Chapitre 42

Groupe symétrique

42.1 Définition

Définition 1 Soit $n \in \mathbb{N}^\star$. On appelle **permutation** de $[\![1, n]\!]$ toute bijection de $[\![1, n]\!]$ dans $[\![1, n]\!]$. L'ensemble de ces permutations, noté $\mathcal{S}_n$ est appelé **groupe symétrique d'ordre n**.

Remarque

1. $\mathcal{S}_n = \sigma\left([\![1, n]\!]\right)$.
2. $\left(\mathcal{S}_n, \circ\right)$ est un groupe.
3. $\operatorname{card}\left(\mathcal{S}_n\right) = n!$.
4. Si E est un ensemble fini à n éléments, alors $(\mathfrak{S}(E), \circ)$ est isomorphe à $\left(\mathcal{S}_n, \circ\right)$. En effet, si f est une bijection de $[\![1, n]\!]$ dans E, alors

$$\phi : \begin{array}{ccc} \mathfrak{S}(E) & \to & \mathcal{S}_n \\ \sigma & \mapsto & f \circ \sigma \circ f^{-1} \end{array}$$

est un isomorphisme de groupes. Autrement dit, l'étude de $\mathcal{S}_n$ «contient» celle de $\mathfrak{S}(E)$.

Notation Soit $\sigma \in \mathcal{S}_n$. On note

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Définition 2

Soit $p \in [\![2, n]\!]$. Un **cycle de longueur p** est un élément σ de $\mathcal{S}_n$ tel qu'il existe p éléments distincts de $i_1, i_2, \dots, i_p \in [\![1, n]\!]$ vérifiant

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots \quad \sigma(i_{p-1}) = i_p, \quad \sigma(i_p) = i_1$$
$$\text{et } \forall j \in [\![1, n]\!] \setminus \{ i_1, \dots, i_p \}, \sigma(j) = j.$$

- L'ensemble $\{ i_1, \dots, i_p \}$ est le **support** du cycle σ.
- Ce cycle se note également $\begin{pmatrix} i_1 & i_2 & \dots & i_p \end{pmatrix}$.
- Un cycle de longueur 2 est une **transposition**.

Exemple 3

On considère la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}.$$

La permutation σ est un cycle de longueur 4. On a $\sigma = \begin{pmatrix} 1 & 5 & 2 & 3 \end{pmatrix}$ mais aussi $\sigma = \begin{pmatrix} 2 & 3 & 1 & 5 \end{pmatrix}$.
On a aussi

$$\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix}$$
$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 5 \end{pmatrix}$$
$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathrm{Id}_{[\![1,5]\!]}$$
$$\sigma^{-1} = \begin{pmatrix} 3 & 2 & 5 & 1 \end{pmatrix}.$$

Remarque

Deux cycles à supports disjoints commutent.

42.2 Décomposition des permutations

Théorème 4

Toute permutation de $[\![1, n]\!]$ distincte de $\mathrm{Id}_{[\![1,n]\!]}$ peut s'écrire comme composée de cycles de supports deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Démonstration. Non exigible. ∎

Exemple 5

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 7 & 8 \end{pmatrix} = \begin{pmatrix} 7 & 8 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix}.$$

Remarque

Cette décomposition permet de calculer facilement les puissance d'une permutation.

Théorème 6

Toute permutation de $[\![1,n]\!]$ peut s'écrire comme composée de transposition. Cette décomposition n'est pas unique.

Démonstration. Il suffit de montrer que tout cycle est composée de transposition. Soit $\begin{pmatrix} i_1 & i_2 & \dots & i_p \end{pmatrix}$ un cycle de longueur p, alors

$$\begin{pmatrix} i_1 & i_2 & \dots & i_p \end{pmatrix} = \begin{pmatrix} i_1 & i_2 \end{pmatrix} \circ \begin{pmatrix} i_2 & i_3 \end{pmatrix} \circ \dots \circ \begin{pmatrix} i_{p-1} & i_p \end{pmatrix}.$$

∎

Remarque

- $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix}$.

42.3 Signature d'une permutation

Définition 7

Soit $\sigma \in \mathcal{S}_n$ $(n \geq 2)$. Soit $(i,j) \in [\![1,n]\!]^2$. On dit que (i,j) est une **inversion** pour σ si

$$i < j \quad \text{et} \quad \sigma(i) > \sigma(j).$$

La **signature** de σ est $(-1)^p$ où p est le nombre d'inversions de σ. On la note $\epsilon(\sigma)$.

- Si $\epsilon(\sigma) = 1$, on dit que σ est une **permutation paire**.
- Si $\epsilon(\sigma) = -1$, on dit que σ est une **permutation impaire**.

Exemple 8

Avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$.

$$1 < 2 \quad \text{et} \quad \sigma(1) = 5 > \sigma(2) = 1.$$

Donc le couple $(1,2)$ est une inversion pour σ.

Exemple 9

On a $\epsilon\left(\mathrm{Id}_{[\![1,n]\!]}\right) = (-1)^0 = 1$.

Proposition 10

Soit $\sigma \in \mathcal{S}_n$, alors

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

Théorème 11

Soit $n \in \mathbb{N}^\star$ et $(\sigma, \sigma') \in \mathcal{S}_n^2$. Alors

$$\epsilon\left(\sigma \circ \sigma'\right) = \epsilon(\sigma)\epsilon(\sigma').$$

En d'autres termes,

$$\epsilon : \begin{array}{ccc} \left(\mathcal{S}_n, \circ\right) & \to & (\{-1, 1\}, \times) \\ \sigma & \mapsto & \epsilon(\sigma) \end{array}$$

est un morphisme de groupes. C'est le seul morphisme non identiquement égal à 1.

Démonstration. Non exigible. ∎

Proposition 12

Soit $\sigma \in \mathcal{S}_n$.

1. *La signature d'une transposition est toujours -1.*
2. *On peut écrire $\sigma = \tau_1 \circ \ldots \circ \tau_q$ où les τ_i sont des transpositions. Alors $\epsilon(\sigma) = (-1)^q$.*
3. *La signature d'une cycle de longueur p est $(-1)^{p-1}$.*