101 — Groupe Opérant sur Un Ensemble. Exemples et Applications

G est un groupe, E un ensemble

1 - Définitions et Premiers Exemples

1) Définitions

Def 1 Une action (à gauche) de G sur E est une application $\begin{aligned} G\times E &\to E \\ (g,x) &\mapsto g\cdot x\end{aligned}$ telle que (i) $\forall x\in E$, $1_G\cdot x = x$
(ii) $\forall g,g'\in G$, $\forall x\in E$, $g\cdot(g'\cdot x) = (gg')\cdot x$

De manière équivalente, une action est la donnée d'un morphisme de groupes $\varphi : \begin{aligned} G &\to \mathfrak{S}(E) \\ g &\mapsto \tau_g : \begin{aligned} E&\to E \\ x&\mapsto g\cdot x\end{aligned}\end{aligned}$

On le note $G \curvearrowright E$

Ex 2
- $\varphi : \begin{aligned}\mathbb{Z} &\to \mathfrak{S}(\mathbb{R}) \\ n &\mapsto \tau_n : \begin{aligned}\mathbb{R}&\to\mathbb{R} \\ x&\mapsto x+n\end{aligned}\end{aligned}$ définit une action de $\mathbb{Z}$ sur $\mathbb{R}$
- $m\in\mathbb{N}^*$, $\mathfrak{S}_m$ agit sur $[\![1,m]\!]$ via $\begin{aligned}(\mathfrak{S}_m\times[\![1,m]\!]) &\to [\![1,m]\!] \\ (\sigma, k) &\mapsto \sigma(k)\end{aligned}$

Def 3 Soit G opérant sur E, on définit
(i) pour $x\in E$, $Stab_G(x) = \{g\in G, g\cdot x = x\}$ le stabilisateur de x
(ii) pour $x\in E$, $O_x = \{g\cdot x, g\in G\}$ l'orbite de x
(iii) pour $g\in G$, $Fix(g) = \{x\in E, g\cdot x = x\}$ l'ensemble des points fixes de g

Rq 4 Pour $x\in E$, $Stab_G(x)$ est un sous-groupe de G

Def 5 L'action $G\curvearrowright E$ est dite
(i) fidèle si $\forall g\in G$, $g\cdot x = x\ \forall x\in E \Leftrightarrow g = 1_G$
(ii) libre si $\forall g\in G\setminus\{1_G\}$, $Fix(g) = \emptyset$
(iii) transitive si $\forall x,x'\in E$, $O_x = O_{x'}$
(iv) k-transitive, $k\in\mathbb{N}$, si l'action définie par $\begin{aligned} G\times E^{*k} &\to E^{*k} \\ (g,(x_1,\dots,x_k)) &\mapsto (g\cdot x_1,\dots,g\cdot x_k)\end{aligned}$ est transitive
où $E^{*k} = \{(x_1,\dots,x_k)\in E^k,\ i\neq j \Rightarrow x_i\neq x_j\}$
(v) simplement transitive si elle est libre et transitive.

Rq 6 Si l'action est k-transitive, elle est $(k-1)$ transitive
Si l'action est libre, elle est fidèle

Ex 7 1) L'action de $\mathbb{Z}$ sur $\mathbb{R}$ définie plus haut est libre mais pas transitive
2) L'action de $\mathfrak{S}_m$ sur $[\![1,m]\!]$ est fidèle et n-transitive mais pas libre
3) La Restriction de l'action de $\mathfrak{S}_m$ sur $[\![1,m]\!]$ à $\mathcal{A}_m$ est $n-2$ transitive

2) Premières Applications

Lemme 8 Soit G opérant sur E, la relation sur E définie par $x\sim y$ s'il existe $g\in G$ tel que $y = g\cdot x$ est une relation d'équivalence. De plus, les orbites de E sous G sont les classes d'équivalence de cette relation

Prop 9 (Équation aux classes) Soit G opérant sur E, on suppose E fini et on note Ω l'ensemble des orbites de E sous l'action. Alors $|E| = \sum_{\omega\in\Omega}|\omega|$

Appli 10 (Théorème de Fermat) Soit $n\in\mathbb{N}^*$, p premier, si p ne divise pas n, $n^{p-1}\equiv 1[p]$

Appli 11 (Théorème de Cauchy) Soit G groupe fini, p premier, si $p\,|\,|G|$, alors il existe $x\in G$ d'ordre p.

Prop 12 (Relation orbite/stabilisateurs) Soit G opérant sur E, $x\in E$. L'application $\begin{aligned}G&\to O_x\\ g&\mapsto g\cdot x\end{aligned}$ induit par passage au quotient une bijection $\bar{f} : G/Stab_G(x) \xrightarrow{\sim} O_x$
En particulier, $Card(O_x) < +\infty$ ssi $[G:Stab_G(x)] < +\infty$
Enfin, si G est fini, $|G| = |Stab_G(x)| \times Card(O_x)$

Prop 13 (Formule de Burnside) Soit G opérant sur E. On suppose G et E finis, on note Ω l'ensemble des Orbites de E. Alors $|\Omega| = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$

Appli 14 Soit g opérant sur E, $q\in\mathbb{N}^*$
Un coloriage de E en (au plus) q couleurs est une application $f : E\to[\![1,q]\!]$
2 coloriages f, f' sont G-équivalents si il existe $g\in G$, $\forall x\in E$ $f(g^{-1}x) = f'(x)$
On note $C_G(E,q)$ l'ensemble des Classes d'équivalences de coloriages
Alors $|C_G(E,q)| = \frac{1}{|G|}\sum_{g\in G} q^{r(g)}$ où $r(g)$ est le nombre d'orbites de $\langle g\rangle \curvearrowright E$

3) Action d'un groupe par translation et par conjugaison

Def 15 On définit l'action par translation de G sur G par $\begin{aligned}G\times G&\to G\\ (g,h)&\mapsto gh\end{aligned}$

Rq 16 Cette action est simplement transitive

Th 17 (Cayley) Soit G groupe fini d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$

Appli 18 (1er théorème de Sylow) Soit G un groupe fini, $|G| = n = p^\alpha q$, $\alpha\in\mathbb{N}^*$, p premier et $p\wedge q = 1$
un p-Sylow de G est un sous-groupe de G d'ordre p^α.
G admet un p-Sylow et tout p-sous-groupe de G est contenu dans un p-Sylow

Prop 19 Soit G un groupe, H sous-groupe de G, $\begin{aligned}G\times G/H &\to G/H \\ (g,\tilde{g}H)&\mapsto (g\tilde{g})H\end{aligned}$ définit une action transitive de G sur G/H

Appli 20 (Théorème de Lagrange) G groupe fini, H sous groupe de G alors $|H|\,\big|\,|G|$

Appli 21 (Théorème de Frobenius) G groupe fini, H sous groupe de G tel que pour p premier $p\,|\,|H| \Rightarrow p\geq [G:H]$, alors $H\lhd G$
En particulier, soit q le plus petit facteur premier de $|G|$, alors tout sous-groupe d'indice q est distingué dans G.

Def 22 On définit l'action par conjugaison de G sur G par $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$

Rq 23 Si $G \neq \{e\}$, cette action n'est pas libre, elle n'est jamais transitive

Appli 24 Soit p premier, G p-groupe non trivial alors le centre de G est non trivial. En particulier, si $|G| = p^2$, G est abélien

Appli 25 Soit G groupe fini non abélien, $C = \{(a,b),\ ab = ba,\ a,b \in G\}$ alors $\frac{|C|}{|G|^2} \leqslant \frac{5}{8}$

Appli 26 Avec les notations de l'appli 18, (i) Les p-Sylow sont conjugués
(ii) Si N_p est le nombre de p-Sylow de G, $N_p \equiv 1\ [p]$ et $N_p \mid q$

IV - Actions de Groupe sur les Espaces de Matrices

1) Actions de Groupes Matriciels

On fixe $\mathbb{K}$ un corps, $m, n \in \mathbb{N}^*$ des entiers

Def 27 On appelle action par équivalence l'action de $G = GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$ sur $\mathcal{M}_{m,n}(\mathbb{K})$ définie par
$$G \times \mathcal{M}_{m,n}(\mathbb{K}) \to \mathcal{M}_{m,n}(\mathbb{K})$$
$$((P,Q), A) \mapsto PAQ^{-1}$$

Th 28 Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$, l'orbite de A sous l'action par équivalence est $\mathcal{O}_A = \{B \in \mathcal{M}_{m,n}(\mathbb{K}),\ \mathrm{rg}\, A = \mathrm{rg}\, B\}$

Coro 29 Soit p premier, $k \in \mathbb{N}^*$, $q = p^k$, $r \in [\![1, \min(m,n)]\!]$. Le nombre de matrices de rang r ~~dans~~ $\mathcal{M}_{m,n}(\mathbb{F}_q)$ est $q^{\frac{1}{2}[(m-r)(m-r-1) + (n-r)(n-r-1)]} \prod_{i=1}^{m-r} (q^{r_i} - 1) \prod_{j=1}^{n-r} (q^{n_j} - 1)$

Def 30 On appelle action par similitude l'action de $GL_n(\mathbb{K})$ sur $\mathcal{M}_n(\mathbb{K})$ définie par
$$GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$$
$$(P, M) \mapsto PMP^{-1}$$

Th 31 (Réduction de Frobenius) Soit $M \in \mathcal{M}_n(\mathbb{K})$, il existe une unique famille de polynômes unitaires $P_1, \dots, P_r$ telle que pour $i \in \{1, \dots, r-1\}$, $P_{i+1} \mid P_i$ et telle qu'il existe $Q \in GL_n(\mathbb{K})$ telle que $QMQ^{-1} = \begin{pmatrix} C_{P_1} & & 0 \\ & \ddots & \\ 0 & & C_{P_r} \end{pmatrix}$ où C_P est la matrice compagnon du polynôme $P = X^k + \sum_{i=0}^{k-1} a_i X^i$, $C_P = \begin{pmatrix} 0 & & -a_0 \\ 1 & \ddots & \vdots \\ & 1 & -a_{k-1} \end{pmatrix}$,

Les P_i, $i \in \{1, \dots, r\}$ sont appelés invariants de similitude de M

Rq 32 Les orbites de l'action par similitude sont caractérisées par les invariants de similitudes

Coro 33 Avec les notations du théorème 31, P_1 est le polynôme minimal de M et $\prod_{i=1}^{r} P_i$ est son polynôme caractéristique

Appli 34 Pour $n = 2$ ou 3, $M, M' \in \mathcal{M}_n(\mathbb{R})$ sont semblables ssi elles ont même polynôme minimal et même polynôme caractéristique

Th 35 La restriction de l'action par similitude aux matrices diagonalisables sur $\mathbb{K}$ est bien définie. Les orbites de cette action sont caractérisées par le spectre

Appli 36 Soit p premier, $r \in \mathbb{N}^*$, $q = p^r$. On note $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables sur $\mathbb{F}_q$ alors
$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1 + \dots + n_q = n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$$

Def 37 On appelle action par congruence l'action de $GL_n(\mathbb{K})$ sur $\mathcal{S}_n(\mathbb{K})$ définie par
$$GL_n(\mathbb{K}) \times \mathcal{S}_n(\mathbb{K}) \to \mathcal{S}_n(\mathbb{K})$$
$$(P, A) \mapsto PA{}^tP$$

Def 38 (i) Le discriminant de $A \in GL_n(\mathbb{K}) \cap \mathcal{S}_n(\mathbb{K})$, noté $\delta(A)$ est la classe de $\det A$ dans $\mathbb{K}^* / (\mathbb{K}^*)^2$ où $(\mathbb{K}^*)^2 = \{x^2 ; x \in \mathbb{K}^*\}$

(ii) $\mathbb{K} = \mathbb{R}$, on pose $p(A) = \max\{\dim F,\ F \subset \mathbb{R}^n,\ \forall x \in F \setminus \{0\},\ x A {}^t x > 0\}$ et $s = \mathrm{rg}(A) - p(A)$
(p, s) est appelé signature de A

Th 39 (i) $\mathbb{K} = \mathbb{C}$, $A, A' \in \mathcal{S}_n(\mathbb{C})$, $\mathrm{Orb}(A) = \mathrm{Orb}(A') \iff \mathrm{rg}\, A = \mathrm{rg}\, A'$
(ii) $\mathbb{K} = \mathbb{R}$, $A, A' \in \mathcal{S}_n(\mathbb{R})$, $\mathrm{Orb}(A) = \mathrm{Orb}(A') \iff (p(A), s(A)) = (p(A') = s(A'))$
(iii) $\mathbb{K} = \mathbb{F}_q$, q impair $A, A' \in \mathcal{S}_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$ $\mathrm{Orb}(A) = \mathrm{Orb}(A') \iff \delta(A) = \delta(A')$

Appli 40 (Loi de réciprocité quadratique)
Soient p, q premiers impairs, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ où $\left(\frac{\cdot}{p}\right)$ désigne le symbole de Legendre sur $\mathbb{F}_p$

2) Représentations Linéaires de Groupes

Def 41 Soit G un groupe fini, une représentation linéaire de G est la donnée d'un espace vectoriel V sur $\mathbb{C}$ et d'un morphisme $\rho : G \to GL(V)$. C'est une action linéaire de G sur V.
Une sous-représentation de V est un sous-espace vectoriel de V stable par $\rho(g)$ pour tout $g \in G$.
V est dite irréductible si ses seules sous-représentations sont $\{0\}$ et V

Th 42 (Maschke) Soit G groupe fini, (V, ρ) représentation de G. Toute sous-représentation de G admet un supplémentaire stable par G.

Def 43 Soit $\rho : G \to GL(V)$ représentation de G, si V est de dimension finie, on appelle degré de la représentation la dimension de V

Rq 44 Dans la suite, on ne considère que des représentations de degré fini.

Ex 45 Soit G groupe fini opérant sur E fini de cardinal $n \geqslant 1$, on a un morphisme $\varphi : G \to \mathfrak{S}_n$. Soit V $\mathbb{C}$-espace vectoriel de dimension finie n et de base $(v_1, \dots, v_n)$. On pose $\rho(g)(v_i) = v_{\varphi(g)(i)}$ pour $g \in G$, $i \in [\![1, n]\!]$
(V, ρ) est une représentation de G appelée représentation par permutation.

Def 46 Soit G groupe fini, $\rho : G \to GL(V)$ représentation de degré fini de G. Le caractère de ρ est l'application $\chi = \chi_V : \begin{array}{l} G \to \mathbb{C} \\ g \mapsto tr(\rho(g)) \end{array}$

χ est dit irréductible si ρ l'est

Ex 47 La représentation par permutation a pour caractère $\chi : g \in G \mapsto Card\{i,\ \sigma_g(i) = i\}$ où $\varphi(g) = \sigma_g$

DEV ①

Th 48 Soit G un groupe fini, $\chi_1, \dots, \chi_m$ les caractères irréductibles de G et H sous-groupe de G, H est distingué dans G ssi $H = \bigcap_{j \in J} \ker(\chi_j)$, $J \subset \{1, \dots, m\}$

où $\ker(\chi_j) = \{g \in G,\ \chi(g) = \chi(e)\}$

Appli 49 Soit D_6 le groupe diédral à 12 éléments, les sous groupes distingués de D_6 sont $\{e\}$, $\langle r \rangle$, $\langle s, r^2 \rangle$, $\langle sr, r^2 \rangle$, $\langle r^3 \rangle$, $\langle r^2 \rangle$ et D_6

III - Actions et Géométrie

1) Demi-Plan de Poincaré et Groupe Modulaire

Def 50 On note $\mathbb{H} = \{z \in \mathbb{C},\ Im(z) > 0\}$ le demi plan de Poincaré

et $D = \{z \in \mathbb{H},\ |z| \geq 1,\ -\frac{1}{2} \leq Re(z) \leq \frac{1}{2}\} \subset \mathbb{H}$

Def 51 On pose $SL_2(\mathbb{Z}) = \{g \in GL_2(\mathbb{Z}),\ det(g) = 1\}$

DEV ②

Prop 52 $SL_2(\mathbb{Z})$ agit sur $\mathbb{H}$ via $\begin{array}{l} SL_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \dfrac{az+b}{cz+d} \end{array}$

Th 53 Soit $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$

$SL_2(\mathbb{Z})$ est engendré par S et T

Coro 54 Soit $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \{\pm I_2\}$, $PSL_2(\mathbb{Z}) = \langle S, T \mid S^2, (ST)^3 \rangle$

2) Groupes d'isométrie Affines

Def 55 Soit $n \geq 1$, $X \subset \mathbb{R}^n$. On note $Is(X)$ (resp. $Is^+(X)$) le sous-groupe des isométries affines (resp. positives) de $\mathbb{R}^n$ qui stabilisent X

Th 56 On note T_4 le tétraèdre et C_6 le cube, alors $Is(T_4) \simeq \sigma_4$ et $Is^+(T_4) \simeq A_4$

et $Is(C_6) \simeq \sigma_4 \times \mathbb{Z}/2\mathbb{Z}$, $Is^+(C_6) \simeq \sigma_4$

Th 57 $r > 0$, on définit le simplexe régulier t_n par récurrence
- $A_0, A_1 \in \mathbb{R}$, $d(A_0, A_1) = r$ $\quad t_1 = (A_0, A_1)$
- $t_n = (A_0, \dots, A_n)$, $A_n \in \mathbb{R}^n$ $\quad d(A_n, A_i) = r$ pour $i \leq n-1$

$\forall n \geq 1$, $Is(t_n) \simeq \sigma_{n+1}$ et $Is^+(t_n) \simeq A_{n+1}$