CHAPITRE 14

GROUPE SYMÉTRIQUE

GROUPES DES PERMUTATIONS D'UN ENSEMBLE

Soit X un ensemble et $\mathcal{S}(X)$ l'ensemble des permutations de X.

Si f, g sont des permutations de X, il en est de même de $f \circ g$; $(f, g) \mapsto f \circ g$ définit donc une loi de composition interne sur l'ensemble $\mathcal{S}(X)$; cette loi de composition interne est associative ; elle admet un élément neutre, à savoir l'application identique Id_X ; enfin, si f est une permutation de X, il en est de même de l'application réciproque f^{-1} et celle-ci est évidemment inverse de f pour la loi de composition interne considérée.

Théorème 1 — *$(\mathcal{S}(X), \circ)$ est un groupe.*

Le groupe $\mathcal{S}(X)$ s'appelle le **groupe des permutations** de l'ensemble X ou **groupe symétrique** de X.

C'est l'étude de ces groupes par Galois (lorsque X est un ensemble fini) qui a conduit, historiquement, à la notion générale et «abstraite» de groupe.

Supposons maintenant X fini de cardinal $n \geq 1$ et donnons nous un bijection

$$\begin{array}{rccc} \varphi : & [\![1, n]\!] & \to & X \\ & i & \mapsto & x_i \end{array}.$$

Alors

$$\begin{array}{rccc} \mathcal{S}([\![1, n]\!]) & \to & \mathcal{S}(X) \\ \sigma & \mapsto & \varphi^{-1} \circ \sigma \circ \varphi \end{array} \quad \text{et} \quad \begin{array}{rccc} \mathcal{S}(X) & \to & \mathcal{S}([\![1, n]\!]) \\ f & \mapsto & \varphi \circ f \circ \varphi^{-1} \end{array}$$

sont des isomorphismes de groupes, réciproque l'un de l'autre.

Cela justifie qu'en pratique, nous n'étudierons que le groupe des permutations des $[\![1, n]\!]$.

14.1 PERMUTATIONS

§1 Définitions

Définition 2

Soit $n \in \mathbb{N}^\star$.

- On appelle **permutation** de $[\![1,n]\!]$ toute bijection de $[\![1,n]\!]$ dans $[\![1,n]\!]$.
- Le groupe des permutations de $[\![1,n]\!]$ est noté $\mathcal{S}_n$.

Remarque

1. $\mathcal{S}_n = \mathcal{S}([\![1,n]\!])$.
2. $(\mathcal{S}_n, \circ)$ est un groupe.
3. $\operatorname{card}(\mathcal{S}_n) = n!$.

Notation

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

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

Exemple 3

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix}$. Alors

$$\sigma' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 5 & 1 \end{pmatrix} \qquad \sigma \circ \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 5 & 2 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix} \qquad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 5 & 6 \end{pmatrix}.$$

Définition 4

Soit $\sigma \in \mathcal{S}_n$ et $x \in [\![1,n]\!]$.

- L'**orbite** de $x \in [\![1,n]\!]$ pour σ est l'ensemble

$$\operatorname{orb}(x) = \left\{ \sigma^k(x) \;\middle|\; k \in \mathbb{N} \right\}.$$

- On dit que x est un **point fixe** pour σ si $\sigma(x) = x$.
- Le **support** de σ est l'ensemble des éléments de E qui ne sont pas fixes pour σ:

$$\operatorname{supp}(\sigma) = \{\, i \in [\![1,n]\!] \mid \sigma(i) \neq i \,\}.$$

- L'**ordre** de σ est le plus petit entier k tel que $\sigma^k = \mathrm{Id}$. C'est aussi l'ordre du sous-groupe monogène engendré par σ.

Exemple 5

Le support de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$ est $\{\, 1,2,3,4,5 \,\}$.
Cette permutation a trois orbites : celle du point fixe $\{\, 6 \,\}$ et deux autres $\{\, 1,2,3 \,\}$ et $\{\, 4,5 \,\}$.
Cette permutation est d'ordre 6.

§2 Cycles

Définition 6

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 $x_1, x_2, \dots, x_p \in [\![1, n]\!]$ vérifiant

$$\sigma(x_1) = x_2, \quad \sigma(x_2) = x_3, \quad \dots \quad \sigma(x_{p-1}) = x_p, \quad \sigma(x_p) = x_1$$
$$\text{et } \forall j \in [\![1, n]\!] \setminus \{ x_1, \dots, x_p \}, \sigma(j) = j.$$

- L'ensemble $\{ x_1, \dots, x_p \}$ est le **support** du cycle σ.
- Ce cycle se note également $\begin{pmatrix} x_1 & x_2 & \dots & x_p \end{pmatrix}$.
- Un cycle de longueur 2 est une **transposition**.

Exemple 7

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

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

Test 8

Conjugaison
Soit σ un élément de $\mathcal{S}_n$ et $\sigma' = \begin{pmatrix} x_1 & x_2 & \dots & x_p \end{pmatrix}$ un cycle de longueur p. Alors

$$\sigma \circ \begin{pmatrix} x_1 & x_2 & \dots & x_p \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_p) \end{pmatrix}.$$

14.2 Décomposition des permutations

Proposition 9 *Deux cycles à supports disjoints commutent.*

Théorème 10 *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 11

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

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

Théorème 12 *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 $(x_1 \quad x_2 \quad \dots \quad x_p)$ un cycle de longueur p, alors

$$(x_1 \quad x_2 \quad \dots \quad x_p) = (x_1 \quad x_2) \circ (x_2 \quad x_3) \circ \dots \circ (x_{p-1} \quad x_p).$$

∎

Remarque

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

14.3 Signature d'une permutation

Définition 13 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 $\varepsilon(\sigma)$.

- 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 14 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 15

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

Proposition 16

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

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

où la notation $\prod_{\{\,i,j\,\}}$ est le produit sur toutes les paires $\{\,i,j\,\} \subset [\![1,n]\!]$ (donc avec $i \neq j$).

Démonstration. Une paire $\{\,i,j\,\}$ est une inversion si, et seulement si $\frac{\sigma(j)-\sigma(i)}{i-j} < 0$. On a donc

$$\prod_{\{\,i,j\,\}} \frac{\sigma(j)-\sigma(i)}{j-i} = (-1)^p \prod_{\{\,i,j\,\}} \frac{|\sigma(j)-\sigma(i)|}{|j-i|},$$

où p désigne le nombre d'inversion de σ.

Or σ est une permutation de $[\![1,n]\!]$ donc $\{\,\sigma(i),\sigma(j)\,\}$ décrit l'ensemble des paires de $[\![1,n]\!]$ lorsque $\{\,i,j\,\}$ décrit l'ensemble des paires de $[\![1,n]\!]$. Ainsi

$$\prod_{\{\,i,j\,\}} |\sigma(j)-\sigma(i)| = \prod_{\{\,i,j\,\}} |j-i|$$

et donc

$$\prod_{\{\,i,j\,\}} \frac{\sigma(j)-\sigma(i)}{j-i} = (-1)^p = \varepsilon(\sigma).$$

∎

Théorème 17

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

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

En d'autres termes,

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

est un morphisme de groupes.

- *C'est le seul morphisme non identiquement égal à 1.*
- *C'est le seul morphisme envoyant toute transposition sur -1.*

Démonstration. Non exigible. ∎

Proposition 18

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 $\varepsilon(\sigma) = (-1)^q$.*
3. *La signature d'une cycle de longueur p est $(-1)^{p-1}$.*