

Leçon 101 - Groupes opérant sur un ensemble. Exemples et applications.

Cadre : (G, \cdot) est un groupe d'élément neutre e , et X est un ensemble

1. Définitions et premières propriétés. —

1. Actions de groupes. —

- Def : Une action de groupes à gauche de G sur X est la donnée d'un morphisme $\phi : G \rightarrow \text{Bij}(X)$. ϕ est appelé morphisme structurel de l'action.
On note $g.x = \phi(g)(x)$, ainsi que $G \curvearrowright X$.
- Ex : $\text{Bij}(X)$ opère sur X par $f.x = f(x)$.
- Def : L'action de G sur X est fidèle si ϕ est injectif.
L'action de G sur X est transitive si $\forall x, y \in X, \exists g \in G$ tq $y = g.x$.
- Ex : L'action de $\text{Bij}(X)$ sur X est fidèle et transitive.
L'action de $GL(E)$ sur $P(E)$ l'ensemble des droites vectorielles de E est fidèle.
- Def : Soit $x \in X$. On définit le stabilisateur de x : $\text{Stab}(x) := \{g \in G \text{ tq } g.x = x\}$, ainsi que l'orbite de x : $\text{Orb}(x) := \{g.x, g \in G\}$.
- Pro : La relation : xRy ssi $\text{Orb}(x) = \text{Orb}(y)$ est une relation d'équivalence. Ainsi, les orbites pour l'action de G forment une partition de X .
- Rem : G agit transitivement dans chaque $\text{Orb}(x)$.
- Ex : Les orbites de \mathbb{R}^n sous l'action naturelle de $O_n(\mathbb{R})$ sont les sphères de centre l'origine.
- App : Décomposition d'une permutation en produit de cycles à supports disjoints.
- Ex : Le stabilisateur de $x \in \{1, \dots, n\}$ sous l'action de Σ_n est isomorphe à Σ_{n-1} .
- Def : On dit que l'action de G sur X est k -transitive ssi pour tous k -uplets (a_1, \dots, a_k) , (b_1, \dots, b_k) , il existe $g \in G$ tq $g.a_i = b_i \forall i$.
- Ex : L'action de Σ_n sur $\{1, \dots, n\}$ est n -transitive. L'action de A_n sur $\{1, \dots, n\}$ est $(n-2)$ -transitive.
- Def : Une action est libre ssi pour tout $g \in G - \{e\}$, $\phi(g)$ est sans points fixes.
- Pro : libre \Rightarrow fidèle.
- Contre-ex : D_3 agit fidèlement sur les sommets du triangle équilatéral.

2. Action d'un groupe fini sur un ensemble fini. —

- Pro : Soit $G \curvearrowright X$. Pour tout $x \in X, \bar{g} \in G/\text{Stab}(x) \mapsto g.x \in \text{Orb}(x)$ est une bijection.
- Cor : Si G est fini, alors $|\text{Orb}(x)| = \frac{|G|}{|G_x|}$.
- Pro : (Formule des classes) Soit G un groupe fini agissant sur un ensemble fini X , et soit $X = \bigcup_{i=1}^r \text{Orb}(x_i)$ la partition de X en orbites sous l'action de G . On a : $|X| = \sum_{i=1}^r |\text{Orb}(x_i)| = \sum_{i=1}^r (G : \text{Stab}(x_i)) = \sum_{i=1}^r \frac{|G|}{|\text{Stab}(x_i)|}$.
- Def : Pour $A \subset G$ on définit $X^A := \{x \in X \text{ tq } a.x = x \forall a \in A\}$.
- Cor : (Formule de Burnside) Le nombre r d'orbites de X sous l'action de G est : $r = \frac{1}{|G|} \sum_{g \in G} |X^g|$.

- Pro : Soit p premier, G un p -groupe, et X un ensemble fini sur lequel G agit. On a alors $|X^G| \equiv |X| \pmod{p}$.
- App : Le centre d'un p -groupe G est non-trivial.
- App : Les groupes de cardinal p, p^2 sont toujours abéliens.
- App : Théorème de Cauchy : Soit G un groupe et p premier tq $p \mid |G|$. Alors G possède un élément d'ordre p .

2. Actions de groupes et théorie des groupes. —

1. Action par translation. —

- Def : G agit sur lui-même ($X=G$) par translation à gauche via : $\phi(g) = (x \mapsto g.x)$.
- Pro : Cette action est fidèle et transitive.
- App : Théorème de Lagrange : Pour H sous-groupe de $G, |H| \mid |G|$.
- App : Théorème de Cayley : Tout groupe fini G est isomorphe à un sous-groupe transitif de $\Sigma_{|G|}$.
- Def : Soit H un sous-groupe de G . G agit sur l'ensemble des classes à gauche modulo H par $\phi(g)(g'H) = (gg'H)$.
- Pro : Cette action est transitive, mais en général pas fidèle ($\text{Ker}(\phi) = \bigcap_{g \in G} gHg^{-1}$)
- App : Théorème de Frobenius : Soit G groupe fini et H sous-groupe de G tel que $|G/H|$ soit minimal et > 1 . Alors H est distingué dans G .
- App : Les groupes d'ordre pq, p, q premiers, possèdent toujours un sous-groupe distingué non trivial.

2. Action par conjugaison. —

- Def : G agit sur lui-même par conjugaison via $\phi(g)(h) = ghg^{-1}$.
- Pro : Pour $G \neq \{e\}$, cette action n'est pas forcément fidèle, et jamais transitive.
- Contre-ex : Pour $G = \Sigma_n, n \geq 3$, l'action est libre.
- Def : L'orbite de $h \in G$ par conjugaison est appelée classe de conjugaison de h . Deux éléments ayant la même classe de conjugaison sont dits conjugués dans G .
- Rem : Le centre de G est l'ensemble des points fixes par conjugaison.
- Pro : La conjugaison préserve l'ordre d'un élément.
- Ex : Les classes de conjugaison du groupe diédral D_n sont de la forme $\{r^k, r^{-k}\}, \{sr^k, sr^{-k}\}, \forall 1 \leq k \leq \frac{n-1}{2}, \{e\}$ si n impair.
Et de la forme $\{r^k, r^{-k}\}, \{sr^k, sr^{-k}\}, \forall 1 \leq k \leq \frac{n-2}{2}, \{r^{\frac{n}{2}}\}, \{sr^{\frac{n}{2}}\}, \{e\}$ si n pair.
- Pro : i) Si $c \in \Sigma_n$ est un cycle d'ordre $m, c = (a_1, \dots, a_m)$, alors $\forall \tau \in \Sigma_n$, on a $\tau.c.\tau^{-1} = (\tau(a_1), \dots, \tau(a_m))$.
ii) Pour c un k -cycle de Σ_n , la classe de conjugaison de c est l'ensemble des k -cycles de Σ_n .
iii) Si $n \geq 5$, les 3-cycles sont conjugués dans A_n .
- App : A_n est simple pour $n \geq 5$.
- Dev : Soit H l'algèbre à division des quaternions, et G le groupe des quaternions de norme 1. L'action par conjugaison de G sur H laisse $\text{Vect}(i, j, k)$ stable, et induit un morphisme surjectif de G vers $SO_3(\mathbb{R})$. On a alors $G/\{\pm 1\} \simeq SO_3(\mathbb{R})$.

- Rem : Cet isomorphisme, permet de ramener le calcul de l'image d'un vecteur de \mathbb{R}^3 par une rotation à des produits dans \mathbb{H} en identifiant les vecteurs $\vec{i}, \vec{j}, \vec{k}$ du repère orthonormé canonique de \mathbb{R}^3 aux éléments i, j, k de \mathbb{H} .

3. Théorèmes de Sylow. —

- Def : Soit G un groupe fini de cardinal n , et p premier tq $p|n$. Un p -Sylow de G est un sous-groupe de G de cardinal $p^{v_p(n)}$.
- Ex : Le groupe $UT_n(\mathbb{F}_p)$ des matrices triangulaires supérieures avec des 1 sur la diagonale est un p -Sylow de $GL_n(\mathbb{F}_p)$.
- Pro : Soit G un groupe et H un sous-groupe de G . Soit S un p -Sylow de H . Alors il existe un p -Sylow S' de G tel que $S = S' \cap H$.
- Théorèmes de Sylow : Soit G un groupe fini de cardinal n , et p premier divisant n .
 - G admet un p -Sylow.
 - Tous les p -Sylow de G sont conjugués.
 - Le nombre n_p de p -Sylow de G vérifie $n_p | \frac{n}{p^{v_p(n)}}$ et $n_p \equiv 1 \pmod{p}$.
- App : Un p -Sylow de G est distingué ssi $n_p = 1$.
- App : Tout groupe d'ordre 63 possède un sous-groupe distingué non-trivial.
- App : Tout groupe d'ordre pq avec $p < q$ premiers et $q \not\equiv 1 \pmod{p}$ est cyclique.

3. Actions de groupes et algèbre linéaire. —

Cadre : K est un corps.

1. Actions sur des espaces de matrices. —

- Def : On fait agir $GL_n(K) \times GL_m(K)$ sur $M_{n,m}(K)$ par $(P, Q).M = PMQ^{-1}$. Deux matrices de $M_{n,m}(K)$ dans la même orbite sont dites équivalentes.
- Pro : Deux matrices de $M_{n,m}(K)$ sont dans la même orbite ssi elles ont le même rang.
- App : Résoudre un système linéaire $MX = B$ revient à résoudre $(PMQ^{-1})X' = B'$ pour $X' = QX$ et $B' = PB$. Def : On fait agir $GL_n(K)$ sur $M_n(K)$ par $P.M = PMP^{-1}$. Deux matrices de $M_n(K)$ dans la même orbite sont dites semblables.
- Pro : Deux matrices sont semblables ssi elles représentent la même application linéaire sur K^n dans deux bases différentes.
- Pro : Deux matrices semblables ont même rang, trace, déterminant, polynôme caractéristique, polynôme minimal.
- Def+Pro : Soit K un corps et $n \geq 1$. On peut faire agir Σ_n sur $M_n(K)$ par $\sigma.M = (c_{\sigma(1)}, \dots, c_{\sigma(n)})$, où c_1, \dots, c_n sont les colonnes de M . Pour T_σ la matrice dont le coefficient (i, j) vaut 1 si $i = \sigma(j)$ et 0 sinon, appelée matrice de permutation associée à σ , on a $\sigma.M = M.T_\sigma$.
- Pro : $\sigma \in \Sigma_n \mapsto T_\sigma \in GL_n(K)$ définit un morphisme de groupes injectif.
- App : Pour tout groupe fini G , on a ainsi un morphisme de groupes injectif de G vers $GL_{\text{Card}(G)}(K)$.

- **Dev** : Théorème de Brauer : Soit \mathbb{K} un corps de caractéristique quelconque, $n \geq 1$, et $\sigma, \sigma' \in \Sigma_n$.

Alors σ et σ' sont conjuguées si et seulement si $T_\sigma, T_{\sigma'}$ sont semblables dans $GL_n(\mathbb{K})$.

- Def : On fait agir $GL_n(K)$ sur $S_n(K)$ par $P.S = PMP^t$. Deux matrices de $S_n(K)$ dans la même orbite sont dites congruentes.
- Thm : Pour q une forme quadratique sur \mathbb{C}^n , la matrice de la forme polaire de q est congruente à $Diag(I_r, 0)$ pour un $r \leq n$.
- Théorème d'inertie de Sylvester : Pour q une forme quadratique sur \mathbb{R}^n , la matrice de la forme polaire de q est congruente à $Diag(I_p, -I_r, 0)$ avec $p + r \leq n$.
- Théorème : Pour q une forme quadratique sur $\mathbb{F}_{p^m}^n$, la matrice de la forme polaire de q est congruente à $Diag(0, I_r)$ avec $r \leq n$ ou à $Diag(0, I_r, \varepsilon)$ avec $r \leq n - 1$ et ε un non-carré de \mathbb{F}_{p^m} .
- **Dev** : Loi de réciprocité quadratique : Soient p, m des nombres premiers impairs distincts.

$$\text{Alors } \left(\frac{p}{m}\right) = \left(\frac{m}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{m-1}{2}}, \text{ où } \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré mod}(p) \\ 0 & \text{si } x = 0 \text{ mod}(p) \\ -1 & \text{sinon} \end{cases}$$

2. Actions sur des espaces vectoriels : représentations linéaires de groupes finis. —

- Def : Une représentation linéaire ρ sur un groupe fini G est un morphisme de groupes $\rho : G \rightarrow GL(V)$ où V est un \mathbb{C} -ev de dimension finie.
- Def : Le caractère χ_ρ d'une représentation linéaire ρ est l'application $g \in G \mapsto \chi_\rho(g) := Tr(\rho(g)) \in \mathbb{C}$.
- Def : Une sous-représentation d'une représentation $\rho : G \rightarrow GL(V)$ est une représentation $\rho' : G \rightarrow GL(V')$ avec V' s-ev de V tel que $\forall g \in G, V'$ est $\rho(g)$ -stable avec $\rho(g)|_{V'} = \rho'(g)$. Une représentation est dite irréductible si elle n'admet aucune sous-représentation stricte non-triviale. Un caractère irréductible est le caractère d'une représentation irréductible.
- Pro : Orthogonalité des caractères irréductibles pour le produit scalaire donné.
- Pro : Les caractères sont des fonctions centrales.
- Def : Table de caractères.
- Thm : Soit G un groupe d'ordre n . Soient ρ_1, \dots, ρ_r un ensemble de représentants des classes d'isomorphie des représentations irréductibles de G , et soient χ_1, \dots, χ_r les caractères irréductibles associés. On note $K_{\chi_i} := \{g \in G \text{ tq } \chi_i(g) = \chi_i(e)\}$. Alors $K_{\chi_i} = Ker(\rho_i)$ et les sous-groupes distingués de G sont exactement les $\bigcap_{i \in I} K_{\chi_i}$, pour tout $I \subset \{1, \dots, r\}$.
- Cor : G est simple ssi pour tout caractère irréductible χ non-trivial et $\forall g \neq e$ on a $\chi(g) \neq \chi(e)$.
- App : V_4 est le seul sous-groupe distingué non-trivial de A_4 . (Table de caractères en annexe)

– App : Sous-groupes distingués de D_6 . (Table de caractères en annexe)

4. Applications à la géométrie. —

1. Groupe des isométries d'un espace affine. —

– Def : On appelle espace affine un ensemble E sur lequel le groupe additif $(V, +)$ d'un espace vectoriel agit à droite transitivement et librement, via $(\vec{u}, M) \in V \times E \mapsto M + \vec{u}$.

Les éléments de E sont appelés les points, et ceux de V les vecteurs.

– Rem : L'action étant libre et transitive, pour tous points $M, N \in E$, il existe un unique vecteur $\vec{u} \in V$ tel que $M + \vec{u} = N$. On note en général \overrightarrow{MN} ce vecteur.

– Def+Pro : Soit E un \mathbb{R} -espace affine de dimension 3 et X une partie non-vide de E . $O(E)$ désigne le groupe des isométries affines de E . Le sous-groupe $Isom(X) := \{f \in O(E) \text{ tq } f(X) = X\}$ des isométries de l'ensemble X agit naturellement sur X .

On note $Isom^+(X)$ le sous-groupes des isométries de X de déterminant 1.

– Pro : On note Δ_4 le tétraèdre régulier. On a alors $Isom(\Delta_4) \simeq \Sigma_4$ et $Isom^+(\Delta_4) \simeq A_4$.

– Pro : On note C_6 le cube en 3 dimensions. Alors $Isom(C_6) \simeq \Sigma_4 \times \mathbb{Z}/2\mathbb{Z}$ et $Isom^+(C_6) \simeq \Sigma_4$.

2. Groupe projectif. —

V est un K -ev de dimension finie n .

– Pro : L'action naturelle de $GL(V)$ sur $P(V)$ induit une action de $SL(V)$ sur $P(V)$.

– Def : On définit $PGL(V) := GL(V)/(K^*.Id_V)$ et $PSL(V) := SL(V)/(\mathbb{U}_n(K).Id_V)$

– Pro : $PGL(V)$ définit une action sur $P(V)$ qui est fidèle et 2-transitive.

$PSL(V)$ définit une action sur $P(V)$ qui est fidèle et 3-transitive.

– App : Pour p premier et $r \geq 1$, on a $Card(PGL_n(\mathbb{F}_{p^r})) = \frac{Card(GL_n(\mathbb{F}_{p^r}))}{p^r - 1}$ et

$$Card(PSL_n(\mathbb{F}_{p^r})) = \frac{Card(SL_n(\mathbb{F}_{p^r}))}{pgd(p^r, n)}.$$

– App : Quelques isomorphismes exceptionnels : $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) \simeq \Sigma_3$

$$PGL_2(\mathbb{F}_3) \simeq \Sigma_4, PSL_2(\mathbb{F}_3) \simeq A_4.$$

$$PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq A_5$$

Références

Ulmer : Action de groupe, stabilisateur, orbites, fidèle, transitif, k-transitif, propriétés, exemples, décomposition d'une permutation en cycles. Relation orbite-stabilisateur, formule des classes, formule de Burnside, Th de Cauchy, points fixes d'un p -groupe. Action par translation à gauche, Th de Cayley, $G \curvearrowright G/H$ transitive, exemples. Action par conjugaison, classes, centre, prop, exemples. Représentations des groupes finis, Sous-groupes distingués et caractères d'un groupe. Espaces affines. Espaces projectifs, PGL, PSL, propriétés.

Perrin : A_n est $(n-2)$ -transitif. p -Sylow, $UT_n(\mathbb{F}_p)$, Th de Sylow, propriétés, exemples (63,15). Isomorphismes exceptionnels de PGL/PSL.

Caldero, Germoni : $SO_3(\mathbb{R})$ et les quaternions. (Dev) Equivalence matricielle, propriétés.

Congruence matricielle, Classification des formes quadratiques, Loi de réciprocité quadratique. (Dev) Groupe d'isométries d'un solide, exemples.

FGN (Algèbre 1) : Th de Frobenius, groupes d'ordre pq jamais simples.

Gourdon : Similitude matricielle, invariants, propriétés, exemples.

Peyré : Représentations des groupes finis, tables de caractères.

Sans Ref : Th de Brauer. (Dev)

January 23, 2018

Vidal Agniel, École normale supérieure de Rennes