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

Adrien Fontaine

21 décembre 2013

Table des matières

Cadre : G un groupe (multiplicatif), e son neutre, H un sous-groupe de G et X un ensemble.

1 Définition et premières propriétés

1.1 Actions de groupe

Définition 1

Perrin p13

on dit que G opère sur X si on s'est donné une application

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g.x \end{array}$$

vérifiant les axiomes suivant :

(i) $\forall g, g' \in G, \forall x \in X, g.(g'.x) = (gg').x$

(ii) $\forall x \in X, e.x = x.$

Remarque 1

C'est équivalent à la donnée d'un homomorphisme $\varphi : G \to \mathfrak{S}(X)$*, où* $\mathfrak{S}(X)$ *désigne l'ensemble des bijections de* X*.*

Définition 2

Perrin p14

- *On dit que G opère transitivement sur X si on a :*

$$\forall x \in X, \forall y \in X, \exists g \in G / g.x = y$$

- *On dit que G opère fidèlement si $\varphi : G \to \mathfrak{S}(X)$ est injectif,* i.e *si on a*

$$(\forall x \in g.x = x) \to g = e$$

Remarque 2

$G/Ker(\varphi)$ *opère fidèlement sur* X*.*

Exemple 1

$PGL(E)$ *opère fidèlement sur* $P(E)$*, où E est une espace vectoriel.*

Définition 3

On introduit la relation d'équivalence suivante :

$$x \sim y \Leftrightarrow \exists g \in G / g.x = y$$

Les classes pour cette action sont les orbites de G sous X. On note $\omega(x)$, l'orbite de $x \in X$.

Remarque 3

G opère transitivement sur $\omega(x)$.

Exemple 2

Décomposition d'une permutation en produit de cycles à supports disjoints.

Définition 4

Si $x \in X$, on définit $G_x = \{g \in G, g.x = x\}$. C'est un sous-groupe de G appelé le stabilisateur de x.

Exemple 3

Dans l'opération naturelle de $\mathfrak{S}_n$ sur $\{1, ..., n\}$, le stabilisateur d'un point est isomorphe à $\mathfrak{S}_{n-1}$.

Définition 5

On dit que l'action de G sur X est n-fois transitive si Perrin p16

$$\forall (x_1, ..., x_n), (y_1, ..., y_n) \in X^n, \exists g \in G, \forall 1 \leq i \leq n, g.x_i = y_i$$

Lemme 1 Perrin p16

L'action de $\mathfrak{A}_n$ sur $\{1, ..., n\}$ est $n-2$-fois transitive.

Proposition 1

- *Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1, ..., a_p)$ et si $\tau \in \mathfrak{S}_n$, on a*

$$\tau \sigma \tau^{-1} = (\tau(a_1), ..., \tau(a_p))$$

- *Dans $\mathfrak{S}_n$, tous les cycles sont d'ordre p sont conjugués.*
- *Si $n \geq 5$, les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$.*

Application :

Théorème 1 Perrin p28

$\mathfrak{A}_n$ est simple pour $n \geq 5$.

1.2 Action d'un groupe fini sur un ensemble fini

But : Préciser le lien entre orbite et stabilisateur de $x \in X$.

Proposition 2

L'application $\bar{g} \mapsto g.x$ de G/G_x dans $\omega(x)$ est bien définie et est une bijection. Perrin p15

Corollaire 1

Si G est fini, on a $\forall x \in X, |G| = |\omega(x)|.|G_x|$. Gourdon p22

Proposition 3

On suppose G fini. Soient $\omega(x_1), ..., \omega(x_k)$ les orbites de l'action de G sur X. Pour tout $g \in G$, on note $Fix(g) = \{x \in X, g.x = x\}$ l'ensemble des éléments de E fixés par g. Alors : Combes p43

(i) $|X| = \sum_{i=1}^{k} |\omega(x_i)| = \sum_{i=1}^{k} \frac{|G|}{|G_x|}$.

(ii) *Le nombre d'orbites est* $k = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$.

Application :

(i) **Théorème 2 (*de Cauchy*)**

Soit G un groupe fini d'ordre n, et soit p un facteur premier de n. Il existe dans G des éléments d'ordre p. Combes p45

(ii) Développement : Perrin p82

Théorème 3 (*de Wedderburn*)

Tout corps fini est commutatif.

2 Applications en théorie des groupes

2.1 Action de G sur lui même par automorphisme intérieur

On fait agir $G \curvearrowright G$ via $g.a = gag^{-1}$.

Définition 6

(i) *Les orbites s'appellent alors classe de conjugaison et si $a' = gag^{-1}$, a' est un conjugué de a.*

(ii) *Le stabilisateur de a s'appelle centralisateur* Perrin p15

$$H_a = \{g \in G, gag^{-1} = a\} = \{g \in G, ga = ag\}$$

(iii) *On définit de même le centralisateur d'une partie A de G :*

$$C_G(A) = \{g \in G, \forall a \in A, ga = ag\}$$

Proposition 4

Le centre d'un p-groupe distinct de $\{e\}$ n'est pas réduit à $\{e\}$. Gourdon p27

Théorème 4

Si G est un groupe d'ordre p^2 avec p premier, alors G est abélien. Gourdon p27

Théorème 5

Si G est un groupe d'ordre p^α, alors pour tout $0 \leq m \leq \alpha$, il existe un sous Gourdon p27 *groupe de G d'ordre p^m.*

2.2 Action de G par translation à gauche

On peut faire opérer $G \curvearrowright G$ par translation à gauche :

$$\forall a, g \in G, g.a = ga$$

Proposition 5

Cette action est fidèle. Perrin p15

Application :

Théorème 6 (*de Cayley*)

Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

On peut aussi faire opérer $G \curvearrowright G/H$ par translation à gauche :

$$\forall g \in G, \forall aH \in G/H, g.(aH) = (ga)H$$

Cette opération est transitive mais non fidèle en général. En effet, si $\varphi : G \to \mathfrak{S}(G/H)$ est le morphisme associé, on a

$$Ker(\varphi) = \bigcap_{a \in G} aHa^{-1}$$

Proposition 6

Soit G un groupe infini et H un sous-groupe de G, distinct de G et d'indice fini. Alors, G n'est pas simple. Perrin p17

Théorème 7 (*de Frobenius*)

Soit G un groupe fini, H un sous-groupe de G. On suppose que p est le plus petit diviseur premier de $|G|$ et que $|H|.p = |G|$. Alors, H est un sous-groupe distingué de G. Oraux X-ENS 1 p48

2.3 Théorèmes de Sylow

Définition 7

Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous-groupe de Sylow de G, un sous-groupe de cardinal p^α.

On fait agir G sur ses p-Sylow. On obtient :

Théorème 8 (*de Sylow*)

Soit G un groupe fini d'ordre $n = p^\alpha m$ avec $p \nmid m$. Alors, G contient au moins un p-sous groupe de Sylow. De plus, tous les p-Sylow sont conjugués Perrin p18-19 *et leur nombre n_p vérifie, $n_p \equiv 1[p]$. Enfin, tout sous-groupe de G qui est un p-groupe, est contenu dans un p-Sylow.*

Corollaire 2

Un p-Sylow est unique, si et seulement si, il est distingué.

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

3 Applications en algèbre linéaire et en algèbre commutative

3.1 En algèbre linéaire

Soit K un corps commutatif.

(i) Le groupe $G = GL_n(K) \times GL_n(K)$ opère sur $E = M_n(K)$ via :

$$(P, Q).M = PMQ^{-1}$$

Deux matrices qui sont dans la même orbite pour cette action de groupe sont dîtes équivalentes.

Proposition 7

Alessandri p20

Pour $A, B \in E = M_n(K)$, on a :

(i) $A \sim B \Leftrightarrow rang(A) = rang(B)$

(ii) Pour $0 \leq r \leq n$, lorsque $rang(A) = r$, on a $A \sim \mathcal{R}_r$ où $\mathcal{R}_r = 0$ si $r = 0$ et

$$\mathcal{R}_r = Diag(\underbrace{1, ..., 1}_{r}, 0, ..., 0) \text{ si } r \geq 1$$

Interprétation :
Le rang est un invariant total pour la classification des matrices à équivalence près. De plus, il y a $(n+1)$-orbites et les matrices $\mathcal{R}_r$ constituent un système complet de représentants de classes d'équivalence.

(ii) On peut également faire agir $G = GL_n(K)$ sur $E = M_n(K)$ via :

$$P.M = PMP^{-1}$$

Grifone p198

Deux matrices qui sont dans la même orbite pour cette action de groupes sont dîtes semblables.

Proposition 8

Deux matrices $A, B \in M_n(K)$, dont les polynômes caractéristiques sont scindés, sont semblables, si et seulement si, elles ont la même réduite de Jordan (à l'ordre des blocs près).

3.2 Représentations linéaires des groupes finis

Définition 8

Une représentation linéaire d'un groupe G est la donnée d'un espace vectoriel E sur un corps K, et d'un morphisme de groupe $\rho : G \to GL(E)$. Autrement dit, le groupe G opère par automorphismes linéaires sur E. Si $dim(E) = n < +\infty$, la représentation est dite finie, de degré n.

Alessandri p31

Définition 9

Le caractère d'une représentation linéaire (ρ, E) est l'application

$$\begin{array}{cccc} \chi_\rho & : & G & \to & K \\ & & g & \mapsto & Tr(\rho(g)) \end{array}$$

Définition 10

On dit que deux représentations (ρ_1, E_1) et (ρ_2, E_2) d'un même groupe G sont isomorphes si il existe un isomorphisme $\sigma : E_1 \to E_2$ tel que

$$\forall g \in G, \forall x \in E_1, \sigma(g.x) = g.\sigma(x)$$

Proposition 9

Si (ρ_1, E_1) et (ρ_2, E_2) sont isomorphes, alors $\chi_{\rho_1} = \chi_{\rho_2}$.

Autrement dit, le caractère est un invariant.
Développement :

Théorème 9 (*de Molien*)

Soit G un sous-groupe fini de $GL_n(\mathbb{C})$. Il agit linéairement sur le sous-espace $V_d \subset \mathbb{C}[X_1, ..., X_n]$ des polynômes homogènes de degré d via :

Leichtnam, Algèbre 1 p117

$$\forall A \in G, \forall P \in V_d, A.P(X_1, ..., X_n) = P({}^t(A^{-1t}(X_1, ..., X_n)))$$

qui est une notation pratique pour dire que l'on substitue $\sum_{j=1}^{n} \alpha_{j,i}$ à X_i, si l'on note $A^{-1} = (\alpha_{i,j})$. On note que V_d n'est qu'un sous-espace vectoriel de $\mathbb{C}[X_1, ..., X_n]$ stable par la même action plus générale sur $\mathbb{C}[X_1, ..., X_n]$ tout entier (une substitution linéaire des variables dans un polynômes homogènes reste homogène de degré d).Le théorème de Molien est l'égalité des séries formelles :

$$\frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - tA)} = \sum_{d \geq 0} dim(V_d^G) t^d$$

avec rayon de convergence au moins 1.

3.3 Action de $\mathfrak{S}_n$ sur $\mathbb{C}[X_1, ..., X_n]$

$\mathfrak{S}_n \curvearrowright \mathbb{C}[X_1, ..., X_n]$ via $\sigma.P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$.
On s'intéresse à l'algèbre $\mathbb{C}[X_1, ..., X_n]^{\mathfrak{S}_n}$ des polynômes invariants par l'action $\mathfrak{S}_n \curvearrowright \mathbb{C}[X_1, ..., X_n]$, qu'on appelle ensemble des polynômes symétriques.

Théorème 10 (*de structure des polynômes symétriques*)

On a :

$$\mathbb{C}[X_1, ..., X_n]^{\mathfrak{S}_n} = \mathbb{C}[\Sigma_1, ..., \Sigma_n]$$

où

$$\Sigma_p = \sum_{1 \leq i_1 < ... < i_p \leq n} X_{i_1} ... X_{i_p}$$

sont les polynômes symétriques élémentaires.

Ramis-Deschamps-Odoux p200-203

On peut également parler de l'action de l'action de $\mathfrak{S}_n$ sur $GL_n(K)$ avec notamment le théorème de Brauer (Objectif Agrégation p322).

4 Applications en géométrie

4.1 Angles orientés et espaces affines

Définition 11

On appelle espace affine, un ensemble $\mathcal{E}$ sur lequel le groupe additif $(E, +)$ d'un espace vectoriel agit (à droite), transitivement et librement.

Combes, p105

Définition 12

Soit E_2 un $\mathbb{R}$-plan vectoriel euclidien de sphère unité S. Le groupe $SO(E_2)$ des rotations opère de façon naturelle sur $S \times S$: $(r.(x, y) = (r(x), r(y)))$. L'orbite de (x, y) est notée $(\widehat{(x, y)})$, c'est l'angle orienté des vecteurs x et y pris dans cet ordre.

Alessandri, p30

4.2 Action de $PSL_2(\mathbb{Z})$ sur le demi plan de Poincaré

À faire si on veut le proposer en développement, ou bien si on maîtrise suffisamment. Sinon, trouver autre chose... Référence : Allessandri p81

Références

[1] Daniel Perrin, *Cours d'algèbre*. Ellipses, 1996.

[2] François Combes, *Algèbre et géométrie*. Bréal, 2003.

[3] Xavier Gourdon, *Algèbre*, 2 ème ésition. Ellipses, 2009.

[4] Serge Francinou, Hervé Gianella, Serge Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*. Cassini, 2007.

[5] Michel Alessandri, *Thèmes de géometrie. Groupes en situation géométrique*. Dunod, 1999.

[6] Eric Leichtnam, *Exercices corrigés de Mathématiques, posés à l'oral des concours de Polytechnique et des ENS, Algèbre 1*. Ellipses, 2000.

[7] E.Ramis, C.Deschamps, J.Odoux, *Cours de Mathématiques spéciales. Tome 1 Algèbre.*. Masson, 1977.

.