Leçon 101 Groupes opérant sur un ensemble, exemples et applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Cours d'algèbre de Daniel Perrin
3. Théorie des groupes de Félix Ulmer
4. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
5. L'algèbre discrète de la transformation de Fourier de Gabriel Peyré
6. Eléménts d'analyse et d'algèbre de Pierre Colmez

Développements.

1. Théorèmes de Sylow
2. Table des caractères de S_4

Table des matières

1 Groupes opérant sur un ensemble

1.1 Actions transitives et fidèles

(Chapitre 1.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère G un groupe et X un ensemble.

1. Définition : On dit que G agit sur X (à gauche), ce que l'on note $G \curvearrowright X$, s'il existe une application $\cdot : (g, x) \in G \times X \longmapsto g.x \in X$ tel que $1.x = x$ et $g.(g'.x) == gg'.x$
2. Remarque : Autrement dit il existe un morphisme de groupes $\varphi : G \longrightarrow Bij(X)$
3. Exemple : $Bij(X) \curvearrowright X$ par $f.x = f(x)$
4. Définition : On dit que l'action est transitive (respectivement simplement transitive) si $\forall (x, y) \in X^2, \exists g \in G, y = g.x$ (respectivement $\exists !$)
5. Définition : On dit que l'action est fidèle si φ est injectif, ie $\forall g \in G, [\forall x \in X, g.x = x] \Longrightarrow g = 1$
6. Remarque : Une action fidèle et transitive n'est pas nécessairement simplement transitive
7. Exemple : L'action naturelle de S_n sur $[\![1, n]\!]$ définie par $\sigma.x = \sigma(x)$ est transitive et fidèle mais non simplement transitive

1.2 Orbites et stabilisateurs

(Chapitre 1.6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère G un groupe fini et X un ensemble fini.

1. Définition : Soit $x \in X$, alors $Orb_G(x) := \{g.x, g \in G\}$ est l'orbite de x
2. Exemple : $Orb_{S(X)}(x) = X$, $Orb_{O_n(\mathbb{R})}(x) = S(0, \|x\|)$
3. Proposition : Les orbites forment une partition de X
4. Exemple : L'action de G sur une orbite est transitive
5. Définition : Soit $x \in X$, alors $Stab_G(x) := \{g \in G \mid g.x = x\}$ est le stabilisateur de x
6. Exemple : $Stab_{S_n}(x) \simeq S_{n-1}$
7. Théorème : Pour tout $x \in X, \overline{g} \in G/Stab(x) \longmapsto g.x \in Orb(x)$ bijectif
8. Corollaire : Relation orbite-stabilisateur : $|Orb_G(x)| = \frac{|G|}{|Stab_G(x)|}$
9. Application : Si $|X| = n$ alors $|S(X)| = n!$ (Exercice 1.10.17 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
10. Théorème : Formule des classes : En notant $Orb_G(x_i)$ les orbites distinctes de l'action, $|X| = \sum_{i=1}^{r} |Orb_G(x_i)| = \sum_{i=1}^{r} \frac{|G|}{|Stab_G(x_i)|}$
11. Définition : $X^G := \{x \in X, \forall g \in G, g.x = x\}$ est l'ensemble des points fixes de X par G, et $Fix_X(g) := \{x \in X, g.x = x\}$ est l'ensemble des points fixes par g
12. Exemple : Si $G = S_n$ et $X = [\![1, n]\!]$, alors $Fix_X((12)) = [\![3, n]\!]$, et $[\![1, n]\!]^{S_{n-1}} = \{n\}$
13. Théorème : Formule de Burnside : Le nombre d'orbites r est $r = \frac{1}{|G|} \sum_{g \in G} |Fix_X(g)|$

    (Exercice 1.10.18 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

2 Action d'un groupe sur lui-même

2.1 Par translation

(Chapitres 1.4 du Cours d'algèbre de Daniel Perrin, 4.2 de Théorie des groupes de Félix Ulmer et 1.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : L'action par translation (à gauche) de G sur G est définie par $g.a = ga$
2. Proposition : Cette action est simplement transitive
3. Application : Théorème de Cayley : Si $|G| = n$ alors G est isomorphe à un sous-groupe de S_n
4. Proposition : Soit H un sous-groupe de G, alors H agit sur G par translation par restriction
5. Application : Théorème de Lagrange : Dans ce cas $|H| \mid |G|$
6. Définition : Soit H un sous-groupe de G, alors l'action par translation à gauche de G sur G/H est définie par $g.g'H = gg'H$
7. Proposition : Cette action transitive
8. Remarque : Si $[G : H] = n$ alors cette action correspond à un morphisme $\varphi : G \longrightarrow S_n$
9. Exemple : $GL_2(\mathbb{F}_2)$ est isomorphe à S_3 en considérant le sous-groupe $H = \left\langle \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right\rangle$ d'ordre 2 et d'indice 3
10. Application : Si $|G| = n$, soit H un sous-groupe de G d'indice k tel que n ne divise pas $k!$, alors il existe un sous-groupe distingué N de G distinct de $\{1\}$ et inclus dans H

2.2 Par conjugaison

(Chapitres 1.4 du Cours d'algèbre de Daniel Perrin et 4.3 de Théorie des groupes de Félix Ulmer)

1. Définition : L'action par conjugaison de G sur G est définie par $g.h = ghg^{-1}$
2. Définition : Les orbites sont appelés classes de conjugaison $Conj(h)$ et les stabilisateurs sont appelés centralisateur $Z(g)$
3. Remarque : Si $G \neq \{1\}$ alors cette action n'est ni libre ni transitive
4. Remarque : $Z(G) = \{g \in G, \forall h \in G, ghg^{-1} = h\}$ est appelé le centre de G
5. Exemple : Dans S_n la classe de conjugaison d'un k-cycle est l'ensemble des k-cycles de S_n, dans A_n la classe d'un 3-cycle est l'ensemble des 3-cycles dans A_n
6. Proposition : Soit $h \in G$, alors $h \in Z(G) \Longleftrightarrow Orb(h) = Conj(h) = \{h\}$
7. Exemple : Dans D_{2n}, on a $Conj(r^i) = \{r^i, r^{-i}\}$, et $Conj(s) = \left\{ \begin{array}{lll} \{r^i s, 0 \leq i \leq n-1\} & si & n\ impair \\ \{r^{2i} s, 0 \leq i \leq \frac{n}{2}\} & si & n\ pair \end{array} \right.$, de plus $Z(D_{2n}) = \left\{ \begin{array}{ll} \{id\} & si\ \ n\ impair \\ \{id, r^{\frac{n}{2}}\} & si\ \ n\ pair \end{array} \right.$
8. Définition : L'action de G par conjugaison sur l'ensemble des sous-groupes de G est définie par $g.H = gHg^{-1}$

9. Proposition : Soit H un sous-groupe de G, alors $H \triangleleft G$ si et seulement si H est un point fixe de cette action
10. Définition : Soit H un sous-groupe de G, alors $N_G(H) = Stab_G(H)$ pour cette action
11. Remarque : $H \triangleleft N_G(H)$ et $N_G(H)$ est le plus grand sous-groupe de G avec cette propriété
12. Exemple : Dans S_3 les trois sous-groupes à deux éléments sont conjugués et sont leurs propres normalisateurs
13. Proposition : $Stab_G(g.x) = gStab_G(x)g^{-1}$

2.3 Applications à l'étude des p-sous-groupes

(Chapitres 1.4 et 1.5 du Cours d'algèbre de Daniel Perrin et 1.7 et 1.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

On considère G un groupe d'ordre $p^\alpha m$ avec p premier et ne divisant pas m.

1. Défintion : On dit que G est un p-groupê si $|G| = p^\alpha$
2. Proposition : Si G est un p-groupe agissant sur X fini alors $|X| \equiv |X^G|[p]$
3. Application : En considérant l'action de $\langle (1...n) \rangle < S_n$ sur $E = \{(g_1, ..., g_p) \in G^p, g_1...g_p = 1\}$, alors on peut montrer le théorème de Cauchy
4. Théorème de Cauchy : Il existe un élément d'ordre p dans G
5. Application : Un groupe abélien d'ordre pq avec p et q premiers distincts est cyclique
6. Définition : Soit H un sous-groupe de G, alors on dit que H est un p-Sylow de G si $|H| = p^\alpha$
7. Exemple : T l'ensemble des matrices triangulaires supérieures de diagonale unitaire est un p-Sylow de $GL_n(\mathbb{F}_p)$
8. Lemme : Soit $H < G$ et S un p-Sylow de G alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H
9. Théorème de Sylow (premier) : G contient au moins un p-Sylow
10. Théorème de Sylow (second) : Soit H un p-sous-groupe de G alors H est contenu dans un p-Sylow de G, les p-Sylow sont conjugués et leur nombre n_p vérifie $n_p \mid n, n_p \equiv 1[p]$
11. Application : Si $|G| = 63$ alors G n'est pas simple

3 Groupes de matrices opérant sur des matrices

3.1 Action par équivalence

(Chapitres I.1 et I.2 de Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni)

On considère K un corps fini de cardinal q.

1. Définition : L'action de $GL_m(K) \times GL_n(K)$ sur $M_{m,n}(K)$ par équivalence est définie par $(P, Q).A = PAQ^{-1}$

2. Théorème : Soit $A \in M_{m,n}(K)$, alors $Orb(A) = \{B \in M_{m,n}(k), rg(A) = rg(B)\} = Orb(I_{m,n,r})$
3. Corollaire : Le théorème du rang se reformule en, pour $A, B \in M_{m,n}(K)$, A et B sont dans la même orbite si et seulement si $rg(A) = rg(B)$
4. Proposition : Soit $A \in M_{m,n}(K)$, alors $|Orb(A)| = \frac{|GL_m(K)||GL_n(K)|}{|Stab(A)|}$
5. Proposition : $Stab(A) = Stab(I_{m,n,r}) \simeq \begin{pmatrix} GL_r(K) & M_{r,m-r}(K) \\ 0 & GL_{m-r}(K) \end{pmatrix} \times \begin{pmatrix} GL_r(K) & 0 \\ M_{n-r,r}(K) & GL_{n-r}(K) \end{pmatrix}$
6. Corollaire : $|Orb(A)| = |Orb(I_{m,n,r})| = q^{a_{m,n,r}} \prod_{i=1}^{m-r}(q^{r+i}-1) \prod_{i=1}^{n-r}(q^{r+i}-1)$ avec $a_{m,n,r} = \frac{1}{2}((m-r)(m-r-1) + (n-r)(n-r-1))$

3.2 Action par conjugaison

(Annexe B d'Algèbre de Xavier Gourdon)

1. Définition : On dit que deux matrices $A, B \in M_n(K)$ sont semblables si A, B sont dans la même orbite
2. Exemple : Soit E un K-espace vectoriel de dimension n, $u \in End(E)$, e, f bases de E de matrice de passage P, alors $Mat_f(u) = PMat_e(u)P^{-1}$, autrement dit les matrices représentants u dans une base sont semblables
3. Proposition : Soit $A, B \in M_n(K)$ semblables, alors A, B ont même rang, trace, déterminant, valeurs propres, polynôme minimal, polynôme caractéristique
4. Remarque : Autrement dit ce sont des invariants partiels de similitudes
5. Exemple : J et 0 ont même polynôme caractéristique mais ne sont pas semblables
6. Théorème : Soit $A \in M_n(K)$, alors A diagonalisable (respectivement trigonalisable) si et seulement si π_A est scindé à racines simples (respectivement scindé)
7. Corollaire : Dans ce cas, un représentant simple de $Orb(A)$ est la matrice diagonale (respectivement triangulaire) correspondante
8. Définition : Soit $x \in E$, alors π_x est le polynôme unitaire tel que $(\pi_x) = \{P \in K[X], P(u)(x) = 0\}$ et $E_x = \{P(u)(x), P \in K[X]$
9. Proposition : Soit $x \in E$, alors E_x est sous-espace de E de dimension $deg(\pi_x)$ et de base $(x, ..., u^{deg(\pi_x)-1})$
10. Théorème : Il existe $x \in E$ tel que $\pi_x = \pi_u$
11. Définition : On dit que u est cyclique s'il existe $x \in E$ tel que $E_x = E$
12. Théorème : Si u cyclique alors il existe une base b de E tel que $Mat_b(u) = C(\pi_u)$ matrice compagnon associée à π_u
13. Théorème : Il existe $F_1, ..., F_r$ sous-espaces de E stables par u tels que $E = F_1 \oplus ... \oplus F_r$, $u_i := u_{|F_i}$ cyclique et $P_i := \pi_{u_i} \mid P_{i-1}$
14. Remarque : La suite des polynômes P_i ne dépend que de u et est appelée les invariants de similitude de u

15. Théorème de réduction de Frobenius : Il existe une base b de E telle que $Mat_b(u) = diag(C(P_1), ..., C(P_r))$
16. Corollaire : Deux endomorphismes sont semblables si et seulement s'ils ont les mêmes invariants de similitude
17. Application : Soit $A, B \in M_n(K)$ semblables sur une extension de corps de K alors A et B sont semblables sur K

4 Groupes finis opérant sur des espace vectoriels

4.1 Représentations linéaires et caractères

(Chapitre 6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On dit que (ρ, V) est une représentation linéaire de G si V est un $\mathbb{C}$-espace vectoriel et $\rho : G \longrightarrow GL(V)$ un morphisme de groupes, de plus $\chi = tr \circ \rho$ appelé caractère de ρ
2. Exemple : Soit $(e_g)_{g\in G}$ une base de $\mathbb{C}^n$, alors $\rho(g)(e_k) = e_{gk}$ définit une représentation de G appelé représentation régulière
3. Définition : Soit (ρ, V) une représentation de G, alors on dit que (ρ, V) est irréductible s'elle n'admet pas de sous-espaces non triviaux de V stables par l'action de G
4. Exemple : $\varepsilon : S_n \longrightarrow \{-1, 1\} \subset GL_1(\mathbb{C})$ est une représentation irréductible de dimension 1 de G, et $\chi_\varepsilon = \varepsilon$
5. Théorème de Maschke : Soit (ρ, V) une représentation de G, alors (ρ, V) se décompose en une somme directe de sous-représentations irréductibles, de même que tout caractère se décompose en somme de caractères irréductibles
6. Définition : Soit $\varphi : G \longrightarrow \mathbb{C}$, alors on dit que φ est centrale si $\varphi(gk) = \varphi(kg)$
7. Exemple : Un caractère est une fonction centrale
8. Théorème : Les caractères irréductibles forment une base orthonormée pour le produit scalaire hermitien $\langle \chi, \phi \rangle = \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{\phi(g)}$ sur l'espace des fonctions centrales
9. Corollaire : $|Conj(G)| = |Irr(G)|$
10. Corollaire : $|G| = \sum_{i=1}^{m} \chi_i(1)^2 = \sum_{i=1}^{m} dim(V_i)^2$ avec $(\chi_i)_{1\leq i\leq m}$ la base précédente
11. Proposition : χ est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$

4.2 Tables de caractères

(Chapitres VIII.1.1 et VIII.1.2 de L'algèbre discrète de la transformation de Fourier de Gabriel Peyré)

1. Définition : La table des caractères de G est le tableau des valeurs des caractères irréductibles sur les classes de conjugaison

2. Exemple : La table des caractères de $\mathbb{Z}/n\mathbb{Z}$ est une matrice de Vandermonde associée à $\omega_n = e^{\frac{2i\pi}{n}}$
3. Proposition : Les colonnes sont orthogonales pour le produit scalaire hermitien standard
4. Théorème : La table des caractères de S_4 est en annexe
5. Définition : Soit χ un caractère de G, alors $ker(\chi) = \{g \in G, \chi(g) = \chi(1)\}$
6. Proposition : Les sous-groupes distingués de G sont exactement les intersections de noyaux de caractères irréductibles de G
7. Application : Les sous-groupes distingués de S_4 sont $\{id\}, V_4, A_4$ et S_4

4.3 Cas des groupes abéliens finis

(Chapitres I.2 de L'algèbre discrète de la transformation de Fourier de Gabriel Peyré, 6.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi et I.2 de Eléménts d'analyse et d'algèbre de Pierre Colmez)

On considère G un groupe abélien.

1. Théorème : G est abélien si et seulement si tout ses caractères irréductibles sont de degré 1
2. Remarque : Les caractères de représentations irréductibles coïncident avec les caractères $\chi : G \longrightarrow \mathbb{C}^*$ morphismes de groupes, et on note $\hat{G}$ leur ensemble appelé groupe dual de G
3. Lemme : G et $\hat{\hat{G}}$ sont isomorphes
4. Lemme : Il existe $g \in G$ d'ordre $o(g) = N(G)$ avec $N(G) := PPCM(o(h), h \in G)$ l'exposant de G
5. Proposition : G et $\hat{G}$ ont le même exposant
6. Théorème de structure des groupes abéliens finis : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$ avec $d_{i+1} \mid d_i$