Théorème

Toute permutation de $\mathcal{S}_n$ est un produit d'au plus n transpositions.

Démonstration : Si $\sigma = \mathrm{id}$ alors il suffit d'écrire $\sigma = (1\ 2)(1\ 2)$ (on rappelle que $n \geq 2$). On peut supposer maintenant que $\sigma \neq \mathrm{id}$.

Supposons que σ est un p-cycle $\sigma = (i_1\ i_2 \cdots\ i_p)$ avec $p \geq 2$. Il est clair que

$$\sigma = (i_1\ i_2)(i_2\ i_3)\cdots(i_{p-1}\ i_p).$$

Donc σ est produit de $p-1$ transpositions. Comme $p \leq n$ le preuve est terminée dans ce cas.

Plus généralement, toute permutation σ se décompose en produit de m p_i-cycles disjoints $c_1, \cdots, c_m$. Ici nous avons gardé seulement les cycles qui sont distincts de l'identité, il y en a au moins un car $\sigma \neq \mathrm{id}$. En utilisant le point précédent on déduit que σ se décompose en un produit de s transpositions où

$$s = \sum_{i=1}^{m}(p_i - 1) = \sum_{i=1}^{m} p_i - m$$

Or $\sum_{i=1}^{m} p_i$ est le cardinal de la réunion des supports des cycles disjoints $c_1, \cdots, c_m$ qui est visiblement plus petit que n.

Voici une autre démonstration, par récurrence sur n, sans utiliser la décomposition en produit de cycles disjoints. On sait déjà que la propriété est vraie pour $n = 2, 3$. Supposons que la propriété est vraie à l'ordre n. Soit $\sigma \in \mathcal{S}_{n+1}$. Il y a deux cas et deux seulement.

- **(i) Le cas où $\sigma(n+1) = n+1$.** On note s la permutation induite par la restriction de σ à $\{1, \cdots, n\}$. Comme s est une permutation de $\{1, \cdots, n\}$, grâce à l'hypothèse de récurrence, $s = \tau'_1 \cdots \tau'_k$ avec $k \leq n$, où les τ'_j sont des transpositions de $\mathcal{S}_n$. On pose $\tau_j(i) = \tau'_j(i)$ si $i \in \{1, \cdots, n\}$ et $\tau_j(n+1) = n+1$; les τ_j sont des transpositions de $\mathcal{S}_{n+1}$ et $\sigma = \tau_1 \cdots \tau_k$.
- **(ii) Le cas où $\sigma(n+1) = j \in \{1, \cdots, n\}$** . Considérons $\sigma' = \tau_{j,n+1}\sigma$ qui est une permutation qui laisse $n+1$ invariant. Le cas précédent nous montre que l'on peut écrire que $\tau_{j,n+1}\ \sigma = \tau_1 \cdots \tau_k$ avec $k \leq n$. Finalement, $\sigma = \tau_{j,n+1}\tau_1 \cdots \tau_k$

Ainsi toute permutation $\sigma \in \mathcal{S}_{n+1}$ est un produit d'au plus $n+1$ transpositions.

Remarque

Le point (ii) de la démonstration ci-dessus se généralise comme suit : soit i un élément du support de σ et $\tau = (i\ \sigma(i))$. Alors i est un point fixe de la permutation $\tau\sigma$.

Exemple

Soit

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

Nous avons la décomposition en produit de cycles,

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

Comme

$$(1\ 5\ 7\ 6\ 3) = (1\ 5)(5\ 7)(7\ 6)(6\ 3) \quad \text{et} \quad (2\ 4\ 8) = (2\ 4)(4\ 8).$$

nous déduisons la décomposition en produit de transpositions de σ suivante :

$$\sigma = (1\ 5)(5\ 7)(7\ 6)(6\ 3)(2\ 4)(4\ 8).$$

Remarque

- La décomposition en produit de transpositions n'est pas unique ; par exemple

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2) = (1\ 3)(3\ 4)(4\ 2) = (2\ 4)(2\ 1)(1\ 3)$$

- Soit $1 \leq i < j \leq n$. Alors on vérifie facilement que

$$(i\ j) = (1\ i)(1\ j)(1\ i).$$

  En particulier, toute permutation se décompose en produit de transpositions de type $(1\ i), i \in X_n$.

Proposition

1. *Toute transposition se décompose en produit d'un nombre* ***impair*** *de transpositions élémentaires de type* $(i\ i+1), i \in X_n$.
2. *En particulier, toute permutation se décompose en produit de transpositions élémentaires de type* $(i\ i+1), i \in X_n$.

Démonstartion : Il suffit de montrer le premier point. C'est clair pour $(i\ i+1)$. De plus,

$$(i\ i+2) = (i\ i+1)(i+1\ i+2)(i+1\ i).$$

Maintenant, grâce à la formule

$$(i\ j+1) = (i\ j)(j\ j+1)(i\ j)$$

une récurrence permet de montrer que si $j \geq i+2$ alors

$$(i\ j) = (i\ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(\mathbf{j\text{-}1\ j}\ )(j-1\ j-2)\cdots(i+1\ i).$$

En effet, si la formule est vraie pour $(i\ j)$ alors

$$\begin{aligned}
(i\ j+1) &= (i\ j)(j\ j+1)(i\ j) \\
&= (i\ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(j-1\ j-2)\cdots(i+1\ i)(\mathbf{j\ j{+}1})(i\ i+1)\cdot \\
&\quad \cdot(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(j-1\ j-2)\cdots(i+1\ i) \\
&= (i\ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(\mathbf{j\ j{+}1})(j-1\ j-2)\cdots\underbrace{(i+1\ i)(i\ i+1)}_{\text{id}}\cdot \\
&\quad \cdot(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(j-1\ j-2)\cdots(i+1\ i) \\
&= (i\ i+1)(i+1\ i+2)\cdots(j-2\ j-1)(j-1\ j)(\mathbf{j\ j{+}1})(j-1\ j)(j-1\ j-2)\cdots(i+1\ i)
\end{aligned}$$

Exemple

La transposition $(1\ 2)$ et le cycle $(1\ 2\ \cdots\ n)$ engendrent le groupe $\mathcal{S}_n$, i.e. toute permutation se décompose en produit de la transposition $(1\ 2)$ et du cycle $(1\ 2\ \cdots\ n)$.
Pour montrer cela, il suffit de montrer que toute transposition élémentaire $(i\ i+1)$ se décompose en produit de la transposition $(1\ 2)$ et du cycle $(1\ 2\ \cdots\ n)$. Or il est facile de vérifier que

$$(i\ i+1) = (2\ 3\ \ldots\ n\ 1)^{i-1}(1\ \ 2)(2\ 3\ \ldots\ n\ 1)^{1-i}$$

Signature d'une permutation

Définition

Soit $\sigma \in \mathcal{S}_n$ et $i, j \in X_n$.

1. On dit que le couple (i,j) présente une **inversion** pour σ si $i < j$ et si $\sigma(i) > \sigma(j)$. Le nombre d'inversions de σ se note $N(\sigma)$.
2. La **signature** de la permutation σ est le nombre $\varepsilon(\sigma) = (-1)^{N(\sigma)}$.

- Il est clair que $\varepsilon(\sigma) \in \{-1, 1\}$. Par exemple, l'identité n'a aucune inversion. Donc $N(\mathrm{id}) = 0$ et $\varepsilon(\mathrm{id}) = (-1)^0 = 1$.
- La transposition élémentaire $(i\ i+1)$

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ 1 & 2 & \dots & i-1 & i+1 & i & i+2 & \dots & n \end{pmatrix}$$

admet une seule inversion et donc $\varepsilon(\tau) = -1$.

Exemple

Soit

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

Tous les couples $(1,2), (1,3), (1,4)$ et $(1,5)$ présentent des inversions pour σ. Tous les couples $(2,3), (2,4)$ et $(5,5)$ présentent des inversions pour σ. Les autres couples ne présentent pas d'inversions pour σ. Ainsi $N(\sigma) = 7$ et $\varepsilon(\tau) = -1$.

Théorème

La signature d'une transposition est -1.

Démonstration Pour cela calculons le nombre d'inversions d'une transposition. Soit τ la transposition qui échange k et l, avec $k < l$:

$$\tau = \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & \dots & l-1 & l & l+1 & \dots & n \\ 1 & 2 & \dots & k-1 & l & k+1 & \dots & l-1 & k & l+1 & \dots & n \end{pmatrix}$$

On a :

- les couples (i,j) avec $i \in \{1, \cdots, k-1\} \cup \{l+1, \cdots, n\}$ et $i < j$ ne présentent pas d'inversion ;
- le couple (k,j) avec $k < j$ présente une inversion si, et seulement si, j appartient à $\{k+1, \cdots, l\}$, ce qui fait $l-k$ inversion(s) ;
- si $i \in \{k+1, \cdots, l-1\}$ et $i < j$, (i,j) présente une inversion si, et seulement si, $j = l$, ce qui fait $l-1-k$ inversion(s).

Ainsi $N(\tau) = (l-k) + (l-1-k) = 2(l-k) - 1$; ce nombre est impair et $\varepsilon(\tau) = (-1)^{N(\tau)} = -1$.

Lemme

Pour toute permutation σ et toute transposition élémentaire τ, $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Démonstration : Supposons que $\tau = (i\ i+1)$. Il n'y a que deux cas.

(1) Supposons que dans les images de σ le couple $(i, i+1)$ n'est pas inversé :

$$\sigma = \begin{pmatrix} 1 & \dots & k-1 & \mathbf{k} & k+1 & \dots & l-1 & \mathbf{l} & l+1 & \dots & n \\ \sigma(1) & \dots & \sigma(k-1) & \mathbf{i} & \sigma(k+1) & \dots & \sigma(l-1) & \mathbf{i+1} & \sigma(l+1) & \dots & n \end{pmatrix}$$
$$\tau\sigma = \begin{pmatrix} 1 & \dots & k-1 & \mathbf{k} & k+1 & \dots & l-1 & \mathbf{l} & l+1 & \dots & n \\ \sigma(1) & \dots & \sigma(k-1) & \mathbf{i+1} & \sigma(k+1) & \dots & \sigma(l-1) & \mathbf{i} & \sigma(l+1) & \dots & n \end{pmatrix}$$

- Pour tout entier $j \in X_n \setminus \{k, l\}$, on a $\sigma(j) = \tau\sigma(j)$. Un couple formé d'éléments de $X_n \setminus \{k, l\}$ présente une inversion pour σ si, et seulement si, il présente une inversion pour $\tau\sigma$.
- Le couple (k, l) ne présente pas d'inversion pour σ alors qu'il présente une inversion pour $(i\ i{+}1)\sigma$.
- Un couple de la forme (m, k) avec $m = 1, \cdots, k-1$, présente une inversion pour σ, si et seulement si, $i = \sigma(k) < \sigma(m)$, si et seulement si, $\tau\sigma(k) = i+1 < \sigma(m)$, si et seulement si, (m, k) présente une inversion pour $\tau\sigma$.
- De même, un couple de la forme (k, m) avec $m = k+1, \cdots, l-1, l+1, \cdots, n$, présente une inversion pour σ, si et seulement si, $\sigma(m) < \sigma(k) = i$, si et seulement si, $\sigma(m) < i+1 = \tau\sigma(k)$, si et seulement si, (k, m) présente une inversion pour $\tau\sigma$.
- De même, un couple de la forme (m, l) avec $m = 1, \cdots, k-1, k+1, \cdots, l-1$, présente une inversion pour σ, si et seulement si, (m, l) présente une inversion pour $\tau\sigma$.
- De même, un couple de la forme (l, m) avec $m = l+1, \cdots, n$ présente une inversion pour σ, si et seulement si, il présente une inversion pour $\tau\sigma$.

Finalement,

$$N((i\ i+1)\sigma) = N(\sigma) + 1$$

et donc $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

(2) Supposons que dans les images de σ le couple $(i, i+1)$ est inversé :

$$\sigma = \begin{pmatrix} 1 & \dots & k-1 & \mathbf{k} & k+1 & \dots & l-1 & \mathbf{l} & l+1 & \dots & n \\ \sigma(1) & \dots & \sigma(k-1) & \mathbf{i+1} & \sigma(k+1) & \dots & \sigma(l-1) & \mathbf{i} & \sigma(l+1) & \dots & n \end{pmatrix}$$
$$\tau\sigma = \begin{pmatrix} 1 & \dots & k-1 & \mathbf{k} & k+1 & \dots & l-1 & \mathbf{l} & l+1 & \dots & n \\ \sigma(1) & \dots & \sigma(k-1) & \mathbf{i} & \sigma(k+1) & \dots & \sigma(l-1) & \mathbf{i+1} & \sigma(l+1) & \dots & n \end{pmatrix}$$

En faisant jouer le rôle de σ à $\tau\sigma$ et vice versa dans le premier cas on voit que $N(\sigma) = N((i\ i{+}1)\sigma) + 1$ et donc $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Théorème

La signature d'un produit de p transpositions est $(-1)^p$.

Démonstration : Soit $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_p$ un produit de p transpositions. Si toutes les transpositions τ_i sont élémentaires alors

$$\varepsilon(\sigma) = \varepsilon(\tau_1 \cdots \tau_2 \cdots \tau_p) = -\varepsilon(\tau_2 \cdots \tau_p) = (-1)^2\varepsilon(\tau_3 \cdots \tau_p) = \cdots = (-1)^p.$$

Dans le cas général, on sait que chacune des transpositions τ_i se décompose en un nombre impair $2k_i + 1$ de transpositions élémentaires. Donc σ est produit de

$$p' = \sum_{i=1}^{p} (2k_i + 1) = p + 2\sum_{i=1}^{p} k_i$$

transpositions élémentaires, si bien que

$$\varepsilon(\sigma) = (-1)^{p'} = (-1)^p.$$

On sait que la décomposition d'une permutation σ en produit de transpositions n'est pas unique. En revanche, la signature nous montre que la parité du nombre de transpositions est commun à toutes ces décompositions et ne dépend donc que σ. En effet, si

$$\sigma = \prod_{1 \leq i \leq p} \tau_i = \prod_{1 \leq i \leq q} \tau_i'$$

sont deux décompositions en produit de transpositions de σ, alors

$$\varepsilon(\sigma) = (-1)^p = (-1)^q$$

Corollaire

La signature d'une permutation σ est $(-1)^p$ si, et seulement si, p est le nombre de transpositions de n'importe quelle décomposition de σ en produit de transpositions.

Définition

1. Une permutation est paire si sa signature est positive.
2. Une permutation est impaire si sa signature est négative.

Corollaire

La signature ε est un morphisme du groupe $(\mathcal{S}, \cdot)$ sur le groupe $\mathbb{U}_2 = \{1, -1\}$ muni de la multiplication. Autrement dit,

$$\forall (\sigma_1, \sigma_2) \in \mathcal{S}_n^2, \quad \varepsilon(\sigma_1 \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

Démonstration : On sait que σ_1, σ_2 se décomposent respectivement en produit de p et q transpositions. Ainsi $\sigma_1\sigma_2$ est le produit de $p+q$ transpositions. Finalement,

$$\varepsilon(\sigma_1\sigma_2) = (-1)^{p+q} = (-1)^p(-1)^p = \varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

La preuve est terminée.

Théorème

1. *L'ensemble $\mathcal{A}_n$ des permutations paires est un sous groupe de $\mathcal{S}_n$ appelé le groupe alterné.*
2. *$\mathcal{A}_n$ et $\mathcal{S}_n \setminus \mathcal{A}_n$ ont le même cardinal qui vaut $\dfrac{n!}{2}$.*

Démonstration : (i) D'abord le produit de deux permutations paires est une permutation paire. De plus, une permutation et son inverse ont la même signature. Donc $\mathcal{A}_n$ est un sous groupe de $\mathcal{S}_n$.

(ii) Comme le cardinal de $\mathcal{S}_n$ est $n!$, il suffit de montrer que $\mathcal{A}_n$ et $\mathcal{S}_n \setminus \mathcal{A}_n$ ont le même cardinal. Ainsi il suffit d'exhiber une bijection de $\mathcal{A}_n$ sur $\mathcal{S}_n \setminus \mathcal{A}_n$. Pour cela, soit τ une transposition. L'application

$$\begin{array}{rcl} \psi : \mathcal{A}_n & \longrightarrow & \mathcal{S}_n \setminus \mathcal{A}_n \\ \sigma & \longmapsto & \psi(\sigma) = \tau\sigma \end{array}$$

est bien définie, bijective et son inverse est donnée par $\psi^{-1}(\sigma) = \tau\sigma$ pour tout $\sigma \in \mathcal{S}_n \setminus \mathcal{A}_n$.

Remarque

En fait, on peut montrer que le seul morphisme de groupe de $\mathcal{S}_n$ sur $\mathbb{U}_2 = \{-1, 1\}$ qui est différent de 1 est la signature.

Exemple : Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 1 & 2 & 7 & 5 & 6 & 8 & 3 \end{pmatrix} \in S_9.$$

Nous avons la décomposition en produit de cycles,

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

Donc la signature de σ est $(1)^2(-1)^1(-1)^2 = -1$. Nous avons aussi la décomposition en produit de transpositions

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

On retrouve que la signature de σ est -1 car le nombre de transpositions dans la décomposition précédente est impair.

On peut aussi calculer le nombre d'inversions de σ.

1. il y a 8 couples de type $(1, j)$ tels que $j > 1$ et $\sigma(1) > \sigma(j)$,
2. il y a 3 couples de type $(2, j)$ tels que $j > 2$ et $\sigma(2) > \sigma(j)$,
3. il n'y a aucun couple de type $(3, j)$ tels que $j > 3$ et $\sigma(3) > \sigma(j)$,
4. il n'y a aucun couple de type $(4, j)$ tels que $j > 4$ et $\sigma(4) > \sigma(j)$,
5. il y a 3 couples de type $(5, j)$ tels que $j > 5$ et $\sigma(5) > \sigma(j)$,
6. il y a un couple de type $(6, j)$ tels que $j > 6$ et $\sigma(6) > \sigma(j)$,
7. il y a un couple de type $(7, j)$ tels que $j > 7$ et $\sigma(7) > \sigma(j)$,
8. il y a un couple de type $(8, j)$ tels que $j > 8$ et $\sigma(8) > \sigma(j)$.

Ainsi il y 17 inversions et on retrouve que la signature de σ est -1.

On peut aussi déduire que l'ordre de σ est 6= $PPCM(2, 3)$. On peut alors calculer facilement les puissances successives de σ. Par exemple,

$$\sigma^{2022} = \mathrm{id},\ \sigma^{2021} = \sigma^5,\ \sigma^{2020} = \sigma^4\ \sigma^{2019} = \sigma^3,\ \sigma^{2018} = \sigma^2\ \sigma^{2017} = \sigma.$$