$(a, g) \mapsto gag^{-1} \text{ Les orbites de cette action sont appelées classe de conjugaison.}$$

Le stabilisateur de $a \in G$ est appelé centralisateur:

$$H_a = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\}$$

Soit A une partie de G on définit le centralisateur de A par

$$C_G(A) = \{g \in G \mid \forall a \in A, ga = ag\}$$

Prop. 30: $C_G(A)$ est le centre de G .

Prop. 31: Soit $\sigma \in S_n$ un cycle d'ordre p , $\sigma = (a_1 \dots a_p)$, soit $\tau \in S_n$ on a:

$$\tau \sigma \tau^{-1} = (\tau(a_1) \dots \tau(a_p))$$

• Dans S_n tous les cycles sont conjugués

• Si $n \geq 5$ les cycles d'ordres 3 sont conjugués dans A_n .

Thm. 32: Pour $n \geq 5$, A_n est simple

Lemme 33: Soit G un p -groupe opérant sur E , $|E| = |EG|$ Cps

Prop. 34: Le centre d'un p -groupe non trivial n'est pas trivial.

Def. 35: Soit X l'ensemble des sous groupe de G , G agit sur X par conjugaison, $(g, x) \mapsto x$. On dit que H et gHg^{-1} sont conjugués.

Le stabilisateur de H est $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ et est appelé normalisateur de H dans G .

Prop. 36: $N_G(H)$ est distingué dans H . C'est le plus grand sous groupe de G distingué dans H .

III - Applications

a) Action sur les espaces de matrices

Action par translation

Thm. 24: $m, n \in \mathbb{N}$. On considère l'action de $GL_n(K)$ par multiplication à gauche sur l'espace $M_{m,n}(K)$. Alors:

• $A, A' \in M_{m,n}(K)$ sont dans la même orbite ssi elles ont même noyau (i.e. $\exists P \in GL_m(K) \ A' = PA \iff \ker(A) = \ker(A')$)

• Toutes matrices est dans l'orbite d'une unique matrice échelonnée réduite en ligne.

Def. 38: On appelle matrice de dilatation $D_i(\alpha)$ où $\alpha \in K$ et $1 \leq i \leq p$ tq $D_i(\alpha) = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & \alpha & \\ & & & 1 \end{pmatrix}$

Def. 39: On appelle matrice de translation $T_{i,j}(\beta) = I_n + \beta E_{i,j}$ où $i, j \in \{1, \dots, n\}$ et $\beta \in K$.

[CERS]

p. 204
205

[CERS]
p. 15

[CERS]
p. 17

[CERS]
p. 15
-16

[CERS]
p. 28

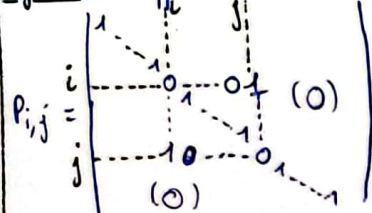
[CERS]
p. 16
-17

[CERS]
p. 18

[CERS]
p. 203

[CAN] p. 130

Def. 40: On appelle matrice de permutation pour $1 \leq i < j \leq n$



Rmq. 41: L'action de translation à gauche par ces matrices décrivent les opérations élémentaires de l'algo. de Gauss. (cf. Annexes)

Action par équivalence

Def. 42: On définit l'action par équivalence de $GL_n(K) \times GL_n(K)$ sur $M_{m,n}(K)$ par

$$(GL_n(K) \times GL_n(K)) \times M_{m,n}(K) \longrightarrow M_{m,n}(K)$$

$$((P, Q), A) \longmapsto PAQ^{-1}$$

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

Thm. 43: $A, B \in M_{m,n}(K)$ sont équivalentes si $rg(A) = rg(B)$

Rmq. 44: Un représentant pour chaque orbite est $r \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & i & \\ & & & 0 \dots 0 \end{pmatrix}$

Action par conjugaison

Def. 45: L'action par conjugaison de $GL_n(K)$ sur $M_n(K)$ est

$$GL_n(K) \times M_n(K) \longrightarrow M_n(K)$$

$$(P, A) \longmapsto PAP^{-1}$$

Deux matrices dans la même orbite sont dites semblables

Action par congruence

Def. 46: L'action par congruence de $GL_n(K)$ sur $S_n(K)$ est

$$GL_n(K) \times S_n(K) \longrightarrow S_n(K)$$

$$(P, A) \longmapsto PAP^T$$

Deux matrices dans la même orbite sont dites congruentes.

Def. 47: Pour q une forme quadratique et A la matrice de q dans une certaine base. On définit $PA := \text{mod} \{ \dim F \mid F \subseteq E, \forall x \in F, x \perp 0 \Rightarrow q(x) = 0 \}$ où E est un K -ev

Thm. 48: Si $K = \mathbb{C}$, 2 matrices sont congruentes si elles ont même rang.

Si $K = \mathbb{R}$, 2 matrices sont congruentes si elles ont même rang et même invariance p (i.e. même signature)

Si $K = \mathbb{F}_q$, 2 matrices sont congruentes si elles ont même déterminant dans $\mathbb{F}_q^* / (\mathbb{F}_q^*)^2$.

[CAN] p. 6

[CAN] p. 18

[CAN] p. 250-251

[CAN] p. 254

b) Géométrie: Isométrie du cube

On se place dans le $\mathbb{R}$ -ev $\mathbb{R}^3$ muni d'un repère orthonormé. On note $A_1, \dots, A_8$ les points de coord. $(\pm 1, \pm 1, \pm 1)$ et C le cube de arête 2

Def. 49: On note $Is(C)$ le groupe des isométries de $\mathbb{R}^3$ qui conservent C .

On note aussi $Is^+(C) = Is(C) \cap O^+(\mathbb{R}^3)$

Thm. 50: $Is(C) = Is(S)$ (= isométrie qui conserve les sommets du cube)

$\Delta = -Id \in Is(C)$. $p: Is(C) \rightarrow Is^+(C) \times \{\pm Id\}$ est une bijection.

$$p \longmapsto \begin{cases} (p, Id) & \text{si } p \in Is^+ \\ (p, \Delta) & \text{sinon} \end{cases}$$

Lemme. 51: Soit $f \in Is^+(C)$. f est entièrement déterminée par $p(A_i)$ et $p(A_j)$ où $i, j \in \{1, \dots, 8\}$ et $\{A_i, A_j\}$ est une arête du cube C .

Thm. 52: $Is^+(C) \cong S_4$ et $Is(C) \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$

c) Dénombrement $p \in P$, $q = p^2 \in U^*$ et E $\mathbb{F}_q$ -ev de dim. $n \in \mathbb{N}^*$.

Prop. 53: $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$

Def. 54: On note $D(E)$ l'ensemble des automorphismes de E diagonalisables.

$$Thm. 55: |D(E)| = \sum_{\substack{m_1, \dots, m_q \\ m_1 + \dots + m_q = n}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{m_1}(\mathbb{F}_q)| \dots |GL_{m_q}(\mathbb{F}_q)|}$$

Def. 56: On note $D(E)$ l'ensemble des endo. de E diagonalisables.

$$Thm. 57: |D(E)| = \sum_{\substack{m_1, \dots, m_q \in \mathbb{N} \\ m_1 + \dots + m_q = n}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{m_1}(\mathbb{F}_q)| \dots |GL_{m_q}(\mathbb{F}_q)|}$$

[CAN] p. 88-92

DEV

CAN p. 105

[CAN] p. 151

DEV

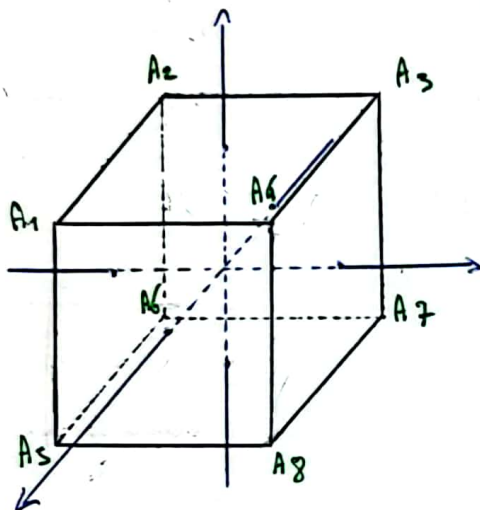
[CAN] p. 63

Annexe 1:

Annexe 1:

Opérations	$D_{i,j}(A)$	$T_{i,j}(B)A$	$P_{i,j}A$
Résultat	$L_i \leftarrow \alpha L_i$	$L_i \leftarrow L_i + \beta L_j$	$L_i \leftrightarrow L_j$

Annexe 2:



Références:

[BERS: Berthuy, Algèbre de grand combat
 [BERS: Perrin, Cours d'algèbre
 [CAL: Caldero, NP problèmes... (1^{re} ed) TM
 [ROM: Rombaldi, Algèbre et géométrie pour l'agrar
 [CVAS: Cabbato, Écart de voyage en Algérie.

Commentaires: