Le groupe symétrique

Plan du chapitre

1 Le groupe symétrique

1.1 Groupe des permutations d'un ensemble

• On rappelle que si E est un ensemble non vide, une **permutation** de E est une bijection de E sur E et que si l'on note $S(E)$ l'ensemble des permutations de E, alors $(S(E), \circ)$ est un groupe.

• Id_E est une permutation de E. La composée de deux permutations de E est une permutation de E. La réciproque d'une permutation de E est une permutation de E. De plus, $\forall (\sigma, \sigma') \in (S(E))^2$, $(\sigma \circ \sigma')^{-1} = \sigma'^1 \circ \sigma^{-1}$ et $\left(\sigma^{-1}\right)^{-1} = \sigma$.

• On démontrera dans le chapitre « Dénombrement » que si E est un ensemble fini non vide ayant n éléments, il y a un nombre fini de permutations de E et ce nombre de permutations est $n!$. On peut admettre momentanément ce résultat.

1.2 Le groupe symétrique

On se place maintenant dans le cas particulier où $E = [\![1, n]\!]$, n étant un entier naturel non nul donné. Dans ce cas, l'ensemble $S(E)$ se note S_n (S_n est donc l'ensemble des permutations de l'ensemble $[\![1, n]\!]$. On peut énoncer

Théorème 1. $(S_n, \circ)$ est un groupe fini de cardinal $n!$.

Une permutation donnée de $[\![1, n]\!]$ se note $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ ou plus simplement $\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.
Ainsi, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$ ou plus simplement $\sigma = \begin{pmatrix} 4 & 1 & 3 & 5 & 2 \end{pmatrix}$ est la permutation de $[\![1, 5]\!]$ définie par : $\sigma(1) = 4$, $\sigma(2) = 1$, $\sigma(3) = 3$, $\sigma(4) = 5$ et $\sigma(5) = 2$.
Pour composer deux permutations σ et σ', nous écrirons $\sigma \circ \sigma' = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} \sigma'(1) & \sigma'(2) & \dots & \sigma'(n) \end{pmatrix}$.
Ainsi, la deuxième permutation écrite est la première effectuée et la composée (ou le produit) de permutations se lit de droite à gauche. Par exemple, si $\sigma = \begin{pmatrix} 4 & 1 & 3 & 2 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 2 & 3 & 4 & 1 \end{pmatrix}$,

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

car par exemple, $\sigma \circ \sigma'(1) = \sigma(\sigma'(1)) = \sigma(2) = 1$.

• $S_1 = S([\![1, 1]\!])$ est un singleton : $S_1 = \left\{Id_{\{1\}}\right\}$.

• $S_2 = S([\![1, 2]\!])$ est constitué de deux éléments : l'identité et la permutation $\begin{pmatrix} 2 & 1 \end{pmatrix}$. La permutation $\begin{pmatrix} 2 & 1 \end{pmatrix}$ échange de position les deux éléments 1 et 2 et est appelée la **transposition** $\begin{pmatrix} 2 & 1 \end{pmatrix}$. Elle se note $\tau_{1,2}$ (ou aussi $\tau_{2,1}$). les transpositions seront étudiées à la section suivante.
Ainsi, $S_2 = \left\{Id_{\{1,2\}}, \tau_{1,2}\right\}$ ou plus simplement $S_2 = \{Id, \tau_{1,2}\}$. On peut donner la « table de Pythagore » du groupe $(S_2, \circ)$:

$\circ$	Id	$\tau_{1,2}$
Id	Id	$\tau_{1,2}$
$\tau_{1,2}$	$\tau_{1,2}$	Id

Ligne 3, colonne 2, du tableau, on a écrit la composée de la permutation $\sigma = \tau_{1,2}$ écrite dans la ligne 3, colonne 1, par la permutation $\sigma' = Id$ écrite à la ligne 1, colonne 2 ou encore ligne 3, colonne 2, du tableau, on a écrit $\sigma \circ \sigma' = \tau_{1,2} \circ Id = \tau_{1,2}$.

On note que le groupe $(S_2, \circ)$ est un groupe commutatif.

• $S_3 = S([\![1, 3]\!])$ est constitué de six éléments. Il y a déjà l'identité et les trois transpositions $\tau_{1,2}$, $\tau_{1,3}$ et $\tau_{2,3}$. Il faut ajouter les deux **permutations circulaires** $c_1 = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix}$ et $c_2 = \begin{pmatrix} 3 & 1 & 2 \end{pmatrix}$. Les permutations circulaires seront étudiées plus loin.
Ainsi, $S_3 = \{Id, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c_1, c_2\}$. Pour dresser la table de Pythagore du groupe $(S_3, \circ)$, ce qui nécessite à priori $6 \times 6 = 36$ calculs, un petit nombre de calculs explicites sont suffisants pour remplir cette table.

- Déjà, Id est élément neutre ce qui permet déjà de remplir 11 cases.

- La réciproque d'une transposition est elle même et d'autre part, $c_2 = (c_1)^{-1}$ se qui permet de remplir 5 cases de plus.

- Ensuite, dans une ligne donnée (ou une colonne donnée) un même élément de S_3 ne peut se répéter deux fois car $\sigma \circ \sigma' = \sigma \circ \sigma'' \Rightarrow \sigma' = \sigma''$ (ou $\sigma' \circ \sigma = \sigma'' \circ \sigma \Rightarrow \sigma' = \sigma''$). Dans une ligne d'une permutation σ du tableau (ou dans une colonne), on retrouve donc une fois et une seule chaque élément de S_3. On dit que la table du groupe fini $(S_3, \circ)$ est un « carré latin ».

- Il ne reste donc à calculer explicitement que deux produits de deux transpositions distinctes et deux produits d'une

transposition par une permutation circulaire.

$\tau_{1,2} \circ \tau_{1,3} = \begin{pmatrix} 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \end{pmatrix} = c_2$,

$\tau_{1,3} \circ \tau_{1,2} = \begin{pmatrix} 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix} = c_1$,

en composant à gauche par $\tau_{1,2}$, on obtient $\tau_{1,2} \circ \tau_{1,3} = c_2 \Rightarrow \tau_{1,2} \circ c_2 = \tau_{1,3}$ et en composant à droite par $\tau_{1,3}$, on obtient $c_2 \circ \tau_{1,3} = \tau_{1,2}$. Tout le reste s'en déduit.

$\circlearrowright_{\circ}$	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	c_1	c_2
Id	Id	$\tau_{1,2}$	$\tau_{1,3}$	$\tau_{2,3}$	c_1	c_2
$\tau_{1,2}$	$\tau_{1,2}$	Id	c_2	c_1	$\tau_{2,3}$	$\tau_{1,3}$
$\tau_{1,3}$	$\tau_{1,3}$	c_1	Id	c_2	$\tau_{1,2}$	$\tau_{2,3}$
$\tau_{2,3}$	$\tau_{2,3}$	c_2	c_1	Id	$\tau_{1,3}$	$\tau_{1,2}$
c_1	c_1	$\tau_{1,3}$	$\tau_{2,3}$	$\tau_{1,2}$	c_2	Id
c_2	c_2	$\tau_{2,3}$	$\tau_{1,2}$	$\tau_{1,3}$	Id	c_1

On note que le groupe $(S_3, \circ)$ n'est pas commutatif. De manière générale, si $n \geqslant 3$, le groupe $(S_n, \circ)$ n'est pas commutatif. En effet, $\tau_{1,2} \circ \tau_{1,3} = \begin{pmatrix} 2 & 1 & 3 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 3 & 2 & 1 & 4 \dots & n \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 & 4 & \dots & n \end{pmatrix}$ et $\tau_{1,3} \circ \tau_{1,2} = \begin{pmatrix} 3 & 2 & 1 & 4 & \dots & n \end{pmatrix} \circ \begin{pmatrix} 2 & 1 & 3 & 4 \dots & n \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}$. Donc, $\tau_{1,2} \circ \tau_{1,3} \neq \tau_{1,3} \circ \tau_{1,2}$.

2 Décomposition d'une permutation en produit de transpositions

2.1 Transpositions

DÉFINITION 1. Soit $n \geqslant 2$. Une transposition de $[\![1, n]\!]$ est une permutation de $[\![1, n]\!]$ qui échange deux éléments distincts de $[\![1, n]\!]$ en fixant les autres éléments de $[\![1, n]\!]$.

Soit $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$. La transposition qui échange i et j se note $\tau_{i,j}$. Elle est définie par :

$$\tau_{i,j}(i) = j,\ \tau_{i,j}(j) = i \text{ et } \forall k \notin \{i, j\},\ \tau_{i,j}(k) = k.$$

Un premier résultat immédiat est :

Théorème 1. Soit $n \geqslant 2$. Pour toute transposition τ de $[\![1, n]\!]$, $\tau \circ \tau = \mathrm{Id}_{[\![1,n]\!]}$ ou encore $\tau^{-1} = \tau$.

2.2 Décomposition d'une permutation en produit de transpositions

Le principal intérêt des transpositions est que toute permutation est une composée de transpositions. On peut parvenir à une permutation quelconque donnée par échanges de position successifs de deux éléments :

Théorème 2. Soit $n \geqslant 2$. Toute permutation σ de $[\![1, n]\!]$ peut s'écrire comme un produit de transpositions.

DÉMONSTRATION .

On montre le résultat par récurrence.

- $S_2 = \{\mathrm{Id}, \tau_{1,2}\}$. $\mathrm{Id} = \tau_{1,2} \circ \tau_{1,2}$ et $\tau_{1,2}$ est une transposition et donc un produit de une transposition.
- Soit $n \geqslant 2$. Supposons le résultat pour n. Soit $\sigma \in S_{n+1}$.
  - Si $\sigma(n+1) = n+1$, la restriction de σ à $[\![1, n]\!]$ réalise une permutation de $[\![1, n]\!]$ que l'on note $\widetilde{\sigma}$. Vérifions le. L'image par $\widetilde{\sigma}$ d'un élément de $[\![1, n]\!]$ est un élément de $[\![1, n+1]\!]$ qui n'est pas $n+1$. Donc, $\widetilde{\sigma}$ est bien une application de $[\![1, n]\!]$ dans lui-même. $\widetilde{\sigma}$ est injective car σ l'est. Enfin, tout élément de $[\![1, n]\!]$ a un antécédent par σ dans $[\![1, n+1]\!]$ qui n'est pas $n+1$ ou encore tout élément de $[\![1, n]\!]$ a un antécédent par $\widetilde{\sigma}$ dans $[\![1, n]\!]$ et $\widetilde{\sigma}$ est surjective. Finalement, $\widetilde{\sigma}$ est une permutation de $[\![1, n]\!]$.

    Par hypothèse de récurrence, $\widetilde{\sigma}$ est un produit de transpositions $\widetilde{\tau_1}$, ..., $\widetilde{\tau_k}$ de $[\![1, n]\!]$. On prolonge ces transpositions à $[\![1, n+1]\!]$ en posant pour tout $i \in [\![1, k]\!]$, $\tau_i(n+1) = n+1$ et on obtient des transpositions τ_1, ..., τ_k de $[\![1, n+1]\!]$ telles que $\sigma = \tau_1 \circ \dots \circ \tau_k$.
  - Si $\sigma(n+1) \neq n+1$, soit $i = \sigma(n+1) \in [\![1, n]\!]$ puis $\sigma' = \tau_{i,n+1} \circ \sigma$. σ' est une permutation de $[\![1, n+1]\!]$ qui fixe $n+1$. D'après le cas précédent, il existe des transpositions τ_1, ...,τ_k telles que $\tau_{i,n+1} \circ \sigma = \sigma' = \tau_1 \circ \dots \tau_k$. Mais alors, $\sigma = \tau_{i,n+1} \circ \tau_1 \circ \dots \tau_k$.

Le résultat est démontré par récurrence.

❑

La démonstration précédente fournit une démarche pratique pour décomposer une permutation en produit de transpositions. On fixe petit à petit les éléments de $[\![1,n]\!]$, en commençant par n puis en descendant, en composant à gauche par des transpositions.

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

• $\sigma(7) = 4$ et donc $\tau_{4,7} \circ \sigma(7) = \tau_{4,7}(4) = 7$.

Plus précisément, $\tau_{4,7} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 7 & 5 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 4 & 6 & 3 & 7 \end{pmatrix}$.

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

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

Ainsi, $\tau_{3,5} \circ \tau_{3,6} \circ \tau_{4,7} \circ \sigma = \tau_{1,3}$. On en déduit que $\tau_{4,7} \circ \tau_{3,6} \circ \tau_{3,5} \circ \tau_{3,5} \circ \tau_{3,6} \circ \tau_{4,7} \circ \sigma = \tau_{4,7} \circ \tau_{3,6} \circ \tau_{3,5} \circ \tau_{1,3}$ et donc

$$\sigma = \tau_{4,7} \circ \tau_{3,6} \circ \tau_{3,5} \circ \tau_{1,3}.$$

3 Signature d'une permutation

3.1 Définition de la signature

DÉFINITION 2. Soient $n \geqslant 2$ puis $\sigma \in S_n$.

La **signature** de σ est $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \dfrac{\sigma(i) - \sigma(j)}{i - j}$.

Convention. Si $n = 1$, $S_1 = \{Id_{\{1\}}\}$ et on pose $\varepsilon(Id_{\{1\}}) = 1$.

Exemple. si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, alors

$$\begin{aligned} \varepsilon(\sigma) &= \frac{2-4}{1-2} \times \frac{2-3}{1-3} \times \frac{2-1}{1-4} \times \frac{4-3}{2-3} \times \frac{4-1}{2-4} \times \frac{3-1}{3-4} \\ &= (-1)^4 \frac{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)}{(1-2)(1-3)(1-4)(2-3)(2-4)(3-4)} \\ &= 1. \end{aligned}$$

3.2 Inversions d'une permutation. Calcul de la signature

DÉFINITION 3. Soient $n \geqslant 2$ puis $\sigma \in S_n$.

Une **inversion** de σ est une paire $\{i,j\}$ d'éléments de $[\![1,n]\!]$ telle que $i < j$ et $\sigma(i) > \sigma(j)$.

Exemple. si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, alors σ a 4 inversions, les paires $\{1,4\}$, $\{2,3\}$, $\{2,4\}$ et $\{3,4\}$. Pour obtenir rapidement ces inversions, on a regardé les nombres de la deuxième ligne en commençant par la gauche. $2 = \sigma(1)$ est strictement plus petit que $4 = \sigma(2)$ et $3 = \sigma(3)$ et donc les paires $\{1,2\}$ et $\{1,3\}$ ne sont pas des inversions. Par contre, $2 > 1 = \sigma(4)$ et $\{1,4\}$ est une inversion de σ. Puis on passe à $4 = \sigma(2)$ en regardant toujours à droite. $\sigma(2) = 4 > 3 = \sigma(3)$ et donc $\{2,4\}$ est une inversion ...

Théorème 3. Soient $n \geqslant 2$ puis $\sigma \in S_n$.

La signature de σ est : $\varepsilon(\sigma) = (-1)^N$ où N est le nombre d'inversions de σ.

DÉMONSTRATION. Soient $n \geqslant 2$ puis $\sigma \in S_n$. Soit N le nombre d'inversions de σ.

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

Dans le produit du numérateur, si $\{i,j\}$ n'est pas une inversion de σ, $(\sigma(i)-\sigma(j))$ s'écrit $k-l$ où $1\leqslant k<l\leqslant n$ et si $\{i,j\}$ est une inversion de σ, $(\sigma(i)-\sigma(j))$ s'écrit $-(k-l)$ où $1\leqslant k<l\leqslant n$. D'autre part, chaque paire $\{k,l\}$, où $1\leqslant k<l\leqslant n$, apparaît une fois et une seule. Donc,

$$\varepsilon(\sigma)=(-1)^N\frac{\prod_{1\leqslant k<l\leqslant n}(k-l)}{\prod_{1\leqslant i<j\leqslant n}(i-j)}=(-1)^N.$$

❑

3.3 Signature d'une transposition.

Théorème 4. La signature d'une transposition est -1

Démonstration. Il s'agit de compter le nombre d'inversions d'une transposition. Soient $(i,j)\in[\![1,n]\!]^2$ tel que $i<j$ puis $\tau=\tau_{i,j}$.

- Une paire $\{k,l\}$ telle que $1\leqslant k<l\leqslant n$ et $\{k,l\}\cap\{i,j\}=\varnothing$ n'est pas une inversion de τ car $\tau(k)=k<l=\tau(l)$.
- La paire $\{i,j\}$ est une inversion de σ car $\tau(i)=j>i=\tau(j)$.
- Il reste à analyser les paires $\{i,k\}$ où $k\notin\{i,j\}$ et les paires $\{j,k\}$ où $k\notin\{i,j\}$.

Si $k<i$, alors $\tau(k)=k<i<j=\tau(i)$. Une paire $\{k,i\}$ telle que $k<i$ n'est pas une inversion de τ.
Si $k>j$, alors $\tau(k)=k>j=\tau(i)$. Une paire $\{k,i\}$ telle que $k>j$ n'est pas une inversion de τ.
Si $i<k<j$, $\tau(i)=j>k=\tau(k)$. Une paire $\{k,i\}$ telle que $i<j<k$ est une inversion de τ.
Au total, il y a $j-1-i$ paires $\{i,k\}$ telles que $k\notin\{i,j\}$ qui sont des inversions de τ (y compris si $j=i+1$).

De même, il il y a $j-1-i$ paires $\{j,k\}$ telles que $k\notin\{i,j\}$ qui sont des inversions de τ.

Au total, le nombre d'inversions de τ est $N=2(i-j-1)+1$. En particulier, τ admet un nombre impair d'inversions et donc $\varepsilon(\tau)=(-1)^N=-1$.

❑

3.4 Permutations paires, permutations impaires

Théorème 5. Soit $n\geqslant 2$.

$\forall(\sigma,\sigma')\in(S_n)^2,\ \varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\times\varepsilon(\sigma')$.

Démonstration. Soient $n\geqslant 2$ puis $(\sigma,\sigma')\in(S_n)^2$.

$$\begin{aligned}\varepsilon(\sigma\circ\sigma')&=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{i-j}=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{\sigma'(i)-\sigma'(j)}\prod_{1\leqslant i<j\leqslant n}\frac{\sigma'(i)-\sigma'(j)}{i-j}\\&=\varepsilon(\sigma')\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{\sigma'(i)-\sigma'(j)}.\end{aligned}$$

Chaque rapport $\frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{\sigma'(i)-\sigma'(j)}$, $1\leqslant i<j\leqslant n$, est du type $\frac{\sigma(k)-\sigma(l)}{k-l}$ avec $k\neq l$. Quite à multiplier par -1 le numérateur et le dénominateur de cette fraction, on peut de plus supposer que $k<l$. Puisque σ' est une permutation de $[\![1,n]\!]$, chaque rapport $\frac{\sigma(k)-\sigma(l)}{k-l}$, $1\leqslant k<l\leqslant n$, apparaît une fois et une seule dans le produit. Donc,

$$\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(\sigma'(i))-\sigma(\sigma'(j))}{\sigma'(i)-\sigma'(j)}=\prod_{1\leqslant k<l\leqslant n}\frac{\sigma(k)-\sigma(l)}{k-l}=\varepsilon(\sigma),$$

et finalement, $\varepsilon(\sigma\circ\sigma')=\varepsilon(\sigma)\times\varepsilon(\sigma')$.

❑

Théorème 6. Soient $n\in\mathbb{N}^*$ puis $\sigma\in S_n$.

Si $\sigma=\tau_1\circ\ldots\circ\tau_k$, $k\in\mathbb{N}^*$, alors $\varepsilon(\sigma)=(-1)^k$.
La décomposition de σ en produit de transpositions n'est pas unique mais la parité du nombre de transpositions utilisé est uniquement définie par σ.

Démonstration. Soient $n\in\mathbb{N}^*$ puis $\sigma\in S_n$. D'après le théorème 2, σ se décompose en un produit de transpositions. Posons

donc $\sigma = \tau_1 \circ \ldots \circ \tau_k$ où les τ_i, $1 \leqslant i \leqslant k$, sont des transpositions.

D'après les théorèmes 4 et 5, $\varepsilon(\sigma) = \varepsilon(\tau_1 \circ \ldots \circ \tau_k) = \prod_{i=1}^{k} \varepsilon(\tau_i) = (-1)^k$.

De plus, si $\sigma = \tau'_1 \circ \ldots \circ \tau'_l$ où les τ'_j, $1 \leqslant j \leqslant l$, sont des transpositions, alors $\varepsilon(\sigma) = (-1)^l$. Puisque $(-1)^k = (-1)^l$, k et l ont même parité.

❑

DÉFINITION 4. Soit $n \geqslant 1$.

Une permutation **paire** (resp. **impaire**) est une permutation de signature 1 (resp. -1).
L'ensemble des permutations paires se note $\mathcal{A}_n$.

Une permutation paire (resp. impaire) est donc une permutation ayant un nombre pair (resp. impair) d'inversions ou aussi une permutation se décomposant en un produit d'un nombre pair (resp. impair) de transpositions.

Théorème 7. $\forall n \geqslant 2$, $\text{card}(\mathcal{A}_n) = \text{card}(S_n \setminus \mathcal{A}_n) = \dfrac{n!}{2}$.

DÉMONSTRATION. Soit τ une transposition fixée de $[\![1, n]\!]$ (τ existe puisque $n \geqslant 2$). Soient $\varphi : \begin{array}{ccc} \mathcal{A}_n & \to & S_n \setminus \mathcal{A}_n \\ \sigma & \mapsto & \tau \circ \sigma \end{array}$ et

$\psi : \begin{array}{ccc} S_n \setminus \mathcal{A}_n & \to & \mathcal{A}_n \\ \sigma & \mapsto & \tau \circ \sigma \end{array}$.

• Si $\sigma \in \mathcal{A}_n$, alors $\varepsilon(\varphi(\sigma)) = \varepsilon(\tau \circ \sigma) = \varepsilon(\tau) \times \varepsilon(\sigma) = (-1) \times 1 = -1$ et donc $\varphi(\sigma) \in S - n \setminus \mathcal{A}_n$. En résumé, φ est une application de $\mathcal{A}_n$ dans $S_n \setminus \mathcal{A}_n$. De même, ψ est une application de $S_n \setminus \mathcal{A}_n$ dans $\mathcal{A}_n$.

• Puisque $\tau^2 = Id_{[\![1,n]\!]}$, pour tout $\sigma \in \mathcal{A}_n$, $\psi(\varphi(\sigma)) = \tau \circ (\tau \circ \sigma) = \sigma$ et donc $\psi \circ \varphi = Id_{\mathcal{A}_n}$. De même, $\varphi \circ \psi = Id_{S_n \setminus \mathcal{A}_n}$. On sait alors que φ est une bijection de $\mathcal{A}_n$ sur $S_n \setminus \mathcal{A}_n$ (de réciproque ψ).

• Puisqu'il existe une bijection de $\mathcal{A}_n$ sur $S_n \setminus \mathcal{A}_n$, on en déduit que ces ensembles ont le même nombre d'éléments (le nombre d'éléments d'un ensemble sera proprement défini dans le chapitre « Dénombrements »). Puisque le nombre de permutations de $[\![1, n]\!]$ est $n!$, on en déduit qu'il y a $\dfrac{n!}{2}$ permutations paires et $\dfrac{n!}{2}$ permutations impaires.

❑

⇨ **Commentaire**.

◇ *Par exemple, S_3 est constitué de 6 permutations : Id, les trois transpositions $\tau_{1,2}$, $\tau_{1,3}$ et $\tau_{2,3}$ et les deux permutations circulaires $c_1 = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix}$ et $c_2 = \begin{pmatrix} 3 & 1 & 2 \end{pmatrix}$. Il y a trois permutations impaires à savoir les trois transpositions : $S_3 \setminus \mathcal{A}_3 = \{\tau_{1,2}, \tau_{1,3}, \tau_{2,3}\}$. Les trois autres sont donc des permutations paires $\mathcal{A}_3 = \{Id, c_1, c_2\}$.*

◇ *De manière générale, on doit retenir entre autres de la démonstration du théorème 7, le fait que $S_n \setminus \mathcal{A}_n = \{\tau \circ \sigma,\ \sigma \in \mathcal{A}_n\}$ où τ est une transposition donnée (ou aussi $S_n \setminus \mathcal{A}_n = \{\sigma \circ \tau,\ \sigma \in \mathcal{A}_n\}$).*

4 Décomposition d'une permutation en produit de cycles à support disjoints

4.1 Orbite d'un élément. Cycles. Permutations circulaires

Théorème 8. Soit $n \geqslant \in \mathbb{N}^*$. Soit $\sigma \in S_n$.

Sur $[\![1, n]\!]$, on définit le relation $\mathcal{R}$ par :

$$\forall (i, j) \in [\![1, n]\!]^2,\ (i \mathcal{R} j \Leftrightarrow \exists p \in \mathbb{Z} / \ j = \sigma^p(i)).$$

$\mathcal{R}$ est une relation d'équivalence sur $[\![1, n]\!]$.

DÉMONSTRATION.

• Soit $i \in [\![1, n]\!]$. $\sigma^0(i) = i$. Donc, $\forall i \in [\![1, n]\!]$, $\exists p \in \mathbb{Z} / \ i = \sigma^p(i)$ ou encore $\forall i \in [\![1, n]\!]$, $i \mathcal{R} i$. Donc, $\mathcal{R}$ est réflexive.

• Soit $(i, j) \in [\![1, n]\!]^2$ tel que $i \mathcal{R} j$. Donc, il existe $p \in \mathbb{Z}$ tel que $j = \sigma^p(i)$. Mais alors $i = \sigma^{p'}(j)$ où $p' = -p \in \mathbb{Z}$. Donc $\forall (i, j) \in [\![1, n]\!]^2$, $(i \mathcal{R} j \Rightarrow j \mathcal{R} i)$. $\mathcal{R}$ est symétrique.

• Soit $(i, j, k) \in [\![1, n]\!]^3$ tel que $i \mathcal{R} j$ et $j \mathcal{R} k$. Donc, il existe $(p, p') \in \mathbb{Z}^2$ tel que $j = \sigma^p(i)$ et $k = \sigma^{p'}(j)$. Mais alors $k = \sigma^{p'}(\sigma^p(i)) = \sigma^{p''}(i)$ où $p'' = pp' \in \mathbb{Z}$. Donc $\forall (i, j, k) \in [\![1, n]\!]^2$, $(i \mathcal{R} j$ et $j \mathcal{R} k \Rightarrow i \mathcal{R} k)$. $\mathcal{R}$ est transitive.

Finalement, $\mathcal{R}$ est une relation d'équivalence sur $[\![1,n]\!]$.

❑

On sait que les classes d'équivalences modulo une relation d'équivalence sur un ensemble non vide E forment une partition de E. Ici, les classes d'équivalence pour la relation $\mathcal{R}$ du théorème 8 s'appellent les **orbites** de la permutation σ. Plus précisément,

DÉFINITION 5. Soit $n \geqslant \in \mathbb{N}^*$. Soit $\sigma \in S_n$.

Pour $x \in [\![1,n]\!]$, l'**orbite** de x sous σ est $O(x) = \left\{\sigma^k(x),\ k \in \mathbb{Z}\right\}$.

Un résultat immédiat est :

Théorème 9. Soit $n \geqslant \in \mathbb{N}^*$. Soit $\sigma \in S_n$.

Tout x de $[\![1,n]\!]$ appartient à une orbite et une seule. Les orbites sous σ forment une partition de $[\![1,n]\!]$.

Théorème 10. Soit $n \geqslant \in \mathbb{N}^*$. Soit $\sigma \in S_n$.

Pour tout x de $[\![1,n]\!]$, il existe $p \in \mathbb{N}^*$ unique tel que $O(x) = \left\{\sigma^k(x),\ 0 \leqslant k \leqslant p-1\right\}$ et de plus,
$\forall (k,l) \in [\![0,p-1]\!]^2,\ \left(k \neq l \Rightarrow \sigma^k(x) \neq \sigma^l(x)\right)$.

DÉMONSTRATION. Soit $x \in \mathbb{N}$. $O(x) = \left\{\sigma^k(x),\ k \in \mathbb{Z}\right\}$. Les $\sigma^k(x)$, $0 \leqslant k \leqslant n$, sont $n+1$ éléments de l'ensemble $[\![1,n]\!]$ qui a n éléments. Les $\sigma^k(x)$, $0 \leqslant k \leqslant n$, ne peuvent être deux à deux distincts (principe des tiroirs). Par suite, il existe $(k,l) \in [\![0,n]\!]^2$ tel que $k < l$ et $\sigma^k(x) = \sigma^l(x)$. On en déduit que $\sigma^{-l}\left(\sigma^k(x)\right) = \sigma^{-l}\left(\sigma^l(x)\right)$ puis que $\sigma^{l-k}(x) = x$.

$k' = l-k$ est un entier naturel non nul tel que $\sigma^{k'}(x) = x$. Par suite, $\left\{k \in \mathbb{N}^*/\ \sigma^k(x) = x\right\}$ est une partie non vide de $\mathbb{N}$ et même de $\mathbb{N}^*$. $\left\{k \in \mathbb{N}^*/\ \sigma^k(x) = x\right\}$ admet un plus petit élément que l'on note p. Par définition, p est un entier naturel non nul tel que $\sigma^p(x) = x$. On en déduit que pour tout $q \in \mathbb{Z}$, $\sigma^{pq}(x) = x$ (par récurrence pour $q \in \mathbb{N}$, puis en prenant l'image des deux membres par la réciproque pour $q \in \mathbb{Z}^-$).

Soit $k \in \mathbb{Z}$. La division euclidienne de k par p s'écrit $k = pq + r$ où $(q,r) \in \mathbb{Z}^2$ et $0 \leqslant r \leqslant p-1$. On en déduit que $\sigma^k(x) = \sigma^r\left(\sigma^{pq}(x)\right) = \sigma^r(x)$. Ainsi, $O(x) \subset \left\{\sigma^k(x),\ 0 \leqslant k \leqslant p-1\right\}$ et finalement $O(x) = \left\{\sigma^k(x),\ 0 \leqslant k \leqslant p-1\right\}$.

Enfin, si il existe $(k,l) \in [\![0,p-1]\!]^2$ tel que $k < l$ et $\sigma^k(x) = \sigma^l(x)$, alors $0 < l-k < p$ et $\sigma^{l-k}(x) = x$ ce qui contredit la définition de p. Donc, les $\sigma^k(x)$, $0 \leqslant k \leqslant p-1$, sont deux à deux distincts. Ceci démontre l'existence de p.

L'unicité de p est due au fait que p est nécessairement le nombre d'éléments de $O(x)$. On note que le nombre d'éléments p de $O(x)$ est aussi le plus petit entier naturel non nul k tel que $\sigma^k(x) = x$.

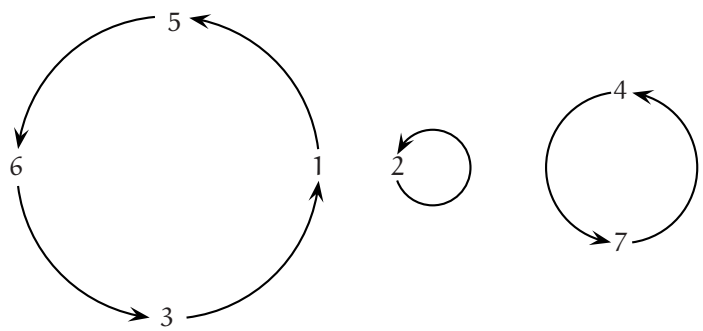
❑

Exemple. Reprenons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix}$. Dans l'orbite de l'élément 1, on trouve $\sigma(1) = 5$, puis $\sigma(\sigma(1)) = \sigma(5) = 6$ puis $\sigma^3(1) = \sigma(6) = 3$. On note alors que $\sigma^4(1) = \sigma(3) = 1$. On en déduit que

$$O(1) = \left\{\sigma^k(1),\ k \in \mathbb{Z}\right\} = \left\{1, \sigma(1), \sigma^2(1), \sigma^3(1)\right\} = \{1,3,5,6\} = O(3) = O(5) = O(6).$$

Ensuite, $\sigma(2) = 2$ et donc pour tout $k \in \mathbb{Z}$, $\sigma^k(2) = 2$. L'orbite de 2 est un singleton : $O(2) = \{2\}$.
Enfin, $\sigma(4) = 7$ et $\sigma^2(4) = 4$. L'orbite de 4 (ou de 7) est $O(4) = \{4,7\}$.

La permutation σ admet donc trois orbites : $O(1) = \{1,3,5,6\}$, $O(2) = \{2\}$ et $O(4) = \{4,7\}$. La permutation σ peut alors se décomposer « en trois morceaux » que l'on peut visualiser sur le graphique ci-dessous, graphique qui concrétise l'utilisation du mot orbite :



Dans le cas général, si l'orbite d'un élément x de $[\![1,n]\!]$ est un singleton, alors $\sigma(x)=x$ et réciproquement, si $\sigma(x)=x$, alors $O(x)=\{x\}$. Les éléments x de $[\![1,n]\!]$ tels que $\sigma(x)=x$ sont les **points fixes** de la permutation σ. Les points fixes de σ sont les éléments de $[\![1,n]\!]$ dont l'orbite est un singleton.

DÉFINITION 6. Soit $n\geqslant 2$.

Un **cycle** de $[\![1,n]\!]$ est une permutation de $[\![1,n]\!]$ qui admet une orbite et une seule non réduite à un singleton. Le **support** de ce cycle est son orbite non réduite à un singleton et la **longueur** de ce cycle est le cardinal de son support.

Une **permutation circulaire** de $[\![1,n]\!]$ est une permutation de $[\![1,n]\!]$ qui admet une orbite et une seule ou encore une permutation circulaire de $[\![1,n]\!]$ est un cycle de longueur n ou encore une permutation circulaire de $[\![1,n]\!]$ est un cycle de $[\![1,n]\!]$ sans point fixe.

Remarque. Les transpositions sont les cycles de longueur 2.

Exemple. La permutation $\sigma=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$ est un cycle de support $\{1,3,4\}$ et donc de longueur 3, mais n'est pas une permutation circulaire car σ admet 2 pour point fixe. Une permutation circulaire est par exemple $\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$.

❑

L'étude des orbites (théorème 10) nous permet immédiatement d'affirmer :

Théorème 11. Soit $n\geqslant 2$. Soit c un cycle de longueur $p\in[\![2,n]\!]$. Il existe p éléments deux à deux distincts $a_0,\dots,a_{p-1}$ de $[\![1,n]\!]$ tels que

$$c(a_0)=a_1,\ c(a_1)=a_2,\ \dots c(a_{p-2})=a_{p-1}\text{ et }c(a_{p-1})=a_0\text{ et }\forall i\in[\![1,n]\!]\setminus\{a_0,\dots,a_{p-1}\},\ \sigma(i)=i.$$

Réciproquement, la permutation définie par les égalités ci-dessus est un cycle de longueur p.

Théorème 12. Soit $n\geqslant 2$. Soit c un cycle de longueur $p\in[\![2,n]\!]$.
Alors $c^p=Id_{[\![1,n]\!]}$ et $\forall k\in[\![1,p-1]\!]$, $c^k\neq Id_{[\![1,n]\!]}$.

DÉMONSTRATION. On reprend les notations du théorème 11. Pour $k\in\mathbb{Z}$, on pose $a_k=a_r$ où r est le reste de la division euclidienne de k par p (ainsi, $a_p=a_0$, $a_{p+1}=a_1$, ...ou aussi $a_{-1}=a_{p-1}$, ...). Avec cette convention, pour tout $k\in\mathbb{Z}$ et tout $i\in[\![0,p-1]\!]$, $c^k(a_i)=a_{k+i}$.

Soit $k\in[\![1,p-1]\!]$. $c^k(a_0)=a_k\neq a_0$. Donc, $c^k\neq Id_{[\![1,n]\!]}$.
Ensuite, $c^p(a_0)=c(a_{p-1})=a_0$. Plus généralement, pour $k\in[\![0,p-1]\!]$, $c^p(a_k)=a_{k+p}=a_k$. Enfin, si $i\notin\{a_0,\dots,a_{p-1}\}$, $c(i)=i$ et donc $c^p(i)=i$.
En résumé, $\forall i\in[\![1,n]\!]$, $c^p(i)=i$ et donc $c^p=Id_{[\![1,n]\!]}$.

❑

Ainsi, la première puissance strictement positive d'un cycle qui est égale à l'identité est sa longueur. On dit que l'**ordre** d'un cycle est sa longueur (l'ordre de c étant la première puissance strictement positive égale à l'identité).

Un autre résultat immédiat est :

Théorème 13. Deux cycles à supports disjoints commutent.

Par contre, si les supports ne sont pas disjoints, les cycles peuvent ne pas commuter. Par exemple, pour $n\geqslant 3$, $\tau_{1,2}$ et $\tau_{1,3}$ sont deux cycles de longueur 2 dont les supports $\{1,2\}$ et $\{1,3\}$ ne sont pas disjoints.
On a $\tau_{1,2}\circ\tau_{1,3}=\begin{pmatrix}3&1&2&\dots\end{pmatrix}$ et $\tau_{1,3}\circ\tau_{1,2}=\begin{pmatrix}2&3&1&\dots\end{pmatrix}$. Donc, $\tau_{1,2}\circ\tau_{1,3}\neq\tau_{1,3}\circ\tau_{1,2}$.

4.2 Décomposition d'une permutation en produit de cycles à support disjoints

On admettra le théorème suivant (qui n'est pas si difficile que ça à démontrer mais dont la démonstration n'est pas exigible) :

Théorème 13. Toute permutation distincte de l'identité se décompose de manière unique, à l'ordre près des facteurs, en produit de cycles à supports deux à deux disjoints.

La décomposition s'obtient en déterminant les orbites. Si on reprend l'exemple de la permutation $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\5&2&1&7&6&3&4\end{pmatrix}$,

on a $\sigma = c_1 \circ c_2 (= c_2 \circ c_1)$ où c_1 est le cycle $\begin{pmatrix} 1 & 3 & 5 & 6 \\ 5 & 1 & 6 & 3 \end{pmatrix}$ et c_2 est le cycle $\begin{pmatrix} 4 & 7 \\ 7 & 4 \end{pmatrix}$ (par commodité d'écriture, on n'a pas écrit tous les points fixes).

Une première utilisation de la décomposition d'une permutation σ distincte de l'identité en produit de cycles à supports deux à deux disjoints est le calcul des puissances de σ. A titre d'exemple, si σ est la permutation ci-dessus, calculons σ^{3146}. **Puisque c_1 et c_2 commutent**, $\sigma^{3146} = c_1^{3146} c_2^{3146}$.

Ensuite, l'ordre d'un cycle est sa longueur et donc $c_1^4 = Id$ puis $\forall k \in \mathbb{Z}$, $c_1^{4k} = Id$. De même, $c_2^2 = Id$ et plus généralement, $\forall k \in \mathbb{Z}$, $c_2^{2k} = Id$. Déjà, $c_2^{3146} = Id$. Ensuite, $c_1^{3146} = c_1^{4\times 786+2} = c_1^2$ et finalement,

$$\sigma^{3146} = c_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 4 & 3 & 1 & 7 \end{pmatrix}.$$

4.3 Un autre calcul de la signature

Théorème 14. La signature d'un cycle de longueur $\ell \geqslant 2$ est $(-1)^{\ell-1}$.

Démonstration. Montrons d'abord par récurrence sur $\ell \geqslant 2$ que la signature d'un cycle de longueur ℓ est $(-1)^{\ell-1}$.

- C'est connu pour $\ell = 2$ (signature d'une transposition).
- Soit $\ell \geqslant 2$. Supposons que tout cycle de longueur ℓ ait pour signature $(-1)^{\ell-1}$. Soit c un cycle de longueur $\ell+1$.
On note $\{a_0, a_1, ..., a_\ell\}$ le support de c et on suppose que, pour $0 \leqslant i \leqslant \ell-1$, $c(a_i) = a_{i+1}$ et que $c(a_\ell) = a_0$.
Montrons alors que $\tau_{a_0,a_\ell} \circ c$ est un cycle de longueur ℓ. $\tau_{a_0,a_\ell} \circ c$ fixe déjà a_ℓ puis, si $0 \leqslant i \leqslant \ell-2$,

$$\tau_{a_0,a_\ell} \circ c(a_i) = \tau_{a_0,a_\ell}(a_{i+1}) = a_{i+1}$$

(car a_{i+1} n'est ni a_0, ni a_ℓ), et enfin $\tau_{a_0,a_\ell} \circ c(a_{\ell-1}) = \tau_{a_0,a_\ell}(a_\ell) = a_0$. $\tau_{a_0,a_\ell} \circ c$ est donc bien un cycle de longueur ℓ. Par hypothèse de récurrence, $\tau_{a_0,a_\ell} \circ c$ a pour signature $(-1)^{\ell-1}$ et donc, c a pour signature $(-1)^{(\ell+1)-1}$.

Le résultat est démontré par récurrence.

❑

Théorème 15. Soient $n \geqslant 1$ puis $\sigma \in S_n$.

Alors, $\varepsilon(\sigma) = (-1)^{n-k}$ où k est le nombre d'orbites de σ.

Démonstration. Montrons que si σ est une permutation quelconque de $[\![1, n]\!]$ ayant k orbites la signature de σ est $(-1)^{n-k}$.

Si σ est l'identité, σ a n orbites et donc $(-1)^{n-k} = (-1)^0 = 1 = \varepsilon(Id)$.

Si σ n'est pas l'identité, on décompose σ en produit de cycles à supports disjoints. On pose $\sigma = c_1 ... c_p$ où p désigne le nombre d'orbites de σ non réduites à un singleton et donc $k-p$ est le nombre de points fixes de σ.
Si ℓ_i est la longueur de c_i, on a donc $n = \ell_1 + ... + \ell_p + (k-p)$ ou encore $n - k = \ell_1 + ... + \ell_p - p$. Mais alors,

$$\varepsilon(\sigma) = \prod_{i=1}^{p} \varepsilon(c_i) = \prod_{i=1}^{p} (-1)^{\ell_i - 1} = (-1)^{\ell_1 + ... + \ell_p - p} = (-1)^{n-k}.$$

❑