

Chapitre 2 : Permutations

Dans ce chapitre, n désigne un entier naturel non nul.

I Généralités

\mathfrak{S}_n est le groupe des permutations sur $\llbracket 1, n \rrbracket$, muni de la loi \circ .

Notations :

- Le neutre est noté Id ou $1_{\mathfrak{S}_n}$
- $\sigma \circ \sigma'$ est noté $\sigma\sigma'$ (attention, non commutatif)
- Le symétrique de σ est noté σ^{-1} .

Soit $\sigma \in \mathfrak{S}_n$:

- Soit $A \subset \{1, \dots, n\}$.

$$\begin{aligned} A \text{ est stable par } \sigma &\stackrel{\text{d\u00e9f}}{\Leftrightarrow} \sigma(A) \subset A \\ &\Leftrightarrow \sigma(A) = A \end{aligned}$$

La deuxième équivalence se justifie par le fait que σ est bijective et A est finie donc $\sigma(A)$ et A ont même cardinal.

- Soit $i \in \llbracket 1, n \rrbracket$.

On dit que σ fixe i , ou que i est invariant par σ , ou encore que i est un point fixe de σ lorsque $\sigma(i) = i$.

- Le support de σ est $\{i \in \llbracket 1, n \rrbracket, \sigma(i) \neq i\}$

Proposition :

Soit $\sigma \in \mathfrak{S}_n$, A le support de σ . Alors A est stable par σ et on peut identifier σ à une permutation sur A ou n'importe quelle partie B telle que $A \subset B \subset \{1, \dots, n\}$.

En effet : soit $i \in A$. Montrons qu'alors $\sigma(i) \in A$, c'est-à-dire que $\sigma(\sigma(i)) \neq \sigma(i)$.

Supposons que $\sigma(\sigma(i)) = \sigma(i)$. Alors $\sigma^{-1}(\sigma(\sigma(i))) = \sigma^{-1}(\sigma(i))$, soit $\sigma(i) = i$, ce qui est impossible car $i \in A$. Donc A est stable par σ .

Ainsi, $\sigma|_A$ définit une bijection de A dans A .

On peut donc considérer que $\sigma|_A \in \mathfrak{S}(A)$ (ensemble des permutations sur A).

Exemple :

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

Alors $\sigma \in \mathfrak{S}_7$, mais on peut considérer que $\sigma \in \mathfrak{S}_4$ ou même $\mathfrak{S}(\{1, 4\})$

II Transpositions et autres cycles

A) Transposition

Définition :

Soient $i, j \in \llbracket 1, n \rrbracket$, distincts.

La transposition sur i et j , notée $\tau_{i,j}$ ou (i, j) est la permutation τ définie par :

$$\begin{cases} \tau(i) = j \\ \tau(j) = i \\ \forall k \in \llbracket 1, n \rrbracket \setminus \{i, j\}, \tau(k) = k \end{cases}$$

Proposition :

Soit $\tau = (i, j)$ une transposition.

Alors le support de τ est $\{i, j\}$, et $\tau^{-1} = \tau$, c'est-à-dire que $\tau \circ \tau = \text{Id}$ ou que τ est d'ordre 2.

B) Cycles

Définition :

Soit $p \geq 2$. Un cycle de longueur p est une permutation σ telle qu'il existe $a_1, a_2, \dots, a_p \in \llbracket 1, n \rrbracket$, distincts deux à deux de sorte que :

$$\sigma(a_1) = a_2 ; \sigma(a_2) = a_3 ; \sigma(a_3) = a_4 ; \dots ; \sigma(a_p) = a_1$$

$$\text{Et } \forall k \in \llbracket 1, n \rrbracket \setminus \{a_1, a_2, \dots, a_p\}, \sigma(k) = k.$$

Proposition :

Si σ est un cycle de longueur p alors le support de σ est de cardinal p et σ est d'ordre p . On note, s'il n'y a pas d'ambiguïté, $\sigma = (a_1, a_2, a_3, \dots, a_p)$.

Théorème (admis) :

Toute permutation s'écrit comme un produit de cycles de supports disjoints.

Proposition :

Deux permutations de supports disjoints commutent.

Démonstration :

Soit σ de support I , σ' de support J .

On suppose que $I \cap J = \emptyset$ (c'est-à-dire que les supports sont disjoints)

Montrons alors que $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Soit $k \in \llbracket 1, n \rrbracket$.

- Si $k \in I$, alors $\sigma \circ \sigma'(k) = \sigma(k)$ (car $\sigma'(k) = k$ puisque $k \notin J$)

Et $\sigma' \circ \sigma(k) = \sigma(k)$ car $\sigma(k) \in I$, donc $\sigma(k) \notin J$. Donc $\sigma \circ \sigma'(k) = \sigma' \circ \sigma(k)$

- On fait le même raisonnement si $k \in J$

- Si $k \notin I \cup J$, alors $\sigma \circ \sigma'(k) = \sigma' \circ \sigma(k) = k$

Donc $\sigma \circ \sigma' = \sigma' \circ \sigma$.

III Décomposition d'une permutation en transpositions, signature

Théorème :

Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en produit de transpositions.

On dit que \mathfrak{S}_n est engendré par les transpositions

Démonstration :

Montrons par récurrence que $\forall n \in \mathbb{N}^*, \forall \sigma \in \mathfrak{S}_n$, « σ se décompose en produit de transposition ». (on note $P(n) = " \forall \sigma \in \mathfrak{S}_n, \dots "$)

- Pour $n = 1, \mathfrak{S}_1 = \{\text{Id}\}$, ok

Pour $n = 2, \mathfrak{S}_2 = \{\text{Id}, \tau_{1,2}\}$, $\text{Id} = \tau_{1,2} \circ \tau_{1,2}$ et $\tau_{1,2} = \tau_{1,2}$

- Soit $n \geq 3$, supposons $P(n-1)$.

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

Si $\sigma(n) = n$, σ peut être vue comme un élément de \mathfrak{S}_{n-1} .

Donc σ se décompose en produit de transpositions sur $\llbracket 1, n-1 \rrbracket$.

Sinon, $\sigma(n) = k$, où $k \in \llbracket 1, n-1 \rrbracket$. Notons alors $\tau = (k, n)$.

Alors $\tau \circ \sigma(n) = n$, donc $\tau \circ \sigma$ s'écrit comme produit de transposition, à savoir :

$$\tau \circ \sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_p$$

Donc $\sigma = \tau \circ \tau \circ \sigma = \tau \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_p$, ce qui achève la récurrence.

Exemple avec cette méthode :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 6 & 5 & 9 & 1 & 7 & 4 & 3 \end{pmatrix};$$

$$(3,9) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 5 & 3 & 1 & 7 & 8 & 9 \end{pmatrix}; (8,4) \circ (3,9) \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 5 & 3 & 1 & 7 & 8 & 9 \end{pmatrix} \dots$$

$$(1,2) \circ (3,1) \circ (4,3) \circ (5,3) \circ (6,1) \circ (8,4) \circ (3,9) \circ \sigma = \text{Id}$$

$$\text{Donc } \sigma = (3,9) \circ (8,4) \circ (6,1) \circ (5,3) \circ (4,3) \circ (3,1) \circ (1,2).$$

Autre exemple : décomposition d'un cycle

$$(1,2,3,4,5,6,7) = (1,7)(1,6)(1,5)(1,4)(1,3)(1,2) = (1,2)(2,3)(3,4)(4,5)(5,6)(6,7)$$

Plus généralement :

$$(a_1, a_2, \dots, a_p) = (a_1, a_p)(a_1, a_{p-1}) \dots (a_1, a_2) = (a_1, a_2)(a_2, a_3) \dots (a_{p-1}, a_p)$$

Théorème, définition (admis) :

Il n'y a pas unicité de la décomposition d'une permutation σ en produit de transposition (évident), mais la parité du nombre de transposition ne dépend que de σ .

Par définition, la signature de σ , notée $\varepsilon(\sigma)$ est 1 si ce nombre est pair, -1 sinon.

Proposition :

L'application $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$ est un morphisme de (\mathfrak{S}_n, \circ) dans $(\{-1, 1\}, \times)$.

$$\sigma \mapsto \varepsilon(\sigma)$$

Démonstration :

Soient σ, σ' décomposées respectivement en p et q transpositions.

Alors $\sigma \circ \sigma'$ se décompose en $p + q$ transpositions.

$$\text{Donc } \varepsilon(\sigma \circ \sigma') = (-1)^{p+q} = (-1)^p (-1)^q = \varepsilon(\sigma) \times \varepsilon(\sigma')$$

Le noyau de ε est $A_n = \{\sigma \in \mathfrak{S}_n, \varepsilon(\sigma) = 1\}$, qui est un sous-groupe de \mathfrak{S}_n .

On l'appelle le groupe alterné sur n éléments ; on a $\text{card}(A_n) = \frac{n!}{2}$

En effet : $\mathfrak{S}_n = A_n \cup (\mathfrak{S}_n \setminus A_n)$. Donc $\text{card}(A_n) + \text{card}(\mathfrak{S}_n \setminus A_n) = \text{card}(\mathfrak{S}_n) = n!$

De plus, l'application $\varphi : \sigma \mapsto \tau \circ \sigma$ (où τ est une transposition fixée) est bijective (d'inverse elle-même), et $\varphi(A_n) = \mathfrak{S}_n \setminus A_n$. Donc $\text{card}(A_n) = \text{card}(\mathfrak{S}_n \setminus A_n)$, d'où le résultat.

Exemple important : un cycle de longueur p est de signature $(-1)^{p-1}$.