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

Références : Perrin, Rombaldi, Ulmer, Berhuy, Caldero (dev)

I - Généralités sur les actions de groupes
1) Actions, orbites, stabilisateurs
2) Application au dénombrement

II - Agir pour mieux connaître le groupe
1) Action par translation
2) Action par conjugaison
3) Action sur un quotient
4) Exemple du groupe symétrique $\mathfrak{S}_n$
5) Application aux théorèmes de Sylow

III - Agir pour mieux connaître l'ensemble
1) Actions sur les espaces de matrices
   a) Par translation
   b) Action de Steinitz
   c) Par conjugaison
2) Géométrie affine

DEV 1 : Cône nilpotent

DEV 2 : Wedderburn

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

Soit G un groupe de neutre e_G et X un ensemble non vide.

I - Généralités sur les actions de groupes

1) Actions, orbites, stabilisateurs [PER]

DEF 1 : On dit que G opère (ou agit) sur X lorsqu'on a une application, appelée action : $\begin{array}{l} G\times X \longrightarrow X \\ (g,x) \longmapsto g\cdot x \end{array}$ vérifiant :

1) $\forall g, g' \in G, \forall x \in X, g\cdot(g'\cdot x) = gg'\cdot x$
2) $\forall x \in X, e_G \cdot x = x$.

PROP 2 : La donnée d'une action est équivalente à celle d'un morphisme $\varphi : G \longrightarrow \mathfrak{S}(X)$, $g \longmapsto \varphi_g : \begin{array}{l} X \longrightarrow X \\ x \longmapsto g\cdot x \end{array}$

DEF 3 : On dit que G opère transitivement sur X lorsqu'on a : $\forall x \in X, \forall y \in X, \exists g \in G, g\cdot x = y$

DEF 4 : On dit que G opère fidèlement lorsque φ est injectif i.e : $g\cdot x = x \ \forall x \in X \Rightarrow g = e_G$.

PROP 5 : La relation sur X : $x R y \Leftrightarrow \exists g \in G, y = g\cdot x$ est une relation d'équivalence. Elle mesure le défaut de transitivité

DEF 6 : La classe de $x \in X$ modulo R est appelée orbite de x et notée $Orb(x)$. G opère transitivement sur $Orb(x)$.

REM 7 : Les orbites partitionnent X.
. Une action est transitive $\Leftrightarrow \forall x \in X, Orb(x) = X$.

EX 8 : $\mathfrak{S}_n$ opère sur $[\![1;n]\!]$ fidèlement et transitivement via $(\sigma, i) \mapsto \sigma(i)$.

DEF 9 : On appelle stabilisateur de $x \in X$ sous l'action de G l'ensemble $Stab(x) = \{g \in G / g\cdot x = x\}$.

PROP 10 : $Stab(x)$ est un sous-groupe de G.

2) Application au dénombrement [PER] [CAL] G fini, X fini

PROP 11 : Soit G agissant sur X. On a une bijection d'ensembles : $\begin{array}{l} G/Stab(x) \longrightarrow Orb(x) \\ g\,Stab(x) \longmapsto g\cdot x \end{array}$

COR 12 : On a donc : $\forall x \in X, \#G = \#Stab(x)\,\#Orb(x)$.

THM 13 : (Equation aux classes) G agit sur X. Soit S un système de représentants des orbites. Alors :

$$\#X = \sum_{x\in S} \#Orb(x) = \sum_{x \in S} \frac{\#G}{\#Stab(x)}.$$

Soit $q = p^n$, p premier, $n \geq 1$. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension finie.

LEMME 14 (Fitting) : Soit $u \in \mathcal{L}(E)$. Les suites $(\ker(u^n))_{n\in\mathbb{N}}$ et $(Im(u^n))_{n\in\mathbb{N}}$ sont respectivement croissante et décroissante et stationnent à partir d'un même rang n_0. De plus, $E = \ker(u^{n_0}) \oplus Im(u^{n_0})$, $v = u_{|\ker(u^{n_0})}$ est un endomorphisme nilpotent et $w = u_{|Im(u^{n_0})}$ est un automorphisme.

DEV 1

THM 15 : Il y a $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d\times d$ à coefficients dans $\mathbb{F}_q$.

PROP 16 : (Formule de Burnside) Soit Ω l'ensemble des orbites de X sous l'action de G. Alors :

$$\#\Omega = \frac{1}{\#G}\sum_{g\in G} \#Fix(g) \text{ où } Fix(g) = \{x \in X / g\cdot x = x\}.$$

II - Agir pour mieux connaître le groupe

1) Action par translation [PER]

DEF 17 : On fait agir G sur lui-même par translation à gauche : $\begin{array}{l} G\times G \longrightarrow G \\ (g,a) \longmapsto ga \end{array}$

PROP 18 : Cette action est simplement transitive au sens où : $\forall a, b \in G, \exists! g \in G, ga = b$

THM 19 : (Cayley) Si G est fini de cardinal n, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

2) Action par conjugaison [PER]

DEF 20 : On fait agir G sur lui-même par conjugaison (on dit aussi par automorphisme intérieur) : $\begin{array}{l} G\times G \longrightarrow G \\ (g,h) \longmapsto ghg^{-1} \end{array}$ Les orbites s'appellent alors classes de conjugaison

Le stabilisateur de a s'appelle centralisateur

DEF 21: On définit le centre de G par $Z(G)=\{g\in G / \forall h\in G, gh=hg\}$

DEF 22: On dit que G est un p-groupe lorsque G est de cardinal une puissance d'un nombre premier.

THM 23 (Equation aux classes pour les p-groupes) Soit G un p-groupe agissant sur X et $X^G=\{x\in X / \forall g\in G, g\cdot x=x\}$ alors on a $\#X\equiv\#X^G \mod p$.

THM 24: Le centre d'un p-groupe n'est pas réduit à $\{e_G\}$.

DEV 2

THM 25: (Wedderburn) Tout corps fini est commutatif

3) Action sur un quotient [PER]

Soit H un sous-groupe de G.

DEF 26: G opère par translation sur G/H en posant : $g.(aH)=(ga)H$.

PROP 27: Cette action est transitive mais pas fidèle en général : $\ker(\varphi)=\bigcap_{a\in G} aHa^{-1}$

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

4) Exemple du groupe symétrique $\mathfrak{S}_n$ [ROM] [ULM]

THM 29. Tout $\sigma\in\mathfrak{S}_n$, $\sigma\neq Id$ se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près des facteurs.

PROP 30: Si $\sigma=\gamma_1\cdots\gamma_p$ est une telle décomposition on a alors $Supp(\sigma)=\bigcup_{i=1}^{p} Supp(\gamma_i)$ et l'ordre de σ est le PPCM des ordres des γ_i

DEF 31: Soit $n\in\mathbb{N}$. On appelle type d'une permutation $\sigma\in\mathfrak{S}_n$ et on note $[l_1,\dots,l_m]$ la liste des cardinaux l_i des orbites dans $[\![1;n]\!]$ de l'action $\langle\sigma\rangle \circlearrowright \mathfrak{S}_n$ du groupe $\langle\sigma\rangle$ sur $[\![1;n]\!]$ rangée en ordre croissant.

REM 32: En d'autres termes, λ_k est le nombre de k-cycles dans la décomposition de σ, λ_1 est le nombre de points fixes.

PROP 33. σ et ρ sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont même type.

EX 34: $\sigma=(163)(24)$ et $\rho=(14)(235)$ sont conjuguées

COR 35: Les classes de conjugaison sont en bijection avec les partitions de $[\![1;n]\!]$: il y en a :

$$B_n=\frac{1}{e}\sum_{k=0}^{+\infty}\frac{k^n}{k!}$$

THM 36: $\forall n\geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles

LEMME 37: Les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$ pour $n\geq 5$.

THM 38: Pour $n=3$ et $n\geq 5$, $\mathfrak{A}_n$ est simple.

5) Application aux théorèmes de Sylow [BERH]

On suppose G fini d'ordre n et que p est premier

DEF 39: Écrivons $\#G=p^m q$ avec $p\nmid q$ et $m\geq 0$. On appelle p-sous-groupe de Sylow ou p-Sylow tout sous-groupe de G d'ordre p^m

EX 40: $\mathbb{Z}/6\mathbb{Z}$ contient un 2-Sylow et un 3-Sylow

THM 41: (Sylow) . Il existe des p-Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow
. Le conjugué d'un p-Sylow de G est encore un p-Sylow de G et tous les p-Sylow sont conjugués. En particulier, si S est un p-Sylow de G, $S \triangleleft G \Leftrightarrow S$ est unique.
. Si n_p est le nombre de p-Sylow de G, $n_p\equiv 1 \mod p$ et $n_p | q$.

EX 42: Un groupe d'ordre 63 n'est pas simple.

THM 43: (Cauchy) G possède au moins un élément d'ordre p.

III - Agir pour mieux connaître l'ensemble

1) Action sur les espaces de matrices [ROM] $K=\mathbb{R}$ ou $\mathbb{C}$

a) Par translation

PROP 44: $GL_n(K)$ agit sur $\mathcal{M}_{n,m}(K)$ par translation à gauche : $GL_n(K)\times\mathcal{M}_{n,m}(K)\longrightarrow\mathcal{M}_{n,m}(K)$, $(P,A)\longmapsto PA$

Deux matrices sont dans la même orbite si et seulement si elles ont même noyau.

REM 45 : Le noyau est dit invariant total pour cette action

THM 46 : (pivot de Gauss) Toute matrice A de $\mathcal{M}_{n,m}(K)$ est dans l'orbite d'une matrice échelonnée réduite. Celle-ci s'obtient en effectuant des opérations élémentaires sur les lignes de A.

REM 47 : Se ramener à une matrice échelonnée réduite est intéressant pour avoir des informations sur le rang, les relations de liaison, avoir une base de l'image...

b) Action de Steinitz

Soit $G = GL_n(K) \times GL_m(K)$

THM 48 : L'application
$$G \times \mathcal{M}_{n,m}(K) \to \mathcal{M}_{n,m}(K)$$
$$(P, Q, A) \mapsto PAQ^{-1}$$
définit une action dont les orbites sont les ensembles $O_r = \{A \in \mathcal{M}_{n,m}(K) \mid rg(A) = r\}$, $r \in [\![0 ; \min(n,m)]\!]$.
Deux matrices dans la même orbite sont dites équivalentes.

PROP 49 : Deux matrices sont équivalentes si et seulement si elles ont même rang.

THM 50 : Une forme normale de chaque orbite est $J_r = \begin{pmatrix} I_r & (0) \\ (0) & 0 \end{pmatrix}$, $J_r \in \mathcal{M}_{n,m}(K)$.

c) Action par conjugaison

DEF 51 : On définit l'action de $GL_n(K)$ sur $\mathcal{M}_n(K)$ par conjugaison
$$GL_n(K) \times \mathcal{M}_n(K) \to \mathcal{M}_n(K)$$
$$(P, A) \mapsto PAP^{-1}$$
Deux matrices dans la même orbite sont dites semblables.

PROP 52 : Deux matrices semblables ont même rang, même trace, même déterminant, même polynôme caractéristique.

PROP 53 : $A \in \mathcal{M}_n(K)$ est diagonalisable ssi elle est dans la même orbite qu'une matrice diagonale.

THM 54 : Pour $K = \mathbb{C}$, l'orbite de $A \in \mathcal{M}_n(\mathbb{C})$ est fermée si et seulement si A est diagonalisable

2) Géométrie affine

[PAT]

Soit $\vec{E}$ un $\mathbb{R}$-espace vectoriel de dimension finie

DEF 55 : Un espace affine E de direction $\vec{E}$ est un ensemble non vide sur lequel on peut définir une action simplement transitive : $(x, \vec{u}) \in E \times \vec{E} \mapsto x + \vec{u}$.

DEF 56 : Soit $(E, \vec{E})$ un espace affine, $(E', \vec{E'})$ un autre espace affine. Une application $f : E \to E'$ est dite affine lorsqu'il existe $\varphi \in \mathcal{L}(\vec{E}, \vec{E'})$ telle que
$\forall (x, \vec{u}) \in E \times \vec{E}$, $f(x + \vec{u}) = f(x) + \varphi(\vec{u})$

PROP 57 : On munit $\vec{E}$ d'un produit scalaire. On peut alors définir une distance sur E par
$\forall (x,y) \in E^2$, $d(x,y) = \|\vec{xy}\|$.

DEF 58 : On appelle isométrie affine toute application $f : E \to E$ telle que $d(f(x), f(y)) = d(x,y)$ pour tout $(x,y) \in E^2$. On note $Is(E)$ l'ensemble des isométries.

DEF 59 : Soit $P \subset E$, $\# P \geq 2$. On note $Is(P)$ l'ensemble des isométries φ de E qui conservent P.

THM 60 : $Is(\text{Tétraèdre}) \simeq \mathfrak{S}_4$ et $Is(\text{Cube}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.