

15.1 DÉFINITION

Définition 1

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

Remarque

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

$$\begin{aligned} \varphi : \mathcal{S}(E) &\rightarrow \mathcal{S}_n \\ \sigma &\mapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

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

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

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots \quad \sigma(i_{p-1}) = i_p, \quad \sigma(i_p) = i_1$$

$$\text{et } \forall j \in \llbracket 1, n \rrbracket \setminus \{i_1, \dots, i_p\}, \sigma(j) = j.$$

- L'ensemble $\{i_1, \dots, i_p\}$ est le **support** du cycle σ .
- Ce cycle se note également $(i_1 \ i_2 \ \dots \ i_p)$.
- 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 $\sigma = (1 \ 5 \ 2 \ 3)$ mais aussi $\sigma = (2 \ 3 \ 1 \ 5)$.

On a aussi

$$\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} = (1 \ 2) \circ (3 \ 5) = (3 \ 5) \circ (1 \ 2)$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} = (1 \ 3 \ 2 \ 5)$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \text{Id}_{\llbracket 1, 5 \rrbracket}$$

$$\sigma^{-1} = (3 \ 2 \ 5 \ 1).$$

Remarque

Deux cycles à supports disjoints commutent.

15.2 DÉCOMPOSITION DES PERMUTATIONS

Théorème 4

Toute permutation de $\llbracket 1, n \rrbracket$ distincte de $\text{Id}_{\llbracket 1, n \rrbracket}$ 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

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

Remarque

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

Théorème 6

Toute permutation de $\llbracket 1, n \rrbracket$ 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 $(i_1 \ i_2 \ \dots \ i_p)$ un cycle de longueur p , alors

$$(i_1 \ i_2 \ \dots \ i_p) = (i_1 \ i_2) \circ (i_2 \ i_3) \circ \dots \circ (i_{p-1} \ i_p).$$

■

Remarque

$$(1 \ 2 \ 3) = (1 \ 2) \circ (2 \ 3) = (1 \ 3) \circ (1 \ 2).$$

15.3 SIGNATURE D'UNE PERMUTATION

Définition 7

Soit $\sigma \in \mathcal{S}_n$ ($n \geq 2$). Soit $(i, j) \in \llbracket 1, n \rrbracket^2$. 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 $\varepsilon(\sigma)$.

- Si $\varepsilon(\sigma) = 1$, on dit que σ est une **permutation paire**.
- Si $\varepsilon(\sigma) = -1$, 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 $\varepsilon(\text{Id}_{\llbracket 1, n \rrbracket}) = (-1)^0 = 1$.

Proposition 10

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

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

Théorème 11

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

$$\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma').$$

En d'autres termes,

$$\begin{aligned} \varepsilon : (\mathcal{S}_n, \circ) &\rightarrow (\{-1, 1\}, \times) \\ \sigma &\mapsto \varepsilon(\sigma) \end{aligned}$$

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 $\sigma = \tau_1 \circ \dots \circ \tau_q$ où les τ_i sont des transpositions. Alors $\varepsilon(\sigma) = (-1)^q$.
3. La signature d'un cycle de longueur p est $(-1)^{p-1}$.