Groupes opérant sur un ensemble. Exemples et applications.

L101

Soit par la suite G un groupe et E ensemble non-vide.

I] Actions de groupe

1] Action d'un groupe sur un ensemble

[Rom] I.6.

Définition 1 : On dit que G opère à gauche sur l'ensemble E s'il existe une application $\begin{array}{l} G\times E \to E \\ (g;x)\mapsto g.x \end{array}$ telle que :

$$\begin{cases} \forall x\in E,\ 1_G.x = x \\ \forall (g;g';x)\in G^2\times E,\ g.(g'.x) = (gg').x \end{cases}$$

ou s'il existe un morphisme de groupes structurel $\varphi : \begin{array}{l} G \to Bij(E) \\ g\mapsto \left[\varphi_g : \begin{array}{l} E\to E \\ x\mapsto g.x \end{array}\right] \end{array}$.

Exemple 2 : Le groupe $S(E)$ des permutations de E agit naturellement sur E par l'action : $\begin{array}{l} S(E)\times E \to E \\ (\sigma ; x)\mapsto \sigma.x = \sigma(x) \end{array}$

Définition 3 : (1) L'action de G sur E est transitive (resp. simplement transitive) si : pour tout $(x;y)\in E^2$, il existe $g\in G$ tel que $y = g.x$ (resp. il existe un UNIQUE $g\in G$ tel que $y = g.x$).

(2) L'action de G sur E est fidèle si le morphisme φ est injectif i.e. ($g\in G$ et pour tout $x\in E$, $g.x = x$) ssi $g = 1$

Remarque 4 : (1) Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

(2) Une action fidèle permet d'identifier G à un sous-groupe de $S(E)$

2] Orbites et stabilisateurs

[Rom] I.6.

Définition 5 : Soit G opérant sur E ($G \curvearrowright E$). Pour tout $x\in E$, le sous-ensemble $Orb(x) = \{g.x \mid g\in G\}\subset E$ est appelé orbite de x sous l'action de G.

Remarque 6 : La relation $x\sim y$ ssi il existe $g\in G$ tel que $y = g.x$ est une relation d'équivalence (réflexif ; transitif ; symétrique) sur E et la classe de $x\in E$ pour cette relation est $Orb(x)$. Les orbites forment alors une partition de E.

Exemple 7 : Pour l'action de $S(E)$ sur E, il y a une seule orbite.

Définition 8 : Soit G opérant sur E. Pour tout $x\in E$, le sous-ensemble $Stab(x) = \{g\in G \mid g.x = x\}\subset G$ est le stabilisateur de x sous l'action de G.

Exemple 9 : Pour l'action de $S(E)$ sur E, pour tout $x\in E$, $Stab(x)$ est isomorphe à $S(E\setminus\{x\})$.

Théorème 10 : Soit G opérant sur E.

Alors : pour tout $x\in E$, $\varphi_x : \begin{array}{l} G/Stab(x) \to Orb(x) \\ \bar{g} \mapsto g.x \end{array}$ est bien définie et bijective

De plus, si G fini, $|Orb(x)| = \dfrac{|G|}{|Stab(x)|}$ (en particulier, $|Orb(x)| \mid |G|$).

3] Action d'un groupe fini sur un ensemble fini

[Rom] I.6.

Théorème 11 : (équation aux classes) Soit G opérant sur E tous deux finis

Alors : en notant $Orb(x_1);\dots;Orb(x_r)$ toutes les orbites deux à deux distinctes,

$$|E| = \sum_{i=1}^{r} |Orb(x_i)| = \sum_{i=1}^{r} \frac{|G|}{|Stab(x_i)|}$$

Définition 12 : Soit G opérant sur E. On note $E^G = \{x\in E \mid Orb(x) = \{x\}\}$ l'ensemble des éléments de E dont l'orbite est réduite à un point

Remarque 13 : En remplaçant dans l'équation aux classes, on a :

$$|E| = |E^G| + \sum_{\substack{i=1 \\ |Orb(x_i)|\geq 2}} |Orb(x_i)|$$

Définition 14 : Soit $p\in\mathbb{N}$ nombre premier. On appelle p-groupe tout groupe de cardinal p^α avec $\alpha\in\mathbb{N}^*$.

Corollaire 15 : Soit p premier et G un p-groupe opérant sur E fini

Alors : $|E^G| \equiv |E| \mod(p)$

Proposition : (formule de Burnside) Soit $Fix(g) = \{x\in E \mid g.x = x\}$ Alors $r = \frac{1}{|G|}\sum_{g\in G} |Fix(g)|$.

II] L'action pour mieux comprendre le groupe

1] Action par translation

[Ulm] IV.2

Définition 16 : Un groupe G agit sur lui même par translation en posant $\begin{array}{l} G\times G \to G \\ (g;h)\mapsto g.h = gh \end{array}$

Proposition 17 : G opère fidèlement et transitivement sur G.

Application 18 : (théorème de Cayley) Tout groupe fini G d'ordre $n\in\mathbb{N}$ est isomorphe à un sous-groupe de S_n.

Proposition 19 : Soit $H < G$.

Alors : l'action $\begin{array}{l} G\times G/H \to G/H \\ (g ; \tilde{g}H) \mapsto (g\tilde{g})H \end{array}$ est transitive.

Contrexemple 20 : Cette action n'est, en général, pas fidèle.

Soit $G = GL_2(\mathbb{F}_3)$ et $H = \langle \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \rangle$. Or : $\varphi : G \to S(G/H)$ n'est pas injectif car $\ker(\varphi) = \langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \rangle$. Ainsi, l'action de G sur G/H n'est pas fidèle.

2] Action par conjugaison

[Ulm] IV.3

Définition 21: Un groupe G agit sur lui-même par conjugaison par l'application
$$G\times G \to G,\quad (g;h)\mapsto g.h = ghg^{-1}.$$
Les orbites par cette action sont appelées classes de conjugaison.
Les stabilisateurs par cette action sont appelés centralisateurs.

Remarque 22: Pour $G\neq\{e\}$, l'action par conjugaison n'est ni fidèle, ni transitive.

Notation 23: On note $Z(G)=G^G=\{g\in G \mid \forall h\in G,\ ghg^{-1}=h\}$ le centre de G.

Exemple 24: $Z(D_n)=\begin{cases}\{e\} & \text{si } n \text{ impair}\\ \{e; r^{\frac{n}{2}}\} & \text{si } n \text{ pair.}\end{cases}$

3] Application aux théorèmes de Sylow

[Per] I.5

Définition 25: Soit G groupe de cardinal $p^\alpha m$ avec p premier et $m\in\mathbb{N}$ tel que $p\nmid m$. On appelle p-sous-groupe de Sylow de G tout sous-groupe de cardinal p^α.

Exemple 26: Soit $G=GL_n(\mathbb{F}_p)$ de cardinal $|G|=(p^n-1)\times\cdots\times(p^n-p^{n-1})=mp^{\frac{n(n-1)}{2}}$ avec $p\nmid m$ et soit $P=\{A=(a_{i,j}) \mid a_{i,j}=0 \text{ si } i>j \text{ et } a_{i,i}=1\}$.
P est un p-sous-groupe de Sylow de G car $|P|=p\times\cdots\times p^{n-1}=p^{\frac{n(n-1)}{2}}$

Théorème 27: (de Sylow) Soit G groupe fini et p premier tel que $p \mid |G|$.
Alors: G contient au moins un p-sous-groupe de Sylow.

Corollaire 28: Soit G groupe de cardinal $|G|=p^\alpha m$ avec $p\nmid m$.
Alors: G contient des sous-groupes d'ordre p^i pour tout $i\le\alpha$.

Théorème 29: (de Sylow bis) Soit G groupe de cardinal $|G|=p^\alpha m$ avec $p\nmid m$.
Alors: (1) Si $H<G$ est un p-groupe, alors il existe un p-Sylow S tel que $H\subset S$.
(2) Les p-Sylow sont tous conjugués (donc leur nombre n_p divise $p^\alpha m$)
(3) $n_p\equiv 1 \mod (p)$ (donc $n_p \mid m$)

Application 30: Un groupe d'ordre 63 n'est pas simple

III] Action pour mieux comprendre l'ensemble

1] Actions sur les espaces de matrices

[Rom] II

Soit $\mathbb{K}$ corps commutatif, $n,m\in\mathbb{N}$

Théorème 31: L'application $GL_n(\mathbb{K})\times\mathcal{M}_{n,m}(\mathbb{K})\to \mathcal{M}_{n,m}(\mathbb{K})$, $(P;A)\mapsto P.A=PA$ définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_{n,m}(\mathbb{K})$ appelée translation à gauche et deux matrices $A,A'\in GL_n(\mathbb{K})$ vérifient $Orb(A)=Orb(A')$ ssi $\ker(A)=\ker(A')$ (le noyau est un invariant total pour l'action de translation à gauche).

Proposition 32: Soit $\lambda\in\mathbb{K}$, $D_i(\lambda)=I_n+(\lambda-1)E_{i,i}$ et $T_{i,j}(\lambda)=I_n+\lambda E_{i,j}$
Alors: (1) Multiplier à gauche par $D_i(\lambda)$ multiplie la i-ème ligne par λ.
(2) Multiplier à droite par $D_j(\lambda)$ multiplie la j-ème colonne par λ.
(3) Multiplier à gauche par $T_{i,j}(\lambda)$ remplace L_i par $L_i+\lambda L_j$
(4) Multiplier à droite par $T_{i,j}(\lambda)$ remplace C_j par $C_j+\lambda C_i$

Proposition 33: Soit $A\in\mathcal{M}_{n,m}(\mathbb{K})$
Alors: il existe une matrice $P\in GL_n(\mathbb{K})$ produit de matrices de permutation et de transvection telle que PA soit échelonnée en lignes.
Ainsi, $PA\in Orb(A)$.
Remarque : Algorithme de résolution d'un système linéaire $Ax=b$: pivot de Gauss.

Théorème 34: L'application $(GL_n(\mathbb{K})\times GL_m(\mathbb{K}))\times\mathcal{M}_{n,m}(\mathbb{K})\to\mathcal{M}_{n,m}(\mathbb{K})$, $((P;Q);A)\mapsto (P,Q).A=PAQ^{-1}$ définit une action de $GL_n(\mathbb{K})\times GL_m(\mathbb{K})$ sur $\mathcal{M}_{n,m}(\mathbb{K})$ appelée action par équivalence dont les orbites sont les $\mathcal{O}_r=\{A\in\mathcal{M}_{n,m}(\mathbb{K})\mid rg(A)=r\}$, $r\in[\![0;\min(n,m)]\!]$
(le rang est un invariant total pour l'action par équivalence)

Proposition 35: Soit $A\in\mathcal{M}_{n,m}(\mathbb{K})$ et $r\in[\![0;\min(n;m)]\!]$.
Alors: $rg(A)=r$ ssi A est équivalente à $A_r:=\begin{pmatrix}I_r&0\\0&0\end{pmatrix}\in\mathcal{M}_{n,m}(\mathbb{K})$

Théorème 36: L'application $GL_n(\mathbb{K})\times\mathcal{M}_n(\mathbb{K})\to\mathcal{M}_n(\mathbb{K})$, $(P;A)\mapsto P.A=PAP^{-1}$ définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ appelée action par conjugaison. Deux matrices qui sont dans la même orbite pour cette action sont dites semblables ou conjuguées.
(le rang, le déterminant, le polynôme caractéristique et la trace sont des invariants pour l'action par conjugaison) (non-total i.e. deux matrices dans la même orbite pour cette action ont même déterminant, polynôme caractéristique et trace mais la réciproque n'est pas vraie)

Proposition 37: Pour $\mathbb{K}$ algébriquement clos, deux matrices $A,B\in\mathcal{M}_n(\mathbb{K})$ sont semblables ssi pour tout $\lambda\in\mathbb{K}$, et tout $k\in\mathbb{N}^*$, $(A-\lambda I_n)^k$ et $(B-\lambda I_n)^k$ sont équivalentes.

[Rom] VI

Théorème 38 : L'application $\begin{array}{rcl} GL_n(\mathbb{K})\times S_n(\mathbb{K}) & \to & S_n(\mathbb{K}) \\ (P\,;\,A) & \mapsto & P.A = PA\,{}^tP \end{array}$ définit une action de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$ appelée action par congruence. Deux matrices dans la même orbite par cette action sont dites congruentes. (le rang et le discriminant (modulo les carrés de $\mathbb{K}^*$) sont des invariants pour cette action).

Théorème 39 : (1) Pour $\mathbb{K}=\mathbb{C}$, deux matrices $A,B\in S_n(\mathbb{C})$ sont congruentes ssi $rg(A)=rg(B)$ i.e. les orbites sont les $\mathcal{O}_r=\{A\in S_n(\mathbb{C}) \mid rg(A)=r\}$ avec $r\in[\![0;n]\!]$. (le rang est un invariant total pour cette action)

(2) Pour $\mathbb{K}=\mathbb{R}$, deux matrices $A,B\in S_n(\mathbb{R})$ sont congruentes ssi $sign(A)=sign(B)$ i.e. les orbites sont les $\mathcal{O}_{(s;t)}=\{A\in S_n(\mathbb{R}) \mid sign(\varphi)=(s;t)\}$ avec φ la forme quadratique associée à la matrice A et $s=\max\limits_{F \text{ sous-ev tq: } \varphi_{|F}\in S^{++}(F)}\{\dim(F)\}$ et $t=r-s$ avec $r=rg(A)$. (la signature est un invariant total pour cette action).

(3) Pour $\mathbb{K}=\mathbb{F}_q$, deux matrices $A,B\in S_n(\mathbb{F}_q)\cap GL_n(\mathbb{F}_q)$ sont congruentes ssi elles ont même discriminant (modulo les carrés de $\mathbb{F}_q^*$).

2] Application aux drapeaux en dimension finie

[Isen]

Définition 40 : Un drapeau (complet) est une suite strictement croissante d'ev : $\{0\}=A_0 \subsetneq A_1 \subsetneq \dots \subsetneq A_n = E$.
On note $\mathcal{D}$ l'ensemble des drapeaux de E.

Proposition 41 : Soit $(f_1;\dots;f_n)$ base de E et pour tout $i\in[\![1;n]\!]$, $F_i=\mathrm{Vect}\{f_1;\dots;f_i\}$ et $F_0=\{0\}$. Soit $\varphi : \begin{array}{rcl} GL_n(\mathbb{K}) & \to & \mathcal{D} \\ (C_1|\dots|C_n) & \mapsto & (\mathrm{Vect}\{C_1;\dots;C_i\})_{i\in[\![0;n]\!]} \end{array}$
Alors : $d=(F_0;\dots;F_n)$ est un drapeau de E et alors φ est surjective.

Notation 42 : Pour $e=(e_1;\dots;e_n)$ la base canonique de E, on note $\delta=\varphi(e)$ le drapeau canonique.

Proposition 43 : L'application $\begin{array}{rcl} GL_n(\mathbb{K})\times\mathcal{D} & \to & \mathcal{D} \\ (A\,;\,d) & \mapsto & A.d=(A(F_i))_{i\in[\![0;n]\!]} \end{array}$ définit une action de $GL_n(\mathbb{K})$ sur $\mathcal{D}$.

Lemme 44 : Cette action est transitive et $\mathcal{D}\simeq GL_n(\mathbb{K})/T_S$ avec T_S l'ensemble des matrices de $GL_n(\mathbb{K})$ triangulaires supérieures.

Théorème 45 : (décomposition de Bruhat) $GL_n(\mathbb{K})=\bigsqcup\limits_{\sigma\in S_n} T_S P_\sigma T_S$

Théorème 46 : Le nombre d'orbites de l'action de $GL_n(\mathbb{K})$ sur $\mathcal{D}\times\mathcal{D}$ est $n!$.

3] Application de l'action par conjugaison à l'algèbre des quaternions

[Isen]

Définition 47 : Le corps gauche des quaternions $\mathbb{H}$ est une $\mathbb{R}$-algèbre non-commutative engendrée par $i;j;k$ tels que : $i^2=j^2=k^2=-1$; $ij=k$; $jk=i$; $ki=j$.
La norme multiplicative d'un quaternion $q=a+ib+jc+kd$ est $N(q)=\sqrt{a^2+b^2+c^2+d^2}$

Notation 48 : On note $Sp(1)=\{q\in\mathbb{H} \mid N(q)=1\}$ et $Im(\mathbb{H})=\{q\in\mathbb{H} \mid Re(q)=0\}$

Propriétés 49 : (1) $2\,Re(q)=q+\overline{q}$ avec $\overline{q}=a-ib-jc-kd$
(2) $\overline{q_1q_2}=\overline{q_2}\;\overline{q_1}$
(3) $N(q)^2=q\overline{q}$
(4) $Z(\mathbb{H})=\{q\in\mathbb{H} \mid \forall q'\in\mathbb{H},\ qq'q^{-1}=q'\}=\mathbb{R}$
(5) $Z(\mathbb{H})\cap Sp(1)=\{\pm1\}$

Lemme 50 : (admis) La sphère unité $\mathbb{S}^{n-1}$ de $\mathbb{R}^n$ est connexe par arcs. En particulier, $Sp(1)$ est connexe par arcs.

Définition 51 : Un retournement de $\mathbb{R}^3$ pour $v\in\mathbb{R}^3$ est
$r_v : \begin{array}{rcl} \mathbb{R}^3 & \to & \mathbb{R}^3 \\ z & \mapsto & 2\dfrac{\langle z;v\rangle}{\|v\|_2^2}v-z \end{array}$ symétrie orthogonale par rapport à une droite

Théorème 52 : $SO_3(\mathbb{R})$ est engendré par les retournements.

Théorème 53 : $SO_3(\mathbb{R})\simeq Sp(1)/\{\pm1\}$ avec $Sp(1)=\{q\in\mathbb{H} \mid N(q)=1\}$.

Références:

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[Ulm] Théorie des groupes - Ulmer

[Per] Cours d'algèbre - Perrin

[Isen] L'oral à l'agrégation de mathématiques - Isenmann