Leçon 105: Groupe des permutations d'un ensemble fini. Applications.

Adrien Fontaine

24 avril 2013

Table des matières

1 Généralités sur le groupe symétrique

1.1 Définitions et premières propriétés

Définition 1

Soit E un ensemble fini. Une bijection de E dans E est appelée une permutation de E. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E.

Tauvel p38

Proposition 1

$\mathfrak{S}(E)$ muni de la loi de composition des applications est un groupe.

Notation : Pour $E = \{1, ..., n\}$, on note $\mathfrak{S}_n$ au lieu de $\mathfrak{S}(E)$.

Proposition 2

Si $Card(E) = n$, alors $\mathfrak{S}(E) \cong \mathfrak{S}_n$. De plus, $Card(\mathfrak{S}_n) = n!$.

Pour cette raison, on s'intéresse désormais uniquement à $\mathfrak{S}_n$. De plus, cela permet d'utiliser l'ordre naturel sur $\{1, ..., n\}$ et la notation

$$\begin{bmatrix} 1 & ... & n \\ \sigma(1) & ... & \sigma(n) \end{bmatrix}$$

pour signifier que la permutation que la permutation $\sigma \in \mathfrak{S}_n$ prend les valeurs $\sigma(1)$ en 1, ..., $\sigma(n)$ en n.
Par ailleurs, le théorème suivant justifie une partie de l'intérêt que l'on porte au groupe symétrique :

Théorème 1 (*de Cayley*)

Tout groupe G de cardinal n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Perrin et le livre de Rached Mneimné, Element de géométrie pour un résumé très synthétique de la preuve des théorèmes de Sylow

Application : On peut déduire du théorème de Cayley une preuve des théorèmes de Sylow.

On montre d'abord le théorème de Sylow pour $GL_n(\mathbb{F}_p)$, puis on injecte G dans $\mathfrak{S}_n$ et $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ via les matrices de permutation. Enfin, on montre que si on connait un Sylow d'un groupe G, on peut en trouver un pour un sous-groupe H.

1.2 Orbites et cycles

Définition 2

Pour $j \in \{1, ..., n\}$ et $s \in \mathfrak{S}_n$, on note $\mathcal{O}_s(j) = \{s^k(j), k \in \mathbb{Z}\}$. On dit que $\mathcal{O}_s(j)$ est la s-orbite de j. Une s-orbite est une partie de $\{1, ..., n\}$ de la forme $\mathcal{O}_s(j)$ pour au moins un $j \in \{1, ..., n\}$.

Définition 3

$[i \sim j \Leftrightarrow j \in \mathcal{O}_s(i) \Leftrightarrow \exists k \in \mathbb{Z} / j = s^k(i)]$ est une relation d'équivalence sur $\{1, ..., n\}$.

Définition 4

On dit que $s \in \mathfrak{S}_n$ est un cycle s'il existe une s-orbite $\mathcal{O}$ telle que $Card(\mathcal{O}) > 1$ et que cette orbite est unique. Alors, $Card(\mathcal{O})$ est appelé la longueur du cycle et $\mathcal{O}$ son support. Un q-cycle est un cycle de longueur q et un 2-cycle est une transposition.

Exemple 1

$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 3 & 2 & 6 \end{bmatrix}$ *est un cycle de longueur 4, de support* $\{2,3,4,5\}$. *On le note* $\begin{bmatrix} 2 & 4 & 3 & 5 \end{bmatrix}$.

Proposition 3

Un p-cycle est un cycle d'ordre p. De plus, tous les p-cycles sont conjugués dans $\mathfrak{S}_n$. En effet, si $\tau = (a_1, ..., a_p)$ et $\sigma \in \mathfrak{S}_n$, alors $\sigma\tau\sigma^{-1} = (\sigma(a_1), ..., \sigma(a_p)$ et l'action de $\sigma(n)$ sur $\{1, ..., n\}$ est n-transitive.

Tauvel p39

On a même le résultat suivant :

Théorème 2

Deux cycles de $\mathfrak{S}_n$ sont conjugués dans $\mathfrak{S}_n$ si et seulement si, ils ont même longueur.

Arnaudiès-Fraysse p181

Théorème 3

(i) Deux cycles à supports disjoints commutent.

(ii) Tout $\sigma \in \mathfrak{S}_n \setminus \{Id\}$ est produit de cycles de supports deux à deux disjoints, et un tel produit est unique à l'ordre près des facteurs.

Tauvel p39

N.B : Ce produit en cycles de supports deux à deux disjoints est appelé décomposition canonique de la permutation σ.

Corollaire 1

Pour $\sigma \in \mathfrak{S} \setminus \{Id\}$, l'ordre de σ est égal au ppcm des longueurs des cycles intervenant dans la décomposition canonique.

Arnaudiès-Fraysse p180

Exemple 2

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & 4 & 5 \end{bmatrix}$$

et ce cycle est d'ordre 6.

Corollaire 2

Toute permutation de $\{1, ..., n\}$ est produit de transpositions.

Tauvel

Corollaire 3

Pour toute permutation $\sigma \in \mathfrak{S}_n$, notons $\nu_1(\sigma)$ le nombre de points fixes

Arnaudiès-Fraysse

de σ, $\nu_k(\sigma)$ le nombre de k-cycles dans la décomposition de σ en cycles à supports disjoints pour $2 \leq k \leq n$. Alors, pour que deux permutations σ et σ' de $\mathfrak{S}_n$ soient conjuguées dans $\mathfrak{S}_n$, il faut et il suffit que

$$\forall 1 \leq k \leq n, \nu_k(\sigma) = \nu_k(\sigma')$$

1.3 Groupe alterné

Définition 5

Soit $\sigma \in \mathfrak{S}_n$ et $m(\sigma)$ le nombre de σ-orbites. La signature de σ est l'élément $\varepsilon(\sigma) \in \{-1, 1\}$ défini par :

$$\varepsilon(\sigma) = (-1)^{n-m(\sigma)}$$

Exemple 3

$\varepsilon(Id) = 1$, $\varepsilon(\sigma) = (-1)^{q-1}$ pour un q-cycle, $\varepsilon(\tau) = -1$ pour une transposition.

Théorème 4

Soient $s \in \mathfrak{S}_n$ et τ une transposition. Alors, $\varepsilon(s\tau) = -\varepsilon(s)$. Tauvel

Corollaire 4

(i) Si $\sigma \in \mathfrak{S}_n$ est un produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.

(ii) L'application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un morphisme de groupes surjectif. Tauvel

(iii) Si $n \geq 2$ et $\sigma \in \mathfrak{S}_n$, on a

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Définition 6

Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est appelé le groupe alterné de $\{1, ..., n\}$, et noté $\mathfrak{A}_n$. Un élément de $\mathfrak{A}_n$ est appelé une permutation paire. Tauvel

Proposition 4

$\mathfrak{S}_n/\mathfrak{A}_n \cong \{-1, 1\}$ et donc $Card(\mathfrak{A}_n) = \frac{n!}{2}$. Tauvel

2 Structure des groupes symétriques et alternés

2.1 Étude de cas particuliers

Exemple : Pour $n = 2$

$$\mathfrak{S}_2 = \{id, (1,2)\} \text{ et } \mathfrak{A}_2 = \{id\}$$

- $\mathfrak{S}_2$ est abélien.

Exemple : Pour $n = 3$

$$\mathfrak{S}_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$
$$\mathfrak{A}_3 = \{id, (1,2,3), (1,3,2)\} = \{id, \sigma, \sigma^2\} \text{ où } \sigma = (1,2,3)$$

Perrin p12

- $\mathfrak{S}_3$ contient un sous-groupe distingué d'ordre 3 : $\mathfrak{A}_3$.
- $\mathfrak{A}_3$ est simple.
- Le sous groupe engendré par $(1,2)$ n'est pas distingué : $\sigma(1,2)\sigma^{-1} = (2,3)$.

Exemple : Pour $n = 4$

- Les sous-groupes distingués de σ_4 sont $\{id\}$,K (le groupe de Klein), $\mathfrak{A}_4$ et $\mathfrak{S}_4$. Arnaudiès-Fraysse p196
- K est un sous-groupe distingué non trivial de $\mathfrak{A}_4$. En particulier, $\mathfrak{A}_4$ n'est pas simple.

2.2 Générateurs

Rappel : On a déjà vu que les cycles, ainsi que les transpositions, engendrent $\mathfrak{A}_n$. On s'intéresse donc aux générateurs non triviaux de $\mathfrak{S}_n$ et de $\mathfrak{A}_n$.

Proposition 5

Si $n \geq 2$, le groupe $\mathfrak{S}_n$ est engendré par l'un quelconque des ensembles suivants :

(i) les transpositions $(1,i)$ avec $2 \leq i \leq n$.

(ii) les transpositions $(i, i+1)$ avec $1 \leq i \leq n-1$. Tauvel

(iii) la transposition $(1,2)$ et le n-cycle $\sigma = (1, ..., n)$.

Proposition 6

Si $n \geq 3$, le groupe $\mathfrak{A}_n$ est engendré par l'un quelconque des éléments suivants :

(i) les permutations $(1,)(1,j)$ avec $2 \leq i, j \leq n$, ainsi que les produits pairs de transposition. Tauvel ou Perrin p11

(ii) les 3-cycles.

(iii) les éléments σ^2, $\sigma \in \mathfrak{S}_n$.

2.3 Centre

Proposition 7

$Z(\mathfrak{S}_n) = \{id\}$ pour $n \geq 3$. En particulier, $\mathfrak{S}_n$ n'est pas abélien pour $n \geq 3$. Tauvel

2.4 Simplicité

Développement :

Théorème 5

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

Corollaire 5 Perrin p28

On a $D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$.

2.5 Automorphismes intérieurs

Théorème 6

Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur : Perrin p30

$$Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$$

3 Applications

3.1 Le déterminant

Définition 7

Soit K un corps, E un K-espace vectoriel et $f : E^p \to K$. Gourdon p134

- *On dit que f est une forme o-linéaire si f est linéaire par rapport à chacune de ses variables. On note $\mathcal{L}_p(E, K)$ l'ensemble des formes p-linéaires.*
- *f est dite alternée si $f(x_1, ..., x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.*
- *f est dite antisymétrique si l'échange de deux vecteurs dans la suite $(x_1, ..., x_p)$ donne à f des valeurs opposées.*

Remarque 1

f est antisymétrique, si et seulement si, $\forall \sigma \in \mathfrak{S}_n, f(x_{\sigma(1)}, ..., x_{\sigma(p)}) = \varepsilon(\sigma) f(x_1, ..., x_p)$.

Théorème 7

Si K est un corps commutatif de caractéristique différente de 2, alors $f \in \mathcal{L}_p(E, K)$ est antisymétrique, si et seulement si, f est alternée. Gourdon p135

Théorème 8

L'ensemble des formes n-linéaires alternées sur un K-espace vectoriel E de dimension n, est un K-espace vectoriel de dimension 1. De plus, il existe une et une seule forme n-linéaire alternée prenant la valeur 1 sur une base donnée de E. Gourdon p135

Définition 8

Soit $B = (e_1, ..., e_n)$ une base de E. La forme n-linéaire alternée valant 1 sur B est appelée déterminant dans la base B et Gourdon p135

$$det_B(x_1, ..., x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} ... x_{n,\sigma(n)}$$

où, pour $1 \leq i \leq n$, les $x_{i,j}$ sont les coordonnées de x_i dans la base B.

3.2 Les polynômes symétriques

Soit A un anneau intègre. Alors, $\mathfrak{S}_n \curvearrowright A[X_1, ..., X_n]$ via

$$\sigma.P(X_1, ..., X_n) = P(X_{\sigma(1)}, ..., X_{\sigma(n)})$$

Définition 9

Un polynôme P est dit symétrique s'il est invariant par l'action de $\mathfrak{S}_n$ sur $A[X_1, ..., X_n]$, i.e *si $\forall \sigma \in \mathfrak{S}_n, \sigma.P = P$. On note $A[X_1, ...X_n]^{\mathfrak{S}_n}$ l'ensemble des polynômes symétriques.*

Développement : Ramis-Deschamps-Odoux p203

Théorème 9 (*de structure des polynômes symétriques*)

Pour tout $P \in A[X_1, ..., X_n]^{\mathfrak{S}_n}$ de degré p, il existe un unique $Q \in A[Y_1, ..., Y_n]$ de poids inférieur ou égal à p, tel que

$$P(x_1, ..., X_n) = Q(\Sigma_1, ..., \Sigma_n)$$

3.3 Groupes d'isométries particuliers

Proposition 8

Une isométrie de $\mathcal{E}$ conserve le polytope $\mathcal{P}$ si et seulement si, elle induit une permutation des sommets de ce polytope. L'application Φ de $Is_{\mathcal{P}}(\mathcal{E})$ dans Szpirglas p421

$\mathfrak{S}(S)$, *l'ensemble des permutations de l'ensemble* S *des sommets de*$\mathcal{P}$, *qui à une isométrie conservant* $\mathcal{P}$ *associe sa restriction à l'ensemble des sommets est un morphisme injectif de groupes.*

Exemple 4

- *Si* T *est un tétraèdre régulier,* $Is(T) \cong \mathfrak{S}_4$.
- *Le groupe des déplacements conservant le cube est isomorphe à* $\mathfrak{S}_4$.

Références

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

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

[3] Patrice Tauvel, *Cours d'algèbre*. Dunod, 2001.

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

[5] Aviva Szpirglas, *Mathématiques L3 Algèbre*. Éditions Pearson.

[6] J.M.Arnaudiès, H.Fraysse, *Cours de Mathématiques 1, Algèbre*. Dunod, 1993.