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

I Généralités

[Odi23] Tout groupe G sera noté multiplicativement.

I.1 Premières actions de groupes

Déf 1. Soit G un groupe et X un ensemble non vide. Une action (à gauche) de G sur X est une application : $\left\{ \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g,x) & \longmapsto & g \cdot x \end{array} \right.$ Telle que :

i) Pour tout $x \in X$, $e \cdot x = x$, où e désigne l'élément neutre de G.

ii) Pour tous $g, h \in G$, pour tout $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$.

Ex 2.

1. Le groupe G agit sur lui même :
   (a) Par translation à gauche : $g \cdot x = gx$, pour tous $g, x \in G$.
   (b) Par conjugaison : $g \cdot x = gxg^{-1}$, pour tous $g, x \in G$.
2. Soit $\mathbb{K}$ un corps commutatif, $n \in \mathbb{N}^*$. Le groupe $GL_n(\mathbb{K})$ agit sur $\mathbb{K}^n$: $A \cdot X = AX$, pour tous $A \in GL_n(\mathbb{K})$, $X \in \mathbb{K}^n$.
3. Soit X un ensemble non vide, $\mathfrak{S}(X)$ le groupe symétrique de X. Alors $\mathfrak{S}(X)$ agit sur X par $\sigma \cdot x = \sigma(x)$, pour tous $\sigma \in \mathfrak{S}$, $x \in X$.

Thm 3. Soient G un groupe et X un ensemble non vide. Pour tous $g \in G$, $x \in X$, $g \cdot x$ définit une action de G sur X, si et seulement si, l'application $\Phi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathfrak{S}(X) \\ g & \longmapsto & \Phi_g : \left\{ \begin{array}{ccc} X & \to & X \\ x & \mapsto & g \cdot x \end{array} \right. \end{array} \right.$ est un morphisme de groupes.

Déf 4. Soit G un groupe opérant sur un ensemble X.

1. On dit que l'action est transitive si : $\forall x, y \in X$, $\exists g \in G$, $g \cdot x = y$.
2. On dit que l'action est libre si : $\forall x \in X$, $g \cdot x = x \Rightarrow g = e$.
3. On dit que l'action est fidèle si Φ est injectif, ie, $g \cdot x = x$ pour tout $x \in X$ implique $g = e$
4. On dit que l'action est simplement transitive si elel est transitive et libre. Autrement dit, $\forall x, y \in X$, $\exists! g \in G$, $g \cdot x = y$.

Ex 5. L'action de G par translation à gauche sur lui-même est fidèle.

Thm 6 (Cayley)**.** Si G est un groupe fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

I.2 Orbites et stabilisateurs

Soit G un groupe agissant sur un ensemble X, on associe à cette action l'application Φ.

Déf 7. Soit $x \in X$.

1. L'orbite de x est $G \cdot x := \{g \cdot x : g \in G\}$
2. Le stabilisateur de x est $\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$

Rq 8. On dira alors qu'une action est transitive si elle n'admet qu'une seule orbite.

Ex 9. Si G opère sur lui même par conjugaison, l'orbite de $h \in G$ est constituée des éléments qui commutent avec h.

Ex 10. Si X n'est pas réduit à un point, on considère l'action de $G := \mathfrak{S}(X)$ sur X définit à l'exemple 2. Alors pour tout $x \in X$, $\mathrm{Stab}_G(x) \simeq \mathfrak{S}(X \backslash \{x\})$.

Prop 11. Pour tout $x \in X$, $\mathrm{Stab}_G(x)$ est un sous-groupe de G. De plus, $\ker \Phi = \bigcap_{x \in X} \mathrm{Stab}_G(x)$. Donc $\ker \Phi$ est un sous-groupe distingué de G.

Prop 12. Pour tout $x \in X$, l'application $f_x : \left\{ \begin{array}{ccc} G/\mathrm{Stab}_G(x) & \longrightarrow & G \cdot x \\ g\,\mathrm{Stab}_G(x) & \longmapsto & g \cdot x \end{array} \right.$ est une bijection.

Cor 13 (Equation des classes)**.** Si G et X sont finis, alors pour tout $x \in X$, $|G| = |G \cdot x||\mathrm{Stab}_G(x)|$

Prop 14. Soient $x, y \in X$. La relation $x \sim y$, si et seulement si, il existe $g \in G$, $g \cdot x = y$, est une relation d'équivalence. Il découle que les orbites de l'action de G sur X forment une partition de X.

Rq 15. Les orbites formant une partition de X, on peut fixer un système de représentant que l'on note Ω.

Cor 16 (Equation aux classes)**.** Si G et X sont finis, alors $|X| = \sum_{x \in \Omega} |G \cdot x| = \sum_{x \in \Omega} \frac{|G|}{|\mathrm{Stab}_G(x)|}$

Thm 17 (Formule de Burnside)**.** On suppose G et X finis. Pour tout $g \in G$, on note $\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\}$ l'ensemble des points fixes de g. Alors $|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

Notation 18. On note $X^G := \{x \in E : G \cdot x = \{x\}\}$ l'ensemble des éléments de X dont l'orbite est réduite à un point.

Déf 19. Soit p un nombre premier. On dit que G est un p-groupe si $|G| = p^\alpha$, où $\alpha \in \mathbb{N}^*$.

Prop 20. Soient p un nombre premier et G un p-groupe agissant sur un ensemble fini X. Alors $|X| \equiv |X^G| \pmod p$.

Cor 21 (Théorème de Cauchy)**.** Soit G un groupe fini d'ordre $n \geq 2$. Soit p un nombre premier tel que $p \mid n$. Alors il existe un élément d'ordre p.

II Actions matricielles

Soit $\mathbb{K}$ un corps commutatif.

II.1 Action par équivalence

[Rom21] Soient $n, m \in \mathbb{N}^*$

Thm 22. $GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$ définit une action sur $M_{n,m}(\mathbb{K})$: $\forall (P,Q) \in GL_n(\mathbb{K}) \times GL_m(\mathbb{K})$, $\forall M \in M_{n,m}(\mathbb{K})$, $(P,Q)\cdot M = PMQ^{-1}$. On l'appelle action par équivalence.

Déf 23. Deux matrices $A, B \in M_{n,m}(\mathbb{K})$ sont dites équivalentes si elles sont dans la même orbite pour cette action.

Thm 24 (Invariant total)**.** Deux matrices sont équivalentes, si et seulement si, elles ont même rang. Entre autre, toute matrice de rang r est équivalente à $\begin{pmatrix} I_r & 0_{r,m-r} \\ 0_{n-r,r} & 0_{n-r,m-r} \end{pmatrix}$.

II.2 Actions matricielles sur les quaternions

[CG17]

Déf 25. On appelle corps des quaternions, et l'on note $\mathbb{H}$ l'algèbre de dimension 4 sur le corps des réels, ayant pour base $(\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k})$, dans laquelle la multiplication est définie par :

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \text{ et } \mathbf{ijk} = -1.$$

Notation 26. On note $SU_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : |a|^2 + |b|^2 = 1 \right\}$.

Prop 27. $SU_2(\mathbb{C})$ est un sous-groupe de $GL_2(\mathbb{C})$, homéomorphe avec $\mathbb{S}^3$.

Notation 28. On note $H^* \simeq \mathbb{R}_+^* I_2 \times SU_2(\mathbb{C}) \subseteq GL_2(\mathbb{C})$.

Thm 29. $\mathbb{H} \simeq H^* \cup \{0\}$. On notera alors $\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : a, b \in \mathbb{C} \right\}$.

Notation 30.

1. Si $x, y, z, t \in \mathbb{R}$, et si l'on note $a = x + iy$, $b = z + it$, un élément de $\mathbb{H}$ s'écrit $h = x\mathbf{1} + y\mathbf{i} + z\mathbf{j} + t\mathbf{k} = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$.
2. On note $\overline{h} = x\mathbf{1} - y\mathbf{i} - z\mathbf{j} - t\mathbf{k}$ le conjugué de h.
3. On note $N(h) = \det h = |a|^2 + |b|^2 = x^2 + y^2 + z^2 + t^2$.
4. On note $\mathbb{I} = \mathrm{Vect}_{\mathbb{R}}(\mathbf{i}, \mathbf{j}, \mathbf{k})$.

Prop 31. N définit une norme sur $\mathbb{H}$, et $N(hh') = N(h)N(h')$ pour tout $h, h' \in \mathbb{H}$.

Thm 32. $\mathbb{H}$ est une sous-algèbre de $M_2(\mathbb{C})$. De plus, c'est un corps non commutatif. Son centre est $\mathbb{R}$.

Prop 33. $SU_2(\mathbb{C})$ agit par conjugaison sur $\mathbb{H}$. $SU_2(\mathbb{C}) \times SU_2(\mathbb{C})$ agit par équivalence sur $\mathbb{H}$.

Thm 34 (DEV 1)**.** Il existe deux isomorphismes de groupes :

1. $SU_2(\mathbb{C})/\{\pm I_2\} \simeq SO_3(\mathbb{R})$.
2. $SU_2(\mathbb{C}) \times SU_2(\mathbb{C})/\{(I_2, I_2), (-I_2, -I_2)\} \simeq SO_4(\mathbb{R})$.

II.3 Action par congruence

[Rom21] Soit $n \in \mathbb{N}^*$, $\mathcal{S}_n(\mathbb{K})$ l'ensemble des matrices symétriques.

Thm 35. $GL_n(\mathbb{K})$ opère sur $\mathcal{S}_n(\mathbb{K})$ par : $\forall P \in GL_n(\mathbb{K})$, $\forall M \in \mathcal{S}_n(\mathbb{K})$, $P \cdot M = PA^tP$

Déf 36. Deux matrices dans la même orbite pour cette action sont dites congruentes.

Lemme 37. Soit q une forme quadratique sur $\mathbb{K}^n$, il existe une base de $\mathbb{K}^n$ telle que la matrice de q est diagonale.

Notation 38. Soit $A \in \mathcal{S}_n(\mathbb{R})$ et q sa forme quadratique sur $\mathbb{R}^n$ canoniquement associée. On note $p(A) = \max\{\dim F : F \subseteq \mathbb{R}^n,\ \forall x \in F,\ q(x) > 0\}$.

Thm 39 (Invariants totaux)**.** 1. Si $\mathbb{K} = \mathbb{C}$, deux matrices symétriques sont congruentes, si et seulement si, elles ont même rang. Entre autre, toute matrice symétrique complexe de rang r est congruente à $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$

2. Si $\mathbb{K} = \mathbb{R}$, deux matrices A, B symétriques sont congruentes, si et seulement si, elles ont même rang et $p(A) = p(B)$. Entre autre, pour toute matrice symétrique réelle de rang r, et telle que $s := p(A)$, A est congruente à $\begin{pmatrix} I_s & 0 & 0 \\ 0 & I_{r-s} & 0 \\ 0 & 0 & 0 \end{pmatrix}$

3. Si $\mathbb{K} = \mathbb{F}_q$, deux matrices symétriques inversibles sont congruentes, si et seulement si, elles ont même déterminant modulo les carrés de $\mathbb{F}_q^*$. Entre autre, toute matrice symétrique inversible sur $\mathbb{F}_q$ est congruente à $\begin{pmatrix} I_{n-1} & 0 \\ 0 & \varepsilon_n \end{pmatrix}$ Où $\varepsilon_n \in \{1, \xi\}$, $\xi \notin \mathbb{F}_q^{*[2]} := \{x^2 : x \in \mathbb{F}_q^*\}$.

App 40 (DEV 2 - Loi de réciprocité quadratique)**.** Soient p, q deux nombres premiers impairs distincts. On note pour tout $x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = 1$ si $x \in \mathbb{F}_p^{*[2]}$, -1 sinon. Alors :

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

III Applications

III.1 Espaces affines

[Rom21] On considère un espace vectoriel sur $\mathbb{R}$ de dimension finie n, noté $\overrightarrow{E}$, et un ensemble E non vide.

Déf 41. E est un espace affine associé à $\overrightarrow{E}$ si $(\overrightarrow{E}, +)$ agit de façon simplement transitive sur E. Si $\overrightarrow{E}$ est de dimension n, on dit que E est de dimension n. On appelle vecteur tout élément de $\overrightarrow{E}$ et point tout élément de E.

Notation 42. $\forall \overrightarrow{u} \in \overrightarrow{E}$, $\forall M \in E$, $\overrightarrow{u} \cdot M =: M + \overrightarrow{u}$. On note $\overrightarrow{AB}$ le vecteur $\overrightarrow{u}$ tel que $A = B + \overrightarrow{u}$.

Ex 43. L'espace vectoriel $\overrightarrow{E}$ est aussi un espace affine associé à $\overrightarrow{E}$.

Prop 44 (Relation de Chasles)**.** $\forall A, B, C \in E$, $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$

Déf 45. Soient E, F deux espaces affines associés à $\overrightarrow{E}, \overrightarrow{F}$. On dit qu'une application $f : E \to F$ s'il existe une application linéaire $l \in \mathscr{L}(\overrightarrow{E}, \overrightarrow{F})$ telle que pour tout $(M, \overrightarrow{u}) \in E \times \overrightarrow{E}$, $f(M + \overrightarrow{u}) = f(M) + l(\overrightarrow{u})$.

Prop 46. Pour toute application affine f, il existe une unique application linéaire associée. On la note alors $\overrightarrow{f}$.

Thm 47. L'ensemble des applications affines bijectives de E dans E est un groupe pour la loi de composition. On l'appelle groupe affine de E, et on le note $GA(E)$.

Prop 48. $GA(E)$ opère sur E par l'action $\forall (f, M) \in GA(E) \times E$, $f \cdot M = f(M)$. Une telle action est transitive.

Prop 49. Le stabilisateur de $M \in E$ pour cette action est le sous-groupe de $GA(E)$: $GA_M(E) = \{f \in GA(E) : f(M) = M\}$, formé des applications affines bijectives qui fixent le point M.

Cor 50. Pour tout $M \in E$, l'application $f \mapsto \overrightarrow{f}$ réalise un isomorphisme de groupes de $GA_M(E)$ dans $GL(\overrightarrow{E})$.

III.2 Dénombrement sur les corps finis

[CG17] Soit $\mathbb{F}_q$ un corps fini à q éléments, $n \in \mathbb{N}^*$.

Prop 51. Pour tout corps $\mathbb{K}$, $\mathbb{K}^*$ agit par homotéthie sur $\mathbb{K}^{n+1}\backslash\{0\}$. C'est à dire, $\forall (\lambda, x) \in \mathbb{K}^* \times \mathbb{K}^{n+1}\backslash\{0\}$, $\lambda \cdot x = \lambda x$.

Cor 52. Soit l'espace projectif $\mathbb{P}^n(\mathbb{F}_q) := D \subseteq \mathbb{F}_q^{n+1} : \dim D = 1\}$. Alors $|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + \ldots + q^n$.

Prop 53. Soit E un $\mathbb{K}$ espace vectoriel de dimension n. Pour tout $k \in [\![0, n]\!]$, on définit $\mathcal{E}_k := \{(F, G) : \dim F = k,\ F \oplus G = E\}$. Alors $GL(E)$ agit transitivement sur $\mathcal{E}_k$ par : $\forall g, (F, G) \in GL(E) \times \mathcal{E}_k$, $g \cdot (F, G) = (g(F), g(G))$.

Cor 54. Le nombre de matrices nilpotentes de $M_n(\mathbb{F}_q)$ est $q^{n(n-1)}$.

Bibliographie

[CG17] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome second*. Calvage et Mounet, 2017.

[Odi23] Alain Ninet Odile Fleury Loic Foissy. *Algèbre et calcul formel*. 2eme edition. ellipses, 2023.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation : Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 2021.