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

I. Le groupe symétrique

1. Définitions et propriétés élémentaires

Définition 1 (Groupe symétrique)**.** [Ber20, p.199] Soit E un ensemble fini non vide. L'ensemble des bijections de E sur lui-même est un groupe pour la composition, est appelé **groupe des permutations** de E ou **groupe symétrique** de E et est noté $\mathfrak{S}(E)$.

Théorème 2. Soit E de cardinal $n \geqslant 1$. Alors $|\mathfrak{S}(E)| = n!$.

Proposition 3. [Ber20] Soient E et E' deux ensembles non vides. Si E et E' sont en bijection, alors $\mathfrak{S}(E) \simeq \mathfrak{S}(E')$.

Corollaire 4. Soit E un ensemble fini de cardinal n. Alors $\mathfrak{S}(E) \simeq \mathfrak{S}(\llbracket 1, n \rrbracket)$. On note $\mathfrak{S}_n$ le groupe $\mathfrak{S}(\llbracket 1, n \rrbracket)$.

Notation 5. Si $\sigma \in \mathfrak{S}_n$, on la note $\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$.

Exemple 6. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ est la permutation $\sigma \in \mathfrak{S}_4$ définie par $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 1$ et $\sigma(4) = 4$.

Remarque 7. On étudiera par la suite uniquement le groupe $\mathfrak{S}_n$ pour $n \geqslant 2$.

Définition 8 (Support d'une permutation)**.** [Ber20, p.200] Soient $n \in \mathbb{N}$ et $\sigma \in \mathfrak{S}_n$. On appelle **support** de σ l'ensemble

$$\mathrm{Supp}(\sigma) = \{k \in \llbracket 1, n \rrbracket,\ \sigma(k) \neq k\}.$$

Propriété 9. [Ber20, p.201] Deux permutations à supports disjoints commutent.

Définition 10 (Cycle)**.** [Ulm21, p.57] Soient $n \in \mathbb{N}^*$, $\ell \in \llbracket 1, n \rrbracket$ et $i_1, \ldots, i_\ell$ des éléments distincts de $\llbracket 1, n \rrbracket$. La permutation γ définie par

$$\gamma(j) \begin{cases} j \text{ si } j \notin \{i_1, \ldots, i_\ell\} \\ i_{k+1} \text{ si } j = i_k \text{ avec } k < \ell \\ i_1 \text{ si } j = i_\ell \end{cases}$$

et notée $(i_1, i_2, \ldots, i_\ell)$ est appelée **cycle** de longueur ℓ ou un ℓ-cycle.

Définition 11 (Transposition)**.** Un cycle de longueur deux est appelé une **transposition**.

2. Structure de $\mathfrak{S}_n$

Orbites d'une permutation

Définition 12 (σ-orbite)**.** [Rom21, p.41] Soit $\sigma \in \mathfrak{S}_n$. On a une action naturelle de $\langle \sigma \rangle$ sur $\llbracket 1, n \rrbracket$ définie par $(\sigma^k, x) \longmapsto \sigma^k \cdot x = \sigma^k(x)$. Les orbites de cette action, appelées σ-orbites, sont les ensembles, $\langle \sigma \rangle \cdot x = \{\sigma^k(x),\ k \in \mathbb{Z}\}$ où x décrit $\llbracket 1, n \rrbracket$.

On définit la relation d'équivalence $x \mathcal{R}_\sigma y \iff (\exists k \in \mathbb{Z},\ y = \sigma^k(x))$.

Proposition 13. Soient $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{Id}\}$, $x \in \llbracket 1, n \rrbracket$ et O_x une σ-orbite de longueur $r \geqslant 2$. Alors r est le plus petit entier tel que $\sigma^r(x) = x$ et $O_x = \{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}$.

Théorème 14. [Rom21, p.42] Une permutation σ est un cycle d'ordre $r \geqslant 2$ si, et seulement s'il n'y a qu'une seule σ-orbite non réduite à un point.

Exemple 15. [Rom21, p.59] Soit $\sigma = (x_1, \ldots, x_r)$ un cycle de longueur paire. σ^2 n'est pas un cycle.

Générateurs de $\mathfrak{S}_n$

Théorème 16. [Ulm21, p.57] Tout $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{Id}\}$ s'écrit comme produit $\sigma = \gamma_1 \gamma_2 \cdots \gamma_m$ de cycles γ_i de longueur supérieure ou égale à 2 dont les supports $\mathrm{Supp}(\gamma_i)$ sont deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Exemple 17. La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$ s'écrit $\sigma = (1,2,4)(3,5)(6)$

Théorème 18. [Ber20, p.207] Soient $\sigma_1, \dots, \sigma_r \in \mathfrak{S}_n$ des permutations à supports deux à deux disjoints. Alors,

$$o(\sigma_1 \cdots \sigma_r) = \text{ppcm}(o(\sigma_1), \dots, o(\sigma_r)).$$

Exemple 19. [Rom21, p.61] Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$. Alors $\sigma^{2009} = (5,4,3,2,1)(6,7)$.

Corollaire 20. [Ber20, p.207] Soit $n \in \mathbb{N}^*$. $\mathfrak{S}_n$ est engendré par les cycles.

Corollaire 21. Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

Proposition 22. [Rom21, p.44] $\mathfrak{S}_n$ est engendré par
- les $n-1$ transpositions $(1,k)$, où $k \in [\![2,n]\!]$,
- $(k,k+1)$ où $k \in [\![1,n-1]\!]$,
- ou $(1,2)$ et $(1,2,\dots,n)$.

Permutations conjuguées

Lemme 23. [Ber20, p.209] Soit $\tau \in \mathfrak{S}_n$. Pour tout p-cycle $(i_1,\dots,i_p)$, $\tau(i_1,\dots,i_p)\tau^{-1} = (\tau(i_1),\dots,\tau(i_p))$.

Théorème 24. [Ber20, p.209] Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si, et seulement si elles ont le même nombre de cycles de chaque longueur.

Lemme 25. [IP19, p.32] Soit $\varphi \in \text{Aut}(\mathfrak{S}_n)$. Si φ transforme transposition en transposition, alors $\varphi \in \text{Int}(\mathfrak{S}_n)$.

Théorème 26. [IP19, p.32] Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur.

II. Groupe alterné

1. Signature d'une permutation

Théorème-Définition 27 (Signature)**.** [Ulm21, p.62] La signature ε est l'unique morphisme de groupes $\mathfrak{S}_n \longrightarrow \mathbb{C}^\times$ telle que La **signature d'une permutation** $\sigma \in \mathfrak{S}_n$ est l'élément $\varepsilon(\sigma)$ de défini par $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}$.

Exemple 28.
1. La signature d'une transposition vaut -1.
2. La signature d'un p-cycle vaut $(-1)^{p-1}$.

2. Structure du groupe alterné

Proposition-Définition 29. Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1,1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$. Ce sous-groupe, noté $\mathfrak{A}_n$, est appelé **sous-groupe alterné**.

Propriété 30.
- $|\mathfrak{A}_n| = \frac{n!}{2}$.
- $\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.

Théorème-Définition 31. [DÉV] Le groupe $\mathfrak{A}_n$ est simple pour $n \geqslant 5$.

III. Applications et exemples d'utilisation du groupe symétrique

1. Dérangements

Définition 32. [Rom21, p.51] On appelle **dérangement** de $[\![1,n]\!]$ toute permutation $\sigma \in \mathfrak{S}_n$ n'ayant aucun point fixe.

Théorème 33. [Rom21, p.53] Pour tout $n \in \mathbb{N}$, le nombre de dérangements de $[\![1,n]\!]$ est $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

2. Théorème de Cayley

Théorème 34 (Cayley)**.** Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}(G)$.

3. Algèbre linéaire

Déterminant

Dans cette sous-section, E désigne un $\mathbb{K}$-ev.

Théorème 35. [Gou21] L'ensemble des formes n-linéaires alternées sur un $\mathbb{K}$-ev E de dimension n est un $\mathbb{K}$-ev de dimension 1. De plus, il existe une unique forme n-linéaire alternée prenant la valeur 1 sur une base donnée de E.

Définition 36. [Gou21] soit $B = (e_1, \dots, e_n)$ une base de E. On appelle **déterminant** dans la base B, notée $\det_B$ l'unique forme n-linéaire alternée sur E prenant la valeur 1 sur la base B. Si $x_1, \dots, x_n \in E$, avec pour tout $i \in [\![1, n]\!]$, $x_i = \sum_{j=1}^{n} x_{i,j} e_j$, $\det_B(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$.

Théorème 37. Soient $x_1, \dots, x_n \in E$. Les propositions suivantes sont équivalentes :

1. Les vecteurs $x_1, \dots, x_n$ sont liés.
2. Pour toute base B de E, $\det_B(x_1, \dots, x_n) = 0$.
3. Il existe une base B de E telle que $\det_B(x_1, \dots, x_n) = 0$.

Matrice de permutation

Définition 38. [Rom21, p.54] Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de E. Soient $\sigma \in \mathfrak{S}_n$ et P_σ la matrice de passage de $\mathcal{B}$ à $\mathcal{B}_\sigma = (e_{\sigma_1}, \dots, e_{\sigma_n})$. On dit que P_σ est une **matrice de permutation**.

Exemple 39. $P_{\mathrm{Id}} = \mathrm{Id}$ et $P_{(1,\cdots,n)} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$.

Théorème 40. $P : \sigma \longmapsto P_\sigma$ est un morphisme de groupes injectif de $\mathfrak{S}_n$ dans $\mathcal{GL}_n(\mathbb{K})$ et pour toute permutation $\sigma \in \mathfrak{S}_n$, $\det(P_\sigma) = \varepsilon(\sigma)$. On a une représentation naturelle de $\mathfrak{S}_n$ dans $\mathbb{K}^n$.

Théorème 41 (Brauer)**. [DÉV]** On suppose que $\mathbb{K}$ est de caractéristique nulle. Soient $\sigma, \tau \in \mathfrak{S}_n$. σ et τ sont conjuguées si, et seulement si P_σ et P_τ sont semblables.

4. Polynômes symétriques

Définition 42. [Rom21, p.55] On dit qu'un polynôme $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si pour toute permutation $\sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

Notation 43. Pour tout $k \in [\![1, n]\!]$, on note $\Sigma_{k,n} = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} X_{i_1} \cdots X_{i_k}$.

Théorème 44. Si $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique, il existe alors un unique polynôme $Q \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$.

5. Le groupe des isométries du cube

[Rom21, p.85] On se place dans $\mathbb{R}^3$ muni d'un repère orthonormé, $A_1, \dots, A_8$ sont les huit points de coordonnées $(\pm 1, \pm 1, \pm 1)$ et $\mathcal{C}$ le cube de sommets $A_1, \dots, A_8$.

Notation 45. On note $Is(\mathcal{C})$ le groupe des isométrie de $\mathbb{R}^3$ qui conservent ce cube, $Is^+(\mathcal{C}) = Is(\mathcal{C}) \cap \mathcal{O}^+(\mathbb{R}^3)$ et $Is^-(\mathcal{C}) = Is() \cap \mathcal{O}^-(\mathbb{R}^\ni)$.

Théorème 46. Le groupe $Is(\mathcal{C})$ est aussi le groupe $Is(\mathcal{S})$ des isométries qui conservent l'ensemble $\mathcal{S}$ des sommets et c'est un sous-groupe fini isomorphe à un sous-groupe de $\mathfrak{S}_8$. La symétrie de centre 0, $\sigma_0 : x \longmapsto -x$ est dans $Is^-(\mathcal{C})$, l'application $\rho \longmapsto \rho \circ \sigma_0$ réalise une bijection de $Is^+(\mathcal{C})$ sur $Is^-(\mathcal{C})$ et $|Is(\mathcal{C})| = 2|Is^+(\mathcal{C})|$.

Développements

1. $\mathfrak{A}_n$ est simple pour $n \geqslant 5$ (31).
2. Théorème de Brauer (41).

Références

[IP19] Lucas Isenmann et Timothée Pecatte. *L'oral à l'agrégation de mathématiques*. Ellipses, 2019.

[Ber20] Grégory Berhuy. *Algèbre, le grand combat*. Calvage & Mounet, 2020.

[Gou21] Xavier Gourdon. *Math en tête, Algèbre-probabilités, 3e édition*. Ellipses, 2021.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation, Algèbre et géométrie, 2e édition*. De Boeck, 2021.

[Ulm21] Félix Ulmer. *Théorie des groupes*. Ellipses, 2021.