

Groupes symétriques

1	Généralités	2
1.1	Rappels	2
1.2	Permutations particulières	3
2	Décompositions d'une permutation	4
2.1	Décomposition en produit de cycles dis- joints	4
2.2	Décomposition en produit de transpositions	6
3	Signature d'une permutation	6
3.1	Signature, groupe alterné	6
3.2	Preuve de l'existence de la signature . .	8

Compétences attendues.

- ✓ Savoir décomposer une permutation en produit de cycles à supports disjoints.
- ✓ Savoir décomposer une permutation en produit de transpositions.
- ✓ Savoir calculer la signature d'une permutation.

1 Généralités

1.1 Rappels

Propriété 1

Soit $n \geq 1$. Notons \mathfrak{S}_n l'ensemble des bijections (aussi appelées *permutations*) de $\llbracket 1, n \rrbracket$ dans lui-même. Muni de la composition des applications, (\mathfrak{S}_n, \circ) est un groupe fini d'ordre $n!$, appelé *groupe symétrique d'indice n* . Il est non commutatif pour $n \geq 3$.

Notation.

Un élément $\sigma \in \mathfrak{S}_n$ se représente communément sous forme d'un tableau à deux lignes :

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

Définition.

Soit $\sigma \in \mathfrak{S}_n$. On appelle *support de σ* , et on note $\text{Supp}(\sigma)$, l'ensemble des $k \in \llbracket 1, n \rrbracket$ qui ne sont pas fixes par σ , c'est-à-dire tels que $\sigma(k) \neq k$.

Exemple. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 4 & 3 & 5 \end{pmatrix}$ est l'élément de \mathfrak{S}_6 qui échange 1 et 2, qui envoie 3 sur 6, 4 sur lui-même, 5 sur 3 et 6 sur 5. Son support est $\text{Supp}(\sigma) = \{1, 2, 3, 5, 6\}$.

Propriété 2

Deux permutations de \mathfrak{S}_n à supports disjoints commutent.

1.2 Permutations particulières

Définition.

Soit $p \in \llbracket 2, n \rrbracket$. On appelle *cycle de longueur p* toute permutation σ de \mathfrak{S}_n pour laquelle il existe p éléments deux à deux distincts a_1, \dots, a_p de $\llbracket 1, n \rrbracket$ tels que :

- pour tout $k \in \llbracket 1, p-1 \rrbracket$, $\sigma(a_k) = a_{k+1}$ et $\sigma(a_p) = a_1$;
- pour tout $i \notin \{a_1, \dots, a_p\}$, $\sigma(i) = i$.

Notation.

Avec les notations introduites dans la définition précédente, on écrit plus simplement le cycle σ sous la forme :

$$\sigma = (a_1 \ a_2 \ \cdots \ a_p).$$

Notons qu'une telle écriture de σ n'est pas unique.

Exemples.

- La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ est en fait le 3-cycle $(1 \ 2 \ 4)$, qui peut aussi être écrit $(2 \ 4 \ 1)$ ou $(4 \ 1 \ 2)$.
- La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ n'est pas un cycle : il s'agit de la composée $(1 \ 2) \circ (3 \ 4)$ de deux 2-cycles.

Remarque. Soit $\sigma = (a_1 \ a_2 \ \dots \ a_p)$ un p -cycle de \mathfrak{S}_n . Alors :

- le support de σ est $\text{Supp}(\sigma) = \{a_1, \dots, a_p\}$;
- σ est un élément d'ordre p de \mathfrak{S}_n , c'est-à-dire :

$$\sigma^p = \text{id}_{\llbracket 1, n \rrbracket} \text{ et pour tout } k \in \llbracket 1, p-1 \rrbracket, \sigma^k \neq \text{id}.$$

En particulier, on notera que σ est bien bijective (c'est bien un élément de \mathfrak{S}_n), d'inverse $\sigma^{-1} = \sigma^{p-1} = (a_p \ a_{p-1} \ \dots \ a_1)$ qui est aussi un p -cycle.

Définition.

On appelle *transposition* de \mathfrak{S}_n tout cycle de longueur 2, c'est-à-dire toute permutation de la forme $\tau = (i \ j)$ qui échange des éléments i et j et laisse fixe les autres éléments.

Remarques.

- Une transposition de \mathfrak{S}_n est une permutation qui possède exactement $n - 2$ points fixes.
- Une transposition τ est un élément d'ordre 2 de \mathfrak{S}_n , et $\tau^{-1} = \tau$.

Exercice 1. Décrire les éléments de \mathfrak{S}_2 et \mathfrak{S}_3 , et écrire la table de ses groupes.

2 Décompositions d'une permutation

2.1 Décomposition en produit de cycles disjoints

Théorème 3 (Décomposition en produit de cycles à supports disjoints)

Toute permutation de \mathfrak{S}_n se décompose en produit de cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre près des facteurs.

Preuve. La preuve qui suit n'est pas exigible en MP2I. Vous pouvez la passer en première lecture. On présente ici les principales étapes de la démonstration, les détails sont laissés en exercices.

Existence de la décomposition. Soit $\sigma \in \mathfrak{S}_n$ une permutation.

- On définit sur l'ensemble $\llbracket 1, n \rrbracket$ la relation binaire \mathcal{R}_σ par :

$$i \mathcal{R}_\sigma j \Leftrightarrow \exists k \in \mathbb{Z}, j = \sigma^k(i).$$

On vérifie que \mathcal{R}_σ est une relation d'équivalence, de sorte que ses classes d'équivalence (qu'on appelle aussi *orbites* dans ce contexte) forment une partition de $\llbracket 1, n \rrbracket$. On notera dans la suite $\mathcal{O}_1, \dots, \mathcal{O}_p$ les orbites distinctes de cardinal plus grand que 2.

- Soit \mathcal{O} une orbite, et $x \in \llbracket 1, n \rrbracket$ un représentant de \mathcal{O} . Alors :

$$\mathcal{O} = \{j \in \llbracket 1, n \rrbracket \mid \exists k \in \mathbb{Z}, j = \sigma^k(x)\} = \{\sigma^k(x), k \in \mathbb{Z}\}.$$

Puisque \mathcal{O} est fini, il existe $p < q$ tels que $\sigma^p(x) = \sigma^q(x)$, et alors $\sigma^{q-p}(x) = x$. L'ensemble $\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\}$ est donc non vide, et admet un plus petit élément s .

Soit $k \in \mathbb{Z}$, et $k = qs + r$ la division euclidienne de k par s avec $0 \leq r < s$. Alors :

$$\sigma^k(x) = \sigma^r \circ (\sigma^s)^q(x) = \sigma^r(x).$$

Donc $\mathcal{O} = \{\sigma^i(x), 0 \leq i < s\}$. Et ces éléments sont deux à deux distincts : en effet, si i et j sont deux éléments de $\llbracket 0, s-1 \rrbracket$ tels que $i \leq j$ et $\sigma^i(x) = \sigma^j(x)$, alors $x = \sigma^{j-i}(x)$ avec $0 \leq j-i < s$, soit encore $i = j$ par définition de s .

On note, pour tout $i \in \llbracket 0, s-1 \rrbracket$, $x_i = \sigma^i(x)$, de sorte que $\mathcal{O} = \{x_0, x_1, \dots, x_{s-1}\}$. On lui associe le s -cycle $c = (x_0 \ x_1 \ \dots \ x_{s-1})$. Par définition des éléments x_0, \dots, x_{s-1} , $\sigma(x_i) = c(x_i)$ et σ et c coïncident sur \mathcal{O} .

- On associe ainsi à chacune des orbites $\mathcal{O}_1, \dots, \mathcal{O}_p$ un cycle c_1, \dots, c_p . Pour tout $x \in \llbracket 1, n \rrbracket$:

- soit $x \notin \bigcup_{i=1}^p \mathcal{O}_i$: dans ce cas, x est un point fixe pour σ et aussi pour chacun des c_i . Et donc $\sigma(x) = c_1 \circ \dots \circ c_p(x)$.
- soit il existe $1 \leq i \leq p$ tel que $x \in \mathcal{O}_i$: dans ce cas, x et $c_i(x)$ sont des points fixes pour les cycles c_j pour $j \neq i$, de sorte que $c_1 \circ \dots \circ c_p(x) = c_i(x) = \sigma(x)$ car c_i et σ coïncident sur \mathcal{O}_i .

Dans tous les cas, $\sigma(x) = c_1 \circ \dots \circ c_p(x)$, et donc $\sigma = c_1 \circ \dots \circ c_p$.

Unicité de la décomposition. Supposons que $c_1 \circ \dots \circ c_p = c'_1 \circ \dots \circ c'_q$ où les c_i (resp. c'_i) sont des cycles à supports disjoints.

- On remarque que les orbites de cardinal plus grand que 2 sous l'action de $c_1 \circ \dots \circ c_p$ sont $\text{Supp}(c_1), \dots, \text{Supp}(c_p)$. Puisque la même remarque vaut pour $c'_1 \circ \dots \circ c'_q$, il suit que $p = q$. Et quitte à renuméroter les cycles, on peut supposer que $\text{Supp}(c_i) = \text{Supp}(c'_i)$ pour tout $1 \leq i \leq p$.
- Soit $i \in \llbracket 1, p \rrbracket$, et considérons $x \in \text{Supp}(c_i) = \text{Supp}(c'_i)$. Alors $c_i(x)$ et $c'_i(x)$ appartiennent aussi à $\text{Supp}(c_i) = \text{Supp}(c'_i)$. En particulier, x , $c_i(x)$ et $c'_i(x)$ n'appartiennent pas à $\text{Supp}(c_j) = \text{Supp}(c'_j)$ pour $j \neq i$. Ainsi :

$$c_i(x) = c_1 \circ \dots \circ c_p(x) = c'_1 \circ \dots \circ c'_p(x) = c'_i(x).$$

Les cycles c_i et c'_i coïncident sur $\text{Supp}(c_i) = \text{Supp}(c'_i)$, et sont donc égaux. D'où l'unicité de la décomposition.

□

Exercice 2. Décomposer en produit de cycles à supports disjoints les permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$ et $\sigma' = (1 \ 3 \ 7 \ 5) \circ (2 \ 5 \ 4) \circ (2 \ 8 \ 4 \ 3)$.

2.2 Décomposition en produit de transpositions

Propriété 4

Soit $\sigma = (a_1 \ a_2 \ \cdots \ a_p)$ un p -cycle de \mathfrak{S}_n . Alors :

$$\sigma = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \cdots \circ (a_{p-2} \ a_{p-1}) \circ (a_{p-1} \ a_p).$$

Théorème 5 (Décomposition en produit de transpositions)

Toute permutation se décompose en produit de transpositions.

Mise en garde.

Il n'y a pas unicité de la décomposition d'une permutation en produit de transpositions. Par exemple :

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

De plus, les transpositions apparaissant dans une telle décomposition ne commutent pas en général.



Pour aller plus loin.

Une conséquence immédiate est que le sous-groupe de \mathfrak{S}_n engendré par l'ensemble des transpositions est \mathfrak{S}_n tout entier. On dit alors que l'ensemble des transpositions *engendre* le groupe \mathfrak{S}_n , ou encore que les transpositions constituent un *système de générateurs* du groupe \mathfrak{S}_n .

Exercice 3. Décomposer en produit de transpositions la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$.

3 Signature d'une permutation

3.1 Signature, groupe alterné

Commençons par donner le résultat principal de cette section.

Théorème 6

Il existe un unique morphisme de groupes $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$ envoyant toute transposition sur -1 .

Définition.

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

- On appelle *signature* de σ l'élément $\varepsilon(\sigma) \in \{-1, 1\}$.
- On dit que σ est *paire* si $\varepsilon(\sigma) = 1$, *impaire* si $\varepsilon(\sigma) = -1$.

Propriété 7 (Calcul de la signature d'une permutation)

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

- (1) Si σ s'écrit comme un produit $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$ de k transpositions, alors $\varepsilon(\sigma) = (-1)^k$.
- (2) Si σ est un p -cycle, alors $\varepsilon(\sigma) = (-1)^{p-1}$.

Conséquence. Toutes les décompositions de σ en produit de transpositions font apparaître un nombre de transpositions dont la parité ne dépend que de σ .

Exercice 4. Déterminer la signature des permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$ et $\sigma' = (1 \ 3 \ 7 \ 5) \circ (2 \ 5 \ 4) \circ (2 \ 8 \ 4 \ 3)$.

Définition.

On appelle *groupe alterné d'ordre n* , et on note \mathfrak{A}_n , le noyau de la signature $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$, c'est-à-dire l'ensemble des permutations paires.

Propriété 8

Le groupe alterné \mathfrak{A}_n est un sous-groupe de \mathfrak{S}_n d'ordre $\frac{n!}{2}$.

Le saviez-vous ?

Un résultat remarquable est que le groupe alterné \mathfrak{A}_n est « simple^a » si, et seulement si, $n = 1, 2$ ou $n \geq 5$. Ce résultat a pour conséquence importante le théorème d'Abel, stipulant qu'il ne peut exister d'expression générique par radicaux des solutions d'une équation algébrique de degré supérieur ou égal à 5.

^aLe terme *simple* signifie que de tels groupes ne sont pas « réductibles à un groupe plus maniable ». Les groupes simples finis peuvent être perçus comme les briques de base de tous les groupes finis, et jouent en ce sens un rôle analogue à celui des nombres premiers pour les nombres entiers.



Niels Henrik Abel (1802-1829)

3.2 Preuve de l'existence de la signature

Nous prouvons dans cette section l'existence du morphisme signature, l'unicité sera démontrée en TD. La preuve qui suit n'est pas exigible en MP2I, je la donne tout de même pour la complétude du cours, mais vous pouvez la passer en première lecture.

Définition.

Soit $\sigma \in \mathfrak{S}_n$. On appelle *signature* de σ , et on note $\varepsilon(\sigma)$, le produit :

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

Astuce.

Puisque pour tous $1 \leq i < j \leq n$:

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

l'ordre dans le couple (i, j) n'a pas d'importance, de sorte que le produit précédent peut se récrire :

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} \frac{\sigma(j) - \sigma(i)}{j - i}$$

où $\mathcal{P}_2(\llbracket 1, n \rrbracket)$ est l'ensemble des paires $\{i, j\}$ avec $i \neq j$ (et pas des couples, une paire n'est pas ordonnée).

Propriété 9

- (1) Pour tout $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) \in \{-1, 1\}$.
- (2) Soit $\tau \in \mathfrak{S}_n$ une transposition. Alors $\varepsilon(\tau) = -1$.

Preuve.

- (1) Puisque σ est bijective, l'application $\{i, j\} \mapsto \{\sigma(i), \sigma(j)\}$ réalise une bijection de $\mathcal{P}_2(\llbracket 1, n \rrbracket)$ sur lui-même. Et donc toute paire $\{k, \ell\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)$ s'écrit de manière unique $\{\sigma(i), \sigma(j)\}$ avec $\{i, j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)$. Ainsi, $\prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |\sigma(i) - \sigma(j)| = \prod_{\{k,\ell\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |k - \ell|$. Et par conséquent :

$$|\varepsilon(\sigma)| = \frac{\prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |\sigma(i) - \sigma(j)|}{\prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |i - j|} = \frac{\prod_{\{k,\ell\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |k - \ell|}{\prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} |i - j|} = 1.$$

Donc ε est à valeurs dans $\{-1, 1\}$.

- (2) Soit $\tau = \begin{pmatrix} k & \ell \\ \ell & k \end{pmatrix}$ une transposition, avec $k < \ell$. Si i et j n'appartiennent pas à $\{k, \ell\}$, alors $\frac{\tau(i) - \tau(j)}{i - j} = \frac{i - j}{i - j} = 1$. Ainsi, dans le produit définissant $\varepsilon(\tau)$ ne restent que les termes où l'un au moins des deux

nombres i, j est dans $\{k, \ell\}$, ce qui donne :

$$\varepsilon(\tau) = \left(\prod_{\substack{i=1 \\ i \neq k, i \neq \ell}}^n \frac{\tau(k) - \tau(i)}{k - i} \times \frac{\tau(\ell) - \tau(i)}{\ell - i} \right) \times \frac{\tau(k) - \tau(\ell)}{k - \ell} = \left(\prod_{\substack{i=1 \\ i \neq k, i \neq \ell}}^n \frac{\ell - i}{k - i} \times \frac{k - i}{\ell - i} \right) \times \frac{\ell - k}{k - \ell} = -1.$$

□

Remarque. On appelle *inversion* d'une permutation σ toute paire $\{i, j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)$ où $\sigma(j) - \sigma(i)$ est de signe opposé à $j - i$. Le résultat précédent montre que la signature $\varepsilon(\sigma)$ de σ est égale à 1 ou -1 selon que le nombre d'inversions de σ soit pair ou impair.

Propriété 10

L'application $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$ est un morphisme de groupes.

Preuve. Pour $\sigma, \sigma' \in \mathfrak{S}_n$:


$$\frac{\varepsilon(\sigma\sigma')}{\varepsilon(\sigma')} = \prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} \frac{\sigma(\sigma'(i)) - \sigma(\sigma'(j))}{i - j} \times \prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} \frac{i - j}{\sigma'(i) - \sigma'(j)} = \prod_{\{i,j\} \in \mathcal{P}_2(\llbracket 1, n \rrbracket)} \frac{\sigma(\sigma'(i)) - \sigma(\sigma'(j))}{\sigma'(i) - \sigma'(j)}.$$

Mais comme mentionné précédemment, $\{i, j\} \mapsto \{\sigma'(i), \sigma'(j)\}$ réalise une bijection de $\mathcal{P}_2(\llbracket 1, n \rrbracket)$ sur lui-même. Donc :

$$\frac{\varepsilon(\sigma\sigma')}{\varepsilon(\sigma')} = \prod_{\{k,\ell\} \in \mathcal{A}} \frac{\sigma(k) - \sigma(\ell)}{k - \ell} = \varepsilon(\sigma).$$

Et donc comme annoncé, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$. □

Liens utiles.

 [Futurama](#), Deux (deux ?) minutes pour... , El Jj.