

Groupe symétrique

E est un ensemble. Sauf dans le paragraphe 1, E est supposé **fini** égal à l'ensemble $\llbracket 1, n \rrbracket$.

1 LES DIFFÉRENTES PERMUTATIONS

1.1 GÉNÉRALITÉ

Définition 1 : Permutations

Une **permutation** d'un ensemble E est une application de E dans E bijective.

Le **groupe symétrique de E** est l'ensemble des permutations de E muni de la composition. Il est noté $S(E)$ ou plus simplement S_n lorsque $E = \llbracket 1, n \rrbracket$.

On a déjà montré que S_n est une groupe !

Notations

On note une permutation $\sigma \in S_n$,
$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}.$$

Exemple 1

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

On a alors

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

Proposition 1

Le groupe $\mathfrak{S}_n$ est fini de cardinal $n!$.

Définition 2 : Orbite

L'**orbite d'un élément** $x \in E$ pour $\sigma \in S(E)$ est l'ensemble $\mathcal{O}(x) := \{\sigma^k(x) \mid k \in \mathbb{N}\}$.

On dit que σ laisse un élément $x \in E$ **fixe**, si $\sigma(x) = x$.

Le **support** de $\sigma \in S(E)$ est l'ensemble des éléments de E qui ne sont pas fixes pour σ .

Orbite d'un élément laissé fixe

Si un élément $x \in E$ est laissé fixe par $\sigma \in S(E)$, alors $\mathcal{O}(x) = \{\sigma^k(x) \mid k \in \mathbb{N}\} = \{x\}$.
Donc la cardinal de l'orbite de x est 1.

Exemple 2

Le support de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 6 & 2 & 3 & 8 & 7 & 4 & 5 \end{pmatrix}$ est $\{2, 3, 4, 5, 6, 8, 9\}$. Cette permutation admet trois orbites : celles des points fixes $\{1\}$ et $\{7\}$ et l'orbite $\{2, 9, 5, 3, 6, 8, 4\}$.

2 CYCLES**Définition 3 : Cycles**

Un **cycle de $S(E)$** est une permutation $\sigma \in S(E)$ qui n'admet qu'une seule orbite sur son support.

La **longueur d'un cycle** est la cardinal de son support. On peut alors parler de l -cycle.

Un 2-cycle est appelé une **transposition**.

Exemple 3

La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}$ est un cycle car $\sigma(1) = 4, \sigma^2(1) = \sigma(4) = 2, \sigma^3(1) = \sigma(2) = 5, \sigma^4(1) = \sigma(5) = 6, \sigma^5(1) = \sigma(6) = 3$ et $\sigma^6(1) = \sigma(3) = 1$. De plus, 7 est laissé fixe par σ

Notation Pour un cycle σ , on note en général $\sigma = (x \ \sigma(x) \ \dots \ \sigma^{n-1}(x))$.

Exemple 4

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}$ peut alors s'écrire

$$(1 \ 4 \ 2 \ 5 \ 6 \ 3) = (4 \ 2 \ 5 \ 6 \ 3 \ 1) = (2 \ 5 \ 6 \ 3 \ 1 \ 4) = (5 \ 6 \ 3 \ 1 \ 4 \ 2) .$$

Produit de cycles

Le produit de permutation est une permutation, mais le produit de cycles n'est pas un cycle, en général. Par exemple, dans S_6

$$(1 \ 4 \ 6 \ 3)(1 \ 4 \ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 5 & 3 \end{pmatrix} ,$$

qui a deux orbites non triviales $\{1, 6, 3\}$ et $\{2, 4\}$.

On remarque que la notation d'un cycle ne nous donne pas le groupe symétrique dans lequel on considère ce cycle. Le cycle $(1 \ 4 \ 6 \ 3)$ peut être dans S_6 comme dans S_{2371} .

Les transpositions

Combien y a-t-il de transpositions dans S_n ? C'est exactement la manière de choisir 2 éléments parmi n , soit $\binom{n}{2}$ transpositions.

De plus, toute transposition est involutive $\tau_{ij} \circ \tau_{ij} = Id$.

Proposition 2

Deux cycles de supports disjoints commutent.

En effet, si les supports sont disjoints les deux cycles agissent sur des ensembles disjoints, donc commutent.

Définition 4 : Conjugaison

On dit que deux permutations $\sigma, \tau \in S_n$ sont conjuguées, dans S_n , s'il existe $\rho \in S_n$ tel que

$$\sigma = \rho \circ \tau \circ \rho^{-1}.$$

Automorphismes intérieurs

Un automorphisme intérieur de S_n est une application f_π définie pour une permutation π de S_n , par

$$\begin{aligned} f_\pi : S_n &\longrightarrow S_n \\ \sigma &\longmapsto \pi \circ \sigma \circ \pi^{-1}. \end{aligned}$$

C'est donc un automorphisme de groupe, et il laisse stable les permutations qui commutent avec π .

Proposition 3

Soit $\sigma \in S_n$. Alors, pour tout $x_1, \dots, x_l \in \llbracket 1, n \rrbracket$ deux à deux distincts,

$$\sigma \circ (x_1 x_2 \dots x_l) \circ \sigma^{-1} = (\sigma(x_1) \sigma(x_2) \dots \sigma(x_l)).$$

Preuve. Calculons l'image d'un élément $\sigma(x_k)$ (avec la convention consistant à considérer les indices modulo l donc $\sigma(x_{l+1}) = \sigma(x_1)$)

$$\sigma \circ (x_1 x_2 \dots x_l) \circ \sigma^{-1} (\sigma(x_k)) = \sigma \circ (x_1 x_2 \dots x_l) (x_k) = \sigma(x_{k+1}).$$

Calculons alors l'image d'un élément $\sigma(y)$ avec $y \notin \{x_1, x_2, \dots, x_l\}$

$$\sigma \circ (x_1 x_2 \dots x_l) \circ \sigma^{-1} (\sigma(y)) = \sigma \circ (x_1 x_2 \dots x_l) (y) = \sigma(y).$$

Donc $\sigma \circ (x_1 x_2 \dots x_l) \circ \sigma^{-1}$ est bien le cycle voulu. $\square$

Exemple 5

Montrons que toutes les transpositions sont conjuguées à la transposition $(1\ 2)$.

Soit $i \neq j$. Considérons $\sigma \in S_n$ une permutation telle que $\sigma(1) = i$ et $\sigma(2) = j$. Alors,

$$\sigma \circ (12) \circ \sigma^{-1} = (ij)$$

On peut aussi le démontrer en utilisant seulement les transpositions. Supposons sans perte de généralité $j \neq 1$ et $i \neq 2$, quitte à échanger les rôles de i et j , et calculons

$$(1j) \circ (12) \circ (1j) = (j2) \quad \text{puis} \quad (2i) \circ (j2) \circ (2i) = (ij)$$

Ainsi, en combinant les deux lignes, on obtient bien la relation de conjugaison

$$(ij) = (2i) \circ (1j) \circ (12) \circ (1j) \circ (2i), \quad \text{car} \quad ((2i) \circ (1j))^{-1} = (1j) \circ (2i).$$

On peut démontrer de la même manière que deux l -cycles sont conjugués dans S_n .

3 DÉCOMPOSITION EN CYCLES DISJOINTS**Théorème 1**

Soit E un ensemble fini. Toute permutation de $S(E)$, différente de l'identité, s'écrit comme composition de cycles de supports deux à deux disjoints.

Preuve. Procédons par récurrence forte sur le cardinal de E . Pour un ensemble à 1 élément, la seule permutation est l'identité, donc le résultat est vrai.

Pour un ensemble à 2 éléments, il n'y a qu'une transposition qui est différente de l'identité, est c'est déjà un cycle.

Soit $n \geq 2$. Supposons que le résultat est vrai pour tous les ensembles de cardinal au plus n et montrons le pour un ensemble E de cardinal $n+1$ et $\sigma \in S(E)$.

Soit $x \in E$ et $\mathcal{O}(x)$ l'orbite de x pour σ . Définissons un cycle s par $s(k) = \begin{cases} k & \text{si } k \notin \mathcal{O}(x) \\ \sigma(k) & \text{sinon} \end{cases}$.

La permutation $\sigma \circ s^{-1}$ laisse stable tous les éléments de $\mathcal{O}(x)$. Le support de $\sigma \circ s^{-1}$ est inclus dans $E \setminus \mathcal{O}(x)$ donc peut être vue comme une permutation de cet ensemble, qui est de cardinal inférieur ou égal à n .

Par hypothèse de récurrence, cette permutation se décompose en une composition de cycles de supports deux à deux disjoints $\sigma \circ s^{-1} = s_1 \circ \dots \circ s_l$.

On obtient donc $\sigma = s_1 \circ \dots \circ s_l \circ s$ et les supports sont bien deux à deux disjoints. $\square$

Unicité

Cette décomposition est commutative, comme les supports des cycles sont deux à deux disjoints. Elle est unique à l'ordre près des cycles, puisque chaque cycle qui apparaît correspond à l'une des orbites de la permutation que l'on décompose.

Exemple 6

Les orbites de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 7 & 6 & 5 & 4 \end{pmatrix}$ sont $\{1, 3\}$, $\{2\}$, $\{4, 7\}$ et $\{5, 6\}$. Donc

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

Proposition 4

Soit $(x_1, \dots, x_l) \in \llbracket 1, n \rrbracket^l$. Le cycle $(x_1 x_2 \dots x_l)$ se décompose des deux manières suivantes en composition de $l - 1$ transpositions

$$(x_1 x_l) \circ (x_1 x_{l-1}) \circ \dots \circ (x_1 x_2) = (x_1 x_2) \circ (x_2 x_3) \circ \dots \circ (x_{l-1} x_l)$$

Preuve. Faites les calculs ! $\square$

⚠ ATTENTION La décomposition d'un cycle en produit de transposition **n'est évidemment pas à support disjoint**, donc n'est pas commutative en général !

Corollaire 4.1

Les transpositions engendrent le groupe S_n .

Preuve. Toute permutation peut s'écrire comme produit de cycles disjoints, qui peuvent chacun s'écrire comme produit de transpositions. $\square$

Exemple 7

En fait, on peut faire mieux. On peut montrer que la famille $\{(1k), k \in [2, n]\}$ engendre le groupe S_n .

D'après la proposition précédente, il suffit de montrer que l'on peut obtenir toute transposition, qui ne permute pas 1, à partir de cette famille. Or

$$(ij) = (1i) \circ (1j) \circ (1i)$$

pour tous $i \neq j$, ce qui montre le résultat.

Définition 5

L'ordre d'une permutation $\sigma \in S_n$ est le plus petit entier $k > 0$ tel que $\sigma^k = \text{Id}$.

Exemple 8

L'ordre d'un cycle est sa longueur. En effet, si $\sigma = (x_1 x_2 \dots x_l) \in S_n$, alors pour tout $k < l$, $\sigma^k(x_1) = x_{k+1} \neq x_1$, donc $\sigma^k \neq \text{Id}$, mais $\sigma^l = \text{Id}$.

Proposition 5

L'ordre de σ est le ppcm des ordres des cycles qui apparaissent dans sa décomposition en cycles à supports disjoints.

Preuve. Soit $\sigma \in S_n$. Notons $\sigma = c_1 \circ c_2 \circ \dots \circ c_p$, où $c_1, \dots, c_p$ sont les cycles à supports disjoints qui apparaissent dans la décomposition de σ .

Comme l'écriture est commutative, on obtient pour tout $k \in \mathbb{N}$, $\sigma^k = c_1^k \circ c_2^k \circ \dots \circ c_p^k$.

Les permutations $c_1^k, c_2^k, \dots, c_p^k$ sont encore à supports disjoints. Par conséquent, $\sigma^k = \text{Id}$ si, et seulement si, pour tout $i \leq p$, $c_i^k = \text{Id}$ soit k est un multiple de la longueur de c_i . En conclusion, l'ordre de σ est le plus petit commun multiple des longueurs des cycles c_i pour tout $i \leq p$. $\square$

Exemple 9

Dans S_7 , l'ordre de $(1\ 3)\ (4\ 7)\ (5\ 6)$ est 2 et l'ordre de $(1\ 3\ 4\ 5)\ (6\ 2\ 7)$ est $4 \vee 3 = 12$.

4 MORPHISME SIGNATURE

Définition 6

Soit $\sigma \in S_n$.

Une paire $\{i, j\}$ est une **inversion pour σ** si $(i - j)(\sigma(i) - \sigma(j)) < 0$.

On note $\text{Inv}(\sigma)$ le **nombre d'inversions de σ** .

La **signature de σ** est le réel $\varepsilon(\sigma) = (-1)^{\text{Inv}(\sigma)}$.

Visualisation du nombre d'inversions**Exemple 10**

Une permutation a toujours un nombre impair d'inversions, donc $\varepsilon(\sigma) = -1$.

Proposition 6

Pour tout $\sigma \in S_n$,

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j},$$

où la notation $\prod_{\{i,j\}}$ signifie le produit sur toutes les paires $\{i, j\}$, donc avec $i \neq j$.

Preuve. Soit $\sigma \in S_n$. Par définition des inversions, on a

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

Or, σ est une permutation de $\llbracket 1, n \rrbracket$ donc $\{\sigma(i), \sigma(j)\}$ décrit l'ensemble des paires de $\llbracket 1, n \rrbracket$ lorsque $\{i, j\}$ décrit l'ensemble des paires de $\llbracket 1, n \rrbracket$. Par conséquent, $\prod_{\{i,j\}} |\sigma(i) - \sigma(j)| = \prod_{\{i,j\}} |i - j|$, ce qui donne le résultat. $\square$

Proposition 7

L'application signature est un morphisme de groupes de S_n dans $\{-1, 1\}$, c'est-à-dire

$$\forall \sigma_1, \sigma_2 \in S_n, \quad \varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \varepsilon(\sigma_2).$$

En particulier, deux permutations σ_1, σ_2 conjuguées ont la même signature.

Preuve. Avec l'expression de la signature obtenue précédemment, pour tous $\sigma_1, \sigma_2 \in S_n$,

$$\varepsilon(\sigma_1 \circ \sigma_2) = \prod_{\{i,j\}} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{i - j} = \left[\prod_{\{i,j\}} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{\sigma_2(i) - \sigma_2(j)} \right] \cdot \left[\prod_{\{i,j\}} \frac{\sigma_2(i) - \sigma_2(j)}{i - j} \right].$$

Par ailleurs, comme σ_2 est une bijection,

$$\prod_{\{i,j\}} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{\sigma_2(i) - \sigma_2(j)} = \prod_{\{i,j\}} \frac{\sigma_1(i) - \sigma_1(j)}{i - j} = \varepsilon(\sigma_1).$$

En conclusion, $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \varepsilon(\sigma_2)$. $\square$

Proposition 8

Soit $\varphi : S_n \rightarrow \mathbb{C}^*$ un morphisme de groupes différent de l'application constante égale à 1. Alors, φ est la signature.

Preuve. Pour toute transposition τ , comme $\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(\text{Id}) = 1$, on obtient $\varphi(\tau) \in \{\pm 1\}$.

- Si $\varphi(\tau) = 1$, alors φ et la fonction constante égale à 1 coïncident sur les transpositions et toute permutation est un produit de transpositions donc $\varphi = 1$.
- Si $\varphi(\tau) = -1$, alors φ et la signature coïncident sur les transpositions et toute permutation est un produit de transpositions donc $\varphi = \varepsilon$.

$\square$

Exemple 11

Exprimons la signature d'une permutation σ de S_n en fonction de son nombre d'orbites et de n . Notons $l_1, \dots, l_r$ les longueurs des différents cycles apparaissant dans la décomposition en cycles à supports disjoints de σ . D'après la propriété de morphisme de ε ,

$$\varepsilon(\sigma) = \prod_{k=1}^r (-1)^{l_k-1} = (-1)^{\sum_{k=1}^r l_k - r}$$

Remarquons ensuite que $\sum_{k=1}^r l_k$ est la taille du support de σ donc $n - f$ où f est le nombre de points fixes de σ . Ainsi, $\varepsilon(\sigma) = (-1)^{n-r-f}$.

Pour conclure, il suffit de remarquer que $r + f$ est le nombre o d'orbites de σ et donc $\varepsilon(\sigma) = (-1)^{n+o}$.