P. Maurer
ENS Rennes

Leçon 105. Groupes des permutations d'un ensemble fini. Applications

Devs :

- Décomposition de Bruhat
- Table des caractères de $\mathcal{S}_4$

Références :

1. Ulmer, Théorie des groupes
2. Perrin, Cours d'algèbre
3. Gourdon, Algèbre
4. Caldero-Germoni, H2G2
5. Peyre, L'algèbre discrète de la transformée de Fourier
6. FGN, Oraux X-ENS Algèbre 1

1 Généralités sur le groupe symétrique

1.1 Définitions et premières propriétés

Définition 1. *On appelle groupe symétrique d'ordre n le groupe $\mathcal{S}_n$ des bijections entre $[\![1,n]\!]$ et lui-même. Le groupe $\mathcal{S}_n$ est d'ordre $|\mathcal{S}_n| = n!$.*

Notation 2. *Pour $\sigma \in \mathcal{S}_n$, on note généralement σ sous la forme du tableau*

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

Définition 3. *Soit $\sigma \in \mathcal{S}_n$. Les éléments $i \in \{1, \ldots, n\}$ qui vérifient $\sigma(i) = i$ sont appelés points fixes de σ, et on note $\mathrm{Fix}(\sigma)$ l'ensemble de ses points fixes.*

On appelle support de σ, et on le note $\mathrm{Supp}(\sigma)$, l'ensemble $\{1, \ldots, n\} \backslash \mathrm{Fix}(\sigma)$.

Proposition 4. *Soit $\sigma, \rho \in \mathcal{S}_n$. On a toujours $\mathrm{Supp}(\sigma\rho) \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$.*

Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\rho) = \varnothing$, on dit que σ et ρ sont des permutations à support disjoint, et dans ce cas, on a $\mathrm{Supp}(\sigma\rho) = \mathrm{Supp}(\sigma) \sqcup \mathrm{Supp}(\rho)$ et

- *$\sigma\rho(i)$ est égal à $\sigma(i)$ si $i \in \mathrm{Supp}(\sigma)$ et à $\rho(i)$ si $i \in \mathrm{Supp}(\rho)$,*
- *$\sigma\rho = \rho\sigma$,*
- *$\sigma\rho = \mathrm{Id}_n \Longleftrightarrow \sigma = \rho = \mathrm{Id}_n$.*

Exemple 5. On considère $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Alors $\mathrm{Supp}(\sigma) = \{1, 2\}$ et $\mathrm{Supp}(\tau) = \{2, 3\}$, et on vérifie que σ et τ ne commutent pas. En particulier, le résultat précédent est faux lorsque le support n'est pas disjoint, et le groupe $\mathcal{S}_n$ n'est, en général, pas commutatif (sauf pour $n = 1$ ou $n = 2$).

Proposition 6. *(théorème de Cayley)*
Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathcal{S}_n$.

Remarque 7. Le théorème de Cayley a une utilité pratique assez restreinte, car $\mathcal{S}_n$ a un cardinal beaucoup plus gros que G.

1.2 Cycles, orbites et types

Définition 8. *Soit $\ell \geq 1$ un entier et $i_1, \ldots, i_\ell$ des éléments distincts de $[\![1,n]\!]$. La permutation γ définie par $\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \ldots, i_\ell\} \\ j+1 & \text{si } j \in \{i_1, \ldots, i_{\ell-1}\} \\ i_1 & \text{si } j = i_{\ell-1} \end{cases}$ est notée $(i_1, \ldots, i_\ell)$ et est appelée cycle de longueur ℓ.*

Un cycle de longueur deux est appelé une transposition.

Proposition 9. *Dans $\mathcal{S}_n$, les k-cycles sont au nombre de $\begin{pmatrix} n \\ k \end{pmatrix}(k-1)!$.*

Théorème 10.
Toute permutation $\sigma \in \mathcal{S}_n$ s'écrit comme produit $\sigma = \gamma_1 \cdots \gamma_m$ de cycles γ_i de longueur $\ell \geq 2$ dont les supports sont deux à deux disjoints et correspondent aux orbites de l'action du groupe $\langle\sigma\rangle$ sur l'ensemble $\{1, \ldots, n\}$. Cette décomposition est unique à l'ordre des facteurs près.

Exemple 11. La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \in \mathcal{S}_6$ se décompose en $\sigma = (1, 2, 4)(3, 5)$.

Définition 12. *Soit $n \geq 0$. On appelle type d'une permutation $\sigma \in \mathcal{S}_n$, et on note $[\ell_1, \ldots, \ell_m]$, la liste des cardinaux ℓ_i des orbites dans $\{1, \ldots, n\}$ de l'action de $\langle\sigma\rangle$ sur $\{1, \ldots, n\}$, rangée en ordre croissant.*

Proposition 13. *Une permutation $\sigma \in \mathcal{S}_n$ de type $[\ell_1, \ldots, \ell_n]$ a pour ordre le plus petit multiple commun des ℓ_i.*

Proposition 14. *Deux permutations σ et ρ sont conjuguées dans $\mathcal{S}_n$ si et seulement si elles ont le même type. En particulier, pour $\omega \in \mathcal{S}_n$, et tout cycle $(i_1, \ldots, i_\ell) \in \mathcal{S}_n$, on a l'identité*

$$\omega\,(i_1, \ldots, i_\ell)\,\omega^{-1} = (\omega(i_1), \ldots, \omega(i_\ell)).$$

Corollaire 15. *Les classes de conjugaison des éléménts de $\mathcal{S}_n$ sont uniquement déterminées par leur type. La proposition 9 permet alors de déterminer le cardinal de ces classes, ce qui est utile notamment pour dresser la table des caractères de $\mathcal{S}_n$, comme on le fera dans le cas $n=4$.*

Exemple 16. Les classes de conjugaison de $\mathcal{S}_4$ sont :

- $[1]$: La classe de l'identité, qui possède 1 élément.
- $[2]$: La classe des transpositions, qui possède 6 éléments.
- $[2,2]$: La classe des doubles transpositions, qui possède 3 éléments.
- $[3]$: La classe des 3-cycles, qui possède 8 éléments.
- $[4]$: La classe des 4-cycles, qui possède 6 éléments.

1.3 Générateurs

Proposition 17. *Tout cycle $(i_1 \cdots i_\ell)$ s'écrit comme produit de transpositions $(i_1 i_2)(i_2\, i_3)\cdots(i_{\ell-1}\, i_\ell)$.*

Corollaire 18. *Le groupe symétrique est engendré par les transpositions.*

Proposition 19. *Le groupe symétrique $\mathcal{S}_n$ est engendré par $(1,2),(1,3),\ldots,(1,n)$.*

Il est aussi engendré par $(1,2)$ et $(1,2,3,\ldots,n)$.

2 Signature et groupe alterné

2.1 Le morphisme signature

Définition 20. *Soit $\sigma\in\mathcal{S}_n$. On appelle signature de σ, et on note $\varepsilon(\sigma)$, le nombre*

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

Proposition 21. *L'application $\varepsilon\colon\mathcal{S}_n\rightarrow\{-1,1\}$ est un morphisme de groupes. Son noyau est appelé le groupe alterné, noté $\mathcal{A}_n$. C'est un sous-groupe distingué de $\mathcal{S}_n$.*

Proposition 22. *La parité du nombre de transpositions dans la décomposition en produit de transpositions $\sigma\in\mathcal{S}_n$ ne dépend pas de la décomposition, et $\varepsilon(\sigma)$ vaut 1 ou -1 selon que ce nombre est pair ou impair.*

Proposition 23. *Si $\sigma\in\mathcal{S}_n$ est de type $[\ell_1,\ldots,\ell_m]$, alors*

$$\varepsilon(\sigma)=(-1)^{\ell_1-1}(-1)^{\ell_2-1}\cdots(-1)^{\ell_m-1}.$$

2.2 Propriétés du groupe alterné

Définition 24. *On dit qu'une permutation $\sigma\in\mathcal{S}_n$ est paire si $\varepsilon(\sigma)=1$. L'ensemble des permutations paire est donc $\mathcal{A}_n=\mathrm{Ker}(\varepsilon)$.*

Proposition 25. *Pour $n\geq 2$, le groupe $\mathcal{A}_n$ est un sous-groupe distingué d'indice 2 de $\mathcal{S}_n$. Il contient $\frac{n!}{2}$ éléments.*

Proposition 26. *Les cycles de longueur 3 engendrent $\mathcal{A}_n$.*

Proposition 27. *Le groupe $\mathcal{A}_n$ est simple pour $n\geq 5$.*

Corollaire 28. *On a $D(\mathcal{A}_n)=\mathcal{A}_n$ pour $n\geq 5$ et $D(\mathcal{S}_n)=\mathcal{A}_n$ pour $n\geq 2$, où D désigne le groupe dérivé.*

3 Quelques applications des groupes symétriques

3.1 En algèbre linéaire : déterminant et groupe linéaire

Définition 29. *Soit $E_1,\ldots,E_p$ et F des k-espaces vectoriels. Une application :*

$$f\colon E_1\times\cdots\times E_p\rightarrow F$$

est dite p-linéaire si en tout point, les p applications partielles sont linéaires. Si $p=2$, f est dite bilinéaire. L'ensemble de ces applications est noté $\mathcal{L}(E_1,\ldots,E_p,F)$. C'est un k-espace vectoriel.

Si $E_1=\cdots=E_p=E$ et $F=k$, on parle de forme p-linéaire sur E, et l'ensemble des formes p-linéairs sur E est noté $\mathcal{L}_p(E,k)$.

Définition 30. *Soit $f\in\mathcal{L}_p(E,k)$.*

- *f est dite alternée si $f(x_1,\ldots,x_p)=0$ dès que deux vecteurs parmi les x_i sont égaux.*
- *f est dite antisymétrique si l'échange de deux valeurs dans le p-uplet $(x_1,\ldots,x_p)$ donne à f des valeurs opposées.*

Proposition 31. *f est antisymétrique si et seulement si pour tout $\sigma\in\mathcal{S}_p$ et pour tout $(x_1,\ldots,x_p)\in E^p$, on a $f(x_{\sigma(1)},\ldots,x_{\sigma(p)})=\varepsilon(\sigma)f(x_1,\ldots,x_p)$.*

Théorème 32. *L'ensemble des formes n-linéaires alternées sur E forme un k-espace vectoriel de dimension 1. De plus, il existe une unique forme n-linéaire alternée prenant la valeur 1 sur une base donnée de E. On l'appelle déterminant dans la base B et on la note $\det_B$.*

Proposition 33. *Soit $(x_1, \ldots, x_n) \in E^n$. On a :*

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

Définition 34. *Soit $f \in \mathcal{L}(E)$ et $B = (e_1, \ldots, e_n)$ une base de E. Le scalaire $\det_B(f(e_1), \ldots, f(e_n))$ ne dépend pas de la base choisie. On l'appelle déterminant de f et on le note $\det(f)$.*

Proposition 35. *Le déterminant vérifie les propriétés suivantes :*

- *Si $f, g \in \mathcal{L}(E)$ alors $\det(f \circ g) = \det(f) \cdot \det(g)$.*
- *On a $\det \mathrm{Id}_E = 1$.*
- *Si $f \in \mathcal{L}(E)$, alors $f \in \mathrm{GL}(E) \Longleftrightarrow \det f \neq 0$, et dans ce cas on a $\det(f^{-1}) = (\det f)^{-1}$.*

Définition 36. *On note $B_n(\mathbb{K})$ l'ensemble des matrices triangulaires inversibles de $\mathrm{GL}_n(\mathbb{K})$. C'est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.*

Définition 37. *Soit $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$. Pour $\sigma \in \mathcal{S}_n$, on note w_σ l'application linéaire donnée par $w_\sigma(e_i) = e_{\sigma(i)}$ pour tout $i \in [\![1, n]\!]$.*

Proposition 38. *L'application $w: \sigma \mapsto w_\sigma$ est un morphisme de groupes injectif de $\mathcal{S}_n$ dans $\mathrm{GL}_n(\mathbb{K})$.*

Développement 1 :

Théorème 39. *(décomposition de Bruhat)*
En notant, pour $\sigma \in \mathcal{S}_n$, $B_n(\mathbb{K})\, w_\sigma\, B_n(\mathbb{K}) := \{t w_\sigma s \ : \ t, s \in B_n(\mathbb{K})\}$, on a la décomposition :

$$\mathrm{GL}_n(\mathbb{K}) = \bigsqcup_{\sigma \in \mathcal{S}_n} B_n(\mathbb{K})\, w_\sigma\, B_n(\mathbb{K})$$

3.2 En géométrie : groupes d'isométries et table de $\mathcal{S}_4$

On considère un espace affine euclidien $\mathcal{E}$ dirigé par l'espace vectoriel $E = \mathbb{R}^n$. $\|.\|$ désigne la norme issue du produit scalaire $\langle .|. \rangle$ sur $\mathcal{E}$.

Définition 40. *On appelle application affine de $\mathcal{E}$ dans lui-même une application $f: \mathcal{E} \to \mathcal{E}$, telle qu'il existe $\varphi \in \mathcal{L}(\mathbb{R}^n)$ vérifiant :*

$$\forall A, B \in \mathcal{E} \quad \overrightarrow{f(A) f(B)} = \varphi(\overrightarrow{AB})$$

Dans ce cas, on dit que φ est la partie linéaire de f et on note $\varphi =: \vec{f}$. On note $\mathrm{Aff}(\mathcal{E})$ l'ensemble des applications affines de $\mathcal{E}$ dans lui-même.

On appelle isométrie de $\mathcal{E}$ toute application $\varphi: \mathcal{E} \to \mathcal{E}$ qui conserve les distances :

$$\forall x, y \in \mathcal{E} \quad \|\varphi(x) - \varphi(y)\| = \|x - y\|$$

On appelle isométrie affine de $\mathcal{E}$ une application affine de $\mathcal{E}$ dans lui-même qui est une isométrie.

Définition 41. *On appelle groupe affine de A l'ensemble $\mathrm{GA}(\mathcal{E})$ des applications affine de A dans lui-même bijectives.*

Proposition 42. *On a $\mathrm{GA}(\mathcal{E}) = \{f \in \mathrm{Aff}(\mathcal{E}) \mid \vec{f} \in \mathrm{GL}(E)\}$.*

Définition 43. *Soit X une partie de $\mathcal{E}$. Le groupe d'isométries de X, note $\mathrm{Is}(X)$, est constitué des isométries affines qui laissent X invariant. C'est un sous-groupe de $\mathrm{GA}(\mathcal{E})$.*

Le groupe des déplacements de X, noté $\mathrm{Is}^+(X)$, est le sous-groupe des applications de $\mathrm{Is}(X)$ dont le déterminant de la partie linéaire vaut 1.

Lemme 44. *Le groupe d'isométries d'un ensemble convexe laisse stable ses points extrémaux.*

Proposition 45. *On considère $\mathcal{E} = \mathbb{R}^3$ en tant qu'espace affine euclidien.*

Le groupe d'isométries du tétraèdre Δ_4 est isomorphe à $\mathcal{S}_4$, et son groupe des déplacements est isomorphe à $\mathcal{A}_4$

Le groupe d'isométries du cube C_6 est isomorphe au produit $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$, et son groupe des déplacements est isomorphe à $\mathcal{S}_4$.

Développement 2 :

Théorème 46. *La table des caractères de $\mathcal{S}_4$ est donnée par*

	[1]	[2]	[2, 2]	[3]	[4]
χ_1	1	1	1	1	1
χ_ε	1	−1	1	1	−1
χ_s	3	1	−1	0	−1
χ_W	2	0	2	−1	0
χ_C	3	−1	−1	0	1

.

3.3 En théorie des groupes : les théorèmes de Sylow

Définition 47. *Pour $n \in \mathbb{N}$ et $\mathbb{K}$ un corps, on note $U_n(\mathbb{K})$ l'ensemble des matrices triangulaires supérieures dont les coefficients diagonaux sont tous égaux à 1. On admet que c'est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$.*

Proposition 48. *Soit p un nombre premier et $n \in \mathbb{N}$. Alors on a :*

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1) \cdots (p^n - p^{n-1}) = m\, p^{\frac{n(n-1)}{2}} \quad \text{et} \quad |U_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}}$$

Où $m = (p-1)\cdots(p^n-1)$ est premier avec p.

Proposition 49. *Soit G un p-groupe agissant sur un ensemble X. On considère l'ensemble des points fixes de X pour cette action $X^G := \{x \in X \ : \ \forall g \in G \quad gx = x\}$. Alors on a l'égalité :*

$$|X| \equiv |X^G| \ [p]$$

Définition 50. *Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. On dit que $H < G$ est un p-Sylow de G si c'est un sous-groupe d'ordre p^α.*

Théorème 51. ***(Sylow via le théorème de Cayley)***

Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k \equiv 1 \pmod p$ et k divise m.*

Exemple 52. Tout groupe d'ordre 15 est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exemple 53. Il n'existe pas de groupe simple d'ordre 63 et 255.