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

Introduction : Le groupe symétrique est un groupe ayant un caractère d'universalité parmi les groupes finis. Il apparaît aussi en algèbre linéaire et en théorie de Galois. Sa bonne connaissance est donc fondamentale.

Soit $n \in \mathbb{N}^*$.

1 Groupe symétrique

1.1 Définitions et premières propriétés

Définition 1. Si X est un ensemble fini, on note $\mathcal{S}_X$ l'ensemble des bijections de X sur X. Ses éléments sont appelés *permutations* de X.

Proposition 2. $(\mathcal{S}_X, \circ)$ est un groupe d'ordre $|X|!$.

***Exemple* 3.** *Si X est un ensemble fini et G un groupe qui agit sur X, l'action induit un morphisme Φ de G dans $\mathcal{S}_X$, défini par $\forall g \in G, \forall x \in X, \Phi(g)(x) = g \cdot x$.*

Si $X = [\![1, n]\!]$, on note $\mathcal{S}_X = \mathcal{S}_n$.

***Exemple* 4.** *$\mathcal{S}_3$ est le seul groupe non abélien d'ordre 6 à isomorphisme près.*

Une permutation $\sigma \in \mathcal{S}_n$ est notée $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Théorème 5 (Cayley)**.** Tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Définition 6. On appelle *k-cycle* $(2 \leq k \leq n)$ une permutation c pour laquelle il existe $i_1, \cdots, i_k \in [\![1, n]\!]$ tels que $c(i_1) = i_2, \cdots, c(i_{k-1}) = i_k, c(i_k) = i_1$. Un tel cycle est noté $(i_1, i_2, \cdots, i_k)$, les autres éléments de $[\![1, n]\!]$ étant fixés. Le *support* d'un cycle c est l'ensemble $\{i \in [\![1, n]\!], c(i) \neq i\}$. Un 2-cycle est appelé *transposition*.

Proposition 7. Un k-cycle est d'ordre k.

Proposition 8. Deux cycles commutent si et seulement si l'un est une puissance de l'autre ou leurs supports sont disjoints.

Proposition 9. Soit $c = (i_1, \cdots, i_k)$ un cycle, soit $\sigma \in \mathcal{S}_n$.
On a $\sigma c \sigma^{-1} = (\sigma(i_1), \cdots, \sigma(i_k))$.

***Application* 10.** *Si $n \geq 3$, alors $Z(\mathcal{S}_n) = \{\mathrm{Id}\}$.*

1.2 Décompositions et parties génératrices

Théorème 11. Toute permutation se décompose de façon unique en produit de cycles à supports disjoints.

***Application* 12.** *L'ordre d'une permutation est le PPCM des longueurs des cycles de sa décomposition.*

***Exemple* 13.** *La permutation* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$ *se décompose en* $(1,4)(2,3,5)$.
Elle est d'ordre 6.

Proposition 14. Deux permutations sont conjuguées si et seulement si leurs décompositions en cycles à supports disjoints sont de la même forme.

***Application* 15.** *Le nombre de classes de conjugaison de $\mathcal{S}_n$ est égal au nombre de partitions de n.*

Théorème 16. Toute permutation de $\mathcal{S}_n$ peut s'écrire comme produit d'au plus $n-1$ transpositions.

***Exemple* 17.** *Les transpositions de la forme $(1, i)$ engendrent $\mathcal{S}_n$, tout comme les transpositions de la forme $(i, i+1)$.*

2 Groupe alterné

2.1 Le morphisme signature

Définition 18. Soit $\sigma \in \mathcal{S}_n$, on note r le nombre de cycles dans la décomposition de σ. On définit la signature de σ par $\varepsilon(\sigma) = (-1)^{n+r}$.

Proposition 19. Si c est un k-cycle, sa signature est $\varepsilon(c) = (-1)^{k+1}$.

Proposition 20. ε est l'unique morphisme de groupes non trivial de $(\mathcal{S}_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Proposition 21. Pour tout $\sigma \in \mathcal{S}_n, \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$.

***Application* 22.** *Si K corps et $A \in \mathcal{M}_n(K)$, son déterminant est défini par* $\det(A) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} A_{\sigma(j), j}$.

Définition 23. Soient $a \in \mathbb{F}_p \backslash \{0\}, p$ premier.
On définit le symbole de Legendre $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ carré dans } \mathbb{F}_p \\ -1 & \text{sinon} \end{cases}$

Théorème 24 (Frobenius-Zolotarev)**.** Soit $p \geq 3$ premier, soit $u \in GL_n(\mathbb{F}_p)$. Sa signature est donnée par $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

2.2 Définition et propriétés du groupe alterné

Définition 25. On appelle *groupe alterné* le sous-groupe $\mathcal{A}_n = \ker(\varepsilon)$ de $\mathcal{S}_n$.

***Exemple* 26.** $\mathcal{A}_3 = \{Id, (1,2,3), (1,3,2)\}$.

Proposition 27. $|\mathcal{A}_n| = \frac{n!}{2}$. Ainsi $\mathcal{A}_n$ est d'indice 2, donc distingué dans $\mathcal{S}_n$.

Proposition 28. $\mathcal{A}_n$ est engendré par les 3-cycles.

Théorème 29. $\mathcal{A}_n$ est simple pour tout $n \geq 5$.

Corollaire 30. Pour tout $n \geq 5, D(\mathcal{A}_n) = \mathcal{A}_n$, et pour tout $n \geq 2, D(\mathcal{S}_n) = \mathcal{A}_n$.

Corollaire 31. Pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}_n$ sont $\{Id\}, \mathcal{A}_n$ et $\mathcal{S}_n$.

3 Applications

3.1 Matrices de permutations

Soit K un corps.

Définition 32. Soit $\sigma \in \mathcal{S}_n$. On définit sa matrice de permutation $P_\sigma = (p_{i,j})_{1 \leq i,j \leq n}$ par $\forall i, j, p_{i,j} = \delta_{i,\sigma(j)}$.

Proposition 33. $\mathcal{S}_n$ agit sur $\mathcal{M}_n(K)$ à gauche par $\sigma \cdot M = P_\sigma M$ et à droite par $M \cdot \sigma = MP_\sigma$. L'action à gauche (resp. à droite) permute les lignes (resp. les colonnes) de M selon σ^{-1} (resp. σ).

Proposition 34. On a alors $\det(P_\sigma) = \varepsilon(\sigma)$ et $P_\sigma^{-1} = P_{\sigma^{-1}}$.

Théorème 35 (Décomposition de Bruhat)**.** Soit $\mathcal{G} = GL_n(K)$, soit $\mathcal{T}_s$ l'ensemble des matrices triangulaires supérieures inversibles à coefficients dans K.
Alors $\mathcal{G} = \bigsqcup_{\sigma \in \mathcal{S}_n} \mathcal{T}_s P_\sigma \mathcal{T}_s$.

***Application* 36.** *Soit E un K-espace vectoriel de dimension n, on note $\mathcal{D}$ l'ensemble de ses drapeaux. Alors $\mathcal{D}$ est en bijection avec $\mathcal{G}/\mathcal{T}_s$. De plus, $\mathcal{G}$ agit sur $\mathcal{G}/\mathcal{T}_s \times \mathcal{G}/\mathcal{T}_s$, et l'ensemble des orbites s'identifie à $\mathcal{S}_n$.*

3.2 Polyèdres

On se place dans un espace affine euclidien $\mathcal{E}$ de dimension 3.

Proposition 37. Soit P un polytope épais de $\mathcal{E}$. Si P est stable par une isométrie f, alors l'ensemble de ses sommets l'est aussi et f induit une permutation sur ses sommets.

Applications.

Isométries du tétraèdre
On considère un tétraèdre régulier.

Proposition 38. Le groupe des isométries qui préservent le tétraèdre est isomorphe à $\mathcal{S}_4$.

Isométries du cube

Proposition 39. $\mathcal{S}_4$ agit sur les grandes diagonales du cube.

Corollaire 40. Le groupe des déplacements qui préservent le cube est isomorphe à $\mathcal{S}_4$.

***Application* 41.** *Table de caractères de $\mathcal{S}_4$ (voir annexe).*

Corollaire 42. Le groupe des isométries du cube est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

3.3 Polynômes symétriques

Soit A anneau commutatif unitaire. $\mathcal{S}_n$ agit sur $A[X_1, \cdots, X_n]$ par
$\sigma \cdot P(X_1, \cdots, X_n) = P(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$.

Définition 43. $P \in A[X_1, \cdots, X_n]$ est dit symétrique si pour tout $\sigma \in \mathcal{S}_n$, on a $\sigma \cdot P = P$.

***Exemple* 44.** *Dans $A[X_1, X_2]$, les polynômes $P = X_1 + X_2, Q = X_1X_2, R = X_1^2X_2 + X_1X_2^2$ sont symétriques.*

Définition 45. Soit $k \leq n$. On définit Σ_k, le polynôme symétrique élémentaire de degré k de $A[X_1, \cdots, X_n]$, par $\Sigma_k = \sum_{\substack{H \subseteq [\![1,n]\!] \\ |H|=k}} \left(\prod_{i \in H} X_i\right)$.

***Exemple* 46.** *Dans $A[X_1, X_2, X_3]$, on a $\Sigma_1 = X_1 + X_2 + X_3, \Sigma_2 = X_1X_2 + X_2X_3 + X_1X_3$, $\Sigma_3 = X_1X_2X_3$.*

Théorème 47. Soit $P \in A[X_1, \cdots, X_n]$ polynôme symétrique.
Alors il existe $T \in A[X_1, \cdots, X_n]$ tel que $P = T(\Sigma_1, \cdots, \Sigma_n)$.

Annexe

Table de caractères de $\mathcal{S}_4$:

	Id	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ'_s	3	-1	0	1	-1
χ_t	2	0	-1	0	2

Développements

— Théorème de Frobenius-Zolotarev.
— Décomposition de Bruhat et application aux drapeaux.
— Table de caractères de $\mathcal{S}_4$.

Références

[Del] J. Delcourt, Théorie des groupes, Dunod.

[Esc] J. Escofier, Théorie de Galois, Dunod.

[FGN] S. Francinou, H. Gianella, S. Nicolas, Oraux X-ENS - Algèbre 1, Cassini.

[Per] D. Perrin, Cours d'algèbre, Ellipses.

[Rau] G. Rauch, Les groupes finis et leurs représentations, Ellipses.