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

1. Définition et première propriété

1.1. Le groupe symétrique

1. Définition. Le *groupe symétrique* d'un ensemble E est le groupe des bijections de E dans lui-même, noté $\mathfrak{S}(E)$. Lorsque $E = [\![1, n]\!]$, on notera $\mathfrak{S}_n = \mathfrak{S}(E)$.
2. Remarque. Le cardinal de $\mathfrak{S}_n$ est $n!$.
3. Notation. Pour une permutation $\sigma \in \mathfrak{S}_n$, on la notera sous la forme
$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$
4. Exemple. La matrice
$$\sigma_0 \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$
représente une permutation de l'ensemble $[\![1, 5]\!]$. On a $\sigma(1) = 4$ et $\sigma(5) = 5$.
5. Remarque. La groupe $\mathfrak{S}_n$ agit naturellement sur l'ensemble $[\![1, n]\!]$ par l'action
$$(\sigma, x) \in \mathfrak{S}_n \times [\![1, n]\!] \longmapsto \sigma(x) \in [\![1, n]\!].$$
6. Proposition. L'action de $\mathfrak{S}_n$ sur $[\![1, n]\!]$ est n-transitive.
7. Définition. Soit $k \in [\![1, n]\!]$. Un *k-cycle* est une permutation $\sigma \in \mathfrak{S}_n$ telle qu'il existe des entiers $a_1, \dots, a_k \in [\![1, n]\!]$ vérifiant
   - $\sigma(a_1) = a_2$, …, $\sigma(a_k) = a_1$;
   - $\sigma(x) = x$ pour tout entier $x \in [\![1, n]\!] \setminus \{a_1, \dots, a_k\}$.

On note alors $\sigma = (a_1 \ \cdots \ a_k)$. Le *support* de la permutation σ est l'ensemble $\{a_1, \dots, a_k\}$. Une *transposition* est un 2-cycle.
8. Exemple. La permutation σ_0 est le 3-cycle $(1\ 4\ 2) = (4\ 2\ 1)$. Attention, dans la définition 7, l'écriture $(a_1 \ \cdots \ a_p)$ n'est unique qu'à permutation circulaire près.
9. Proposition. Soit $\sigma \in \mathfrak{S}_n$ et $k \in [\![1, n]\!]$. Alors σ est un k-cycle si et seulement si les orbites de σ sous $[\![1, n]\!]$ sont toutes réduites à un élément sauf une qui a k éléments.
10. Proposition. Deux permutations à support disjoints commutent.
11. Remarque. La réciproque est fausse : il suffit de prendre la même permutation.

1.2. Théorème de structures et conjugaison de permutations

12. Proposition. Deux k-cycles de $\mathfrak{S}_n$ sont toujours conjugués dans $\mathfrak{S}_n$.
13. Proposition. Soient $\tau \in \mathfrak{S}_n$ et $(a_1 \ \cdots \ a_k) \in \mathfrak{S}_n$ un k-cycle. Alors
$$\tau(a_1 \ \dots \ a_k)\tau^{-1} = (\tau(a_1) \ \cdots \ \tau(a_k)).$$
14. Théorème. Toute permutation appartenant à $\mathfrak{S}_n$ est de la forme $\sigma_1 \cdots \sigma_r$ pour des cycles $\sigma_1, \dots, \sigma_r \in \mathfrak{S}_p$ (respectivement transpositions) à supports disjoints.
15. Exemple. La permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix} \in \mathfrak{S}_6$$
se décompose en le produit $(2\ 6)(3\ 5\ 4)$.
16. Remarque. La décomposition du théorème 14 est unique à l'ordre des facteurs près.
17. Corollaire. Soit $\sigma \coloneqq \sigma_1 \cdots \sigma_r \in \mathfrak{S}_n$ une permutation décomposée comme dans le théorème 14. Alors
$$\mathrm{o}(\sigma) = \mathrm{ppcm}(\mathrm{o}(\sigma_1), \dots, \mathrm{o}(\sigma_r)).$$
18. Remarque. Pour un groupe quelconque G, on a au mieux le résultat
$$\forall g, h \in G, \quad \mathrm{o}(gh) \mid \mathrm{ppcm}(\mathrm{o}(g), \mathrm{o}(h)).$$
19. Corollaire. Deux permutations de $\mathfrak{S}_n$ sont conjuguées dans $\mathfrak{S}_n$ si et seulement si, dans leurs décompositions du théorème 14, elles ont le même nombre de k-cycles pour toute longueur $k \in [\![1, n]\!]$.
20. Exemple. Les permutations $(1\ 2)(5\ 4\ 3)$ et $(1\ 5)(4\ 2\ 3)$ sont conjuguées dans $\mathfrak{S}_5$.
21. Théorème. Soit $n \geqslant 2$ un entier.
   - Les transpositions engendrent $\mathfrak{S}_n$.
   - Les transpositions de la forme $(1\ i)$ avec $i \in [\![2, n]\!]$ engendrent $\mathfrak{S}_n$.

22. Exemple. Pour $a, b \in [\![1, n]\!]$, on a $(a\ b) = (1\ a)(1\ b)$.
23. Corollaire. Un k-cycle peut s'écrire en un produit de $k - 1$ transpositions.

2. Le groupe alterné

2.1. Le morphisme signature

24. Définition. La *signature* d'une permutation $\sigma \in \mathfrak{S}_n$ est l'entier
$$\varepsilon(\sigma) \coloneqq (-1)^{\sharp I(\sigma)} \quad \text{avec} \quad I(\sigma) \coloneqq \{(i, j) \in [\![1, n]\!]^2 \mid i < j, \sigma(i) > \sigma(j)\}.$$
25. Proposition. Soit $\sigma \in \mathfrak{S}_n$. Alors $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$.
26. Proposition. L'application $\varepsilon \colon \mathfrak{S}_n \longrightarrow \{\pm 1\}$ est un morphisme de groupes. De plus, c'est l'unique morphisme de groupes $\mathfrak{S}_n \longrightarrow \{\pm 1\}$ valant -1 sur les transpositions.
27. Corollaire. La signature d'un k-cycle vaut $(-1)^{k-1}$.
28. Définition. Le *groupe alterné* d'ordre n est le noyau $\mathfrak{A}_n \coloneqq \operatorname{Ker} \varepsilon$.

2.2. Structure du groupe alterné

29. Proposition. Si $n \geqslant 3$, les cycles d'ordre 3 engendre $\mathfrak{A}_n$.
30. Exemple. Si $a, b, c, d \in [\![1, n]\!]$, on a $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.
31. Proposition. L'action de $\mathfrak{A}_n$ sur $[\![1, n]\!]$ est simplement $n - 2$-transitive.
32. Proposition. Pour $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
33. Théorème. Pour $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple. Dév. n° 1
34. Corollaire. Les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{\mathrm{Id}\}$.
35. Exemple. Le groupe $\mathfrak{A}_4$ n'est pas distingué puisque
$$\mathrm{D}(\mathfrak{A}_4) = \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} =: V_4.$$
36. Corollaire. Soit $H \leqslant \mathfrak{S}_n$ un sous-groupe d'indice n. Alors $H \simeq \mathfrak{S}_{n-1}$.
37. Proposition. Si $n \geqslant 3$, alors $\mathrm{Z}(\mathfrak{S}_n) = \{\mathrm{Id}\}$. Si $n \geqslant 4$, alors $\mathrm{Z}(\mathfrak{A}_n) = \{\mathrm{Id}\}$.
38. Proposition. On a $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$. Si $n \geqslant 5$, alors $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$.

3. Applications

3.1. Déterminant

39. Théorème. Soit $\mathscr{B}$ une base d'un K-espace vectoriel E de dimension finie. Alors il existe un unique forme n-linéaire alternée $\det_{\mathscr{B}}$ sur E telle que $\det_{\mathscr{B}}(\mathscr{B}) = 1$. De plus, la forme $\det_{\mathscr{B}}$ engendre l'ensemble des formes n-linéaires alternées sur E.

40. Corollaire. Soit $u \in \mathscr{L}(E)$. Alors il existe un unique scalaire $\det_{\mathscr{B}}(u) \in K$ tel que

$$\det_{\mathscr{B}}(u(x_1), \dots, u(x_n)) = \det_{\mathscr{B}}(u) \times \det_{\mathscr{B}}(x_1, \dots, x_n).$$

De plus, ce scalaire $\det_{\mathscr{B}}(u)$ ne dépend pas de la base $\mathscr{B}$. On le note $\det(u)$ et on l'appelle le *déterminant* de l'endomorphisme u.

41. Proposition. Un endomorphisme $u \in \mathscr{L}(E)$ est un isomorphisme si et seulement si son déterminant $\det(u)$ est non nul.

42. Définition. Le déterminant d'une matrice $A \coloneqq (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathscr{M}_n(K)$ est le scalaire

$$\det(M) \coloneqq \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \in K.$$

43. Exemple. Pour $a, b, c, d \in K$, on a

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - cb.$$

44. Proposition. Soient $u \in \mathscr{L}(E)$ et $\mathscr{B}$ une base de E. Alors $\det(u) = \det(\mathrm{Mat}_{\mathscr{B}}(u))$.

3.2. Matrices de permutation

45. Définition. Une *matrice de permutation* est la matrice $M_\sigma \in \mathscr{M}_n(\mathbf{R})$ dans la base canonique d'une application linéaire

$$f_\sigma : \left| \begin{array}{c} \mathbf{R}^n \longrightarrow \mathbf{R}^n, \\ (x_1, \dots, x_n) \longmapsto (x_{\sigma(1)}, \dots, x_{\sigma(n)}) \end{array} \right.$$

pour une permutation $\sigma \in \mathfrak{S}_n$.

46. Exemple. Avec $\sigma \coloneqq (1\ 2)(6\ 4\ 3) \in \mathfrak{S}_6$, on a

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{GL}_6(\mathbf{R}).$$

47. Proposition. Toute matrice de permutation est stochastique.

48. Proposition. Pour deux permutations $\sigma, \tau \in \mathfrak{S}_n$, on a

$$M_\sigma M_\tau = M_{\sigma\tau} \quad \text{et} \quad M_\sigma^{-1} = M_{\sigma^{-1}}.$$

49. Proposition. Soit $\sigma \in \mathfrak{S}_n$. Notons $k \in \mathbf{N}^*$ l'ordre de cette permutation. Alors le polynôme $X^k - 1$ annule la matrice M_σ. En particulier, son spectre complexe est inclus dans le groupe $\mathbf{U}_k \subset \mathbf{C}$ des racines k-ièmes de l'unité.

50. Exemple. Avec $\sigma \coloneqq (1\ 3\ 2) \in \mathfrak{S}_3$, la matrice

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

a pour polynôme caractéristique $1 - X^3$, donc $\mathrm{Sp}_{\mathbf{C}}(M_\sigma) = \{1, j, j^2\} = \mathbf{U}_3$.

3.3. Isométrie du cube [1]

51. Définition. Le *groupe des isométries* d'un sous-ensemble $X \subset \mathbf{R}^3$ est le groupe des isométries de l'espace euclidien $\mathbf{R}^3$ stabilisant l'ensemble X. On le note $\mathrm{Isom}(X)$. De plus, le groupe des telles isométries préservant les angles est noté $\mathrm{Isom}^+(X)$.

52. Exemple. En notant $\mathbf{S}^2 \subset \mathbf{R}^3$ la sphère unité, l'endomorphisme $x \longmapsto -x$ de $\mathbf{R}^3$ appartient au groupe $\mathrm{Isom}(\mathbf{S}^2)$.

53. Proposition. Soit $C \subset \mathbf{R}^3$ le cube. Alors Dév. n° 2

$$\mathrm{Isom}^+(C) \simeq \mathfrak{S}_4 \quad \text{et} \quad \mathrm{Isom}(C) \simeq \mathfrak{S}_4 \times \mathbf{Z}/2\mathbf{Z}.$$

[1] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries*. T. Tome premier. Calvage & Mounet, 2013.
[2] Serge Lang. *Algebra*. Springer, 2002.
[3] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.