Groupe symétrique

Rappel

Soit E un ensemble muni d'un nombre fini d'éléments. Toute bijection de E dans E est appelée une permutation. L'ensemble des permutations de E que l'on note S_E est un groupe associé à la loi o (loi de composition) que l'on appelle groupe symétrique.

Remarque

- Tout ensemble de n éléments étant en bijection avec $[\![1,n]\!]$ (l'ensemble des entiers naturels compris entre 1 et n), il est d'usage plutôt que de travailler sur un ensemble quelconque de n éléments de travailler sur $[\![1,n]\!]$. On note alors S_n l'ensemble des permutation sur $[\![1,n]\!]$
- Toute permutation de S_n sera représentée par une matrice $(2,n)$. Par exemple la permutation σ de S_5 caractérisée par la matrice ci-dessous :
  $\begin{pmatrix}1&2&3&4&5\\4&2&3&5&1\end{pmatrix}$ vérifie $\sigma(1)=4;\ \sigma(2)=2;\ \sigma(3)=3;\ \sigma(4)=5;\ \sigma(5)=1;$

Définition

On appelle support d'une permutation l'ensemble des entiers dont les images diffèrent des antécédents.

Exemple

Reprenons σ de S_5 dont le graphe a été donné plus haut. Le support de σ noté $supp(\sigma)$ est égal à $\{1\,;4\,;5\}$

Définition

Deux permutations dont les supports sont disjoints sont dits disjointes.

Propriété

Deux permutations disjointes commutent.

Preuve

Soient σ_1 et σ_2 deux permutations disjointes.
Soit $i \in [\![1,n]\!]$ et $i \notin supp(\sigma_1) \cup supp(\sigma_2).\ \sigma_1 o\, \sigma_2(i) = \sigma_1(i) = i = \sigma_2(i) = \sigma_2 o \sigma_1(i)$
Soit $i \in [\![1,n]\!]$ et $i \in supp(\sigma_1)$ $(i \notin supp(\sigma_2)\,; \sigma_2(i) = i\ et\ \sigma_1(i) = j$ avec $j \neq i)$
$\sigma_1 o\, \sigma_2(i) = \sigma_1(i) = j$;
$\sigma_1(i) = j \Longrightarrow \sigma_1(j) \neq j \Longrightarrow j \in supp(\sigma_1) \Longrightarrow$
$j \notin supp(\sigma_2)\ (car\ les\ 2\ permutations\ sont\ disjointes) \Longrightarrow \sigma_2(j) = j \Longrightarrow \sigma_2 o\, \sigma_1(i) = \sigma_2(j) = j$
Donc $\sigma_1 o\, \sigma_2(i) = \sigma_2 o\, \sigma_1(i)$.
Bien entendu le problème étant symétrique si $i \in [\![1,n]\!]$ et $i \in supp(\sigma_2)$ alors on aura aussi $\sigma_1 o\, \sigma_2(i) = \sigma_2 o\, \sigma_1(i)$
En résumé σ_1 et σ_2 commutent

Définition

Soit σ une permutation de $[\![1,n]\!]$ et $x \in [\![1,n]\!]$. L'orbite de x pour σ est notée $Orb_\sigma(x)$ et est définie par :
$$\{y \in [\![1,n]\!]\ tq\ \exists k \in \mathbb{Z}, y = \sigma^k(x)\}$$

Exemple

Pour $\sigma = \begin{pmatrix}1&2&3&4&5\\4&2&3&5&1\end{pmatrix}$,
Nous avons $Orb_\sigma(1) = Orb_\sigma(4) = Orb_\sigma(5) = \{1,4,5\}$; $Orb_\sigma(2) = \{2\}$; $Orb_\sigma(3) = \{3\}$

Propriété

Soit σ une permutation de $[\![1,n]\!]$. Soient x et y deux éléments de $[\![1,n]\!]$. Notons $\mathcal{R}$ la relation définie par
$$\forall (x,y) \in [\![1,n]\!]^2, x\mathcal{R}y \iff y \in Orb_\sigma(x)$$
Alors $\mathcal{R}$ est une relation d'équivalence sur $[\![1,n]\!]$

Preuve

- $\mathcal{R}$ est réflexive. $\forall x \in [\![1,n]\!], x \in Orb_\sigma(x)$ car $x = \sigma^0(x)$
- $\mathcal{R}$ est symétrique. $\forall (x,y) \in [\![1,n]\!]^2,\ x\mathcal{R}y \Longrightarrow y \in Orb_\sigma(x) \Longrightarrow \exists k \in \mathbb{Z}, y = \sigma^k(x) \Longrightarrow x = (\sigma^{-1})^k(y) = \sigma^{-k}(y) \Longrightarrow x \in Orb_\sigma(y)$
- $\mathcal{R}$ est transitive. $\forall (x,y,z) \in [\![1,n]\!]^3 \begin{Bmatrix}x\mathcal{R}y\\et\\y\mathcal{R}z\end{Bmatrix} \Longrightarrow \begin{Bmatrix}\exists k \in \mathbb{Z}, y = \sigma^k(x)\\et\\\exists m \in \mathbb{Z}, z = \sigma^m(y)\end{Bmatrix} \Longrightarrow z = \sigma^{k+m}(x) \Longrightarrow x\mathcal{R}z$

Propriété

Les orbites de σ forment une partition de $[\![1,n]\!]$. (Ce sont des les classes d'équivalence de la relation $\mathcal{R}$)

Exemple

Reprenons l'exemple précédent : $[\![1,5]\!] = \{1,4,5\} \cup \{2\} \cup \{3\} = Orb_\sigma(1) \cup Orb_\sigma(2) \cup Orb_\sigma(3)$

Propriété

Supposons que σ possède p orbites disjointes.
(Attention une orbite peut avoir une taille égale à 1)
Soit $O_{i,\sigma}$ une orbite de σ $(1 \leq i \leq p)$ et $x_i \in O_{i,\sigma}$ alors :
$$\exists k_i \in \mathbb{N}, 1 \leq k_i \leq n, O_{i,\sigma} = \{x_i, \sigma(x_i), \sigma^2(x_i), \ldots \sigma^{k_i-1}(x_i)\}.\ k_i \text{ est la taille de } O_{i,\sigma}$$

Preuve

Considérons $A_{x_i} = \{ \sigma^m(x_i), m \in \mathbb{Z}\}$. $A_{x_i} \subset O_{i,\sigma}$ Donc A_{x_i} est de taille fini.

$$\exists (k,l) \in \mathbb{Z}^2 \ (k \neq l) \ tq \ \sigma^k(x_i) = \sigma^l(x_i) \Longrightarrow \sigma^{k-l}(x_i) = x_i = \sigma^{l-k}(x_i)$$

En posant $B_{x_i} = \{ m \in \mathbb{N} \ tq \ \sigma^m(x_i) = x_i\}$ nous pouvons en déduire que B_{x_i} est non vide.

Etant une sous partie de $\mathbb{N}$ il admet un plus petit élément que nous nommerons k_i

$$\forall y \in O_{i,\sigma}, \exists k \in \mathbb{Z} \, tq \, y = \sigma^k(x_i).$$

Réalisons la division euclidienne de k par k_i. $k = ak_i + r$ avec $a \in \mathbb{Z}$ et $0 \leq r < k_i$

$$y = \sigma^k(x_i) = \sigma^{ak_i+r}(x_i) = \sigma^r o \ \sigma^{ak_i}(x_i) = \sigma^r(x_i)$$

Nous avons donc $\forall y \in O_{i,\sigma}$, $\exists r \ avec \ 0 \leq r < k_i$ tel que $y = \sigma^r(x_i)$

Réciproquement nous savons que tout élément de la forme $\sigma^r(x_i)$ appartient à $O_{i,\sigma}$.

Les $\sigma^r(x_i)$ sont-ils tout distincts lorsque r décrit $[\![0; k_i - 1]\!]$? Supposons que ce ne soit pas le cas.

Soit $(y_1, y_2) \in {O_{i,\sigma}}^2$ avec $y_1 = \sigma^{r_1}(x_i)$ et $y_2 = \sigma^{r_2}(x_i)$ avec $0 \leq r_1 < k_i$ et $0 \leq r_1 < k_i$

$$\sigma^{r_1}(x_i) = \sigma^{r_2}(x_i) \Longrightarrow \sigma^{r_1-r_2}(x_i) = \sigma^{r_2-r_1}(x_i) = x_i$$

Supposons que $r_1 - r_2 \geq 0$ (si ce n'est pas le cas il suffira de prendre $r_2 - r_1$)

Nous avons $\sigma^{r_1-r_2}(x_i) = x_i$ et $0 \leq r_1 - r_2 < k_i$. Nous sommes donc arrivés à une contradiction avec la définition de k_i.

Les $\sigma^r(x_i)$ sont donc tout distincts lorsque r décrit $[\![0; k_i - 1]\!]$.

$$O_{i,\sigma} = \{x_i, \sigma(x_i), \sigma^2(x_i), \dots \sigma^{k_i-1}(x_i)\}$$

Exemple	Reprenons l'exemple précédent avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$. $Orb(1) = \{1; \ \sigma(1); \sigma^2(1)\}$
Définition	On appelle $p - cycle$ ou cycle de longeur p toute permutation σ telle qu'il existe $x_1, x_2 \ \dots x_p$ distincts dans $[\![1, n]\!]$ pour lesquels $\sigma(x_1) = x_2; \ \sigma(x_2) = x_3 \ ; \dots \sigma(x_p) = x_1$. Si $x \notin \{x_1, x_2 \ \dots x_p\}$ alors $\sigma(x) = x$ Un tel cycle se note $(x_1, x_2, x_3, \dots \ x_p)$
Exemple	La permutation σ définie par $\sigma = (1,2,3)$ vérifie $\sigma(1) = 2 \ ; \ \sigma(2) = 3; \sigma(3) = 1$ et $\forall x \notin \{1,2,3\} \ \sigma(x) = x$ C'est donc un $3 - \ cycle$
Définition	Un cycle de longeur 2 s'appelle une transposition et se note $\tau_{i,j}$ ou $(i \ \ j)$ $(\tau_{i,j}(i) = j \ ; \ \tau_{i,j}(j) = i$ et $\forall x \notin \{i,j\} \ \tau_{i,j}(x) = x \ )$
Théorème	Toute permutation peut se décomposer en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre des cycles dans la décomposition près.

Preuve

Montrons d'abord l'existence d'une telle décomposition. Soit σ une permutation.

Soient $O_{\sigma,1}, O_{\sigma,2} \dots O_{\sigma,p}$ les orbites de σ constituant la partition de $[\![1, n]\!]$.

(Là encore une orbite peut être de taille égale à 1)

Soient $x_1, x_2, \dots x_p$ des éléments de $O_{\sigma,1}, O_{\sigma,2} \dots O_{\sigma,p}$

Comme vu précédemment chaque $O_{\sigma,i}$ peut se représenter ainsi $\{x_i, \sigma(x_i) , \sigma^2(x_i), \dots \ \sigma^{k_i-1}(x_i)\}$ avec $1 \leq k_i \leq n$ et $\sum_{i=1}^{p} k_i = n$

Soit γ_i la permutation définie par $\begin{cases} \gamma_i(x) = \ \sigma(x) \text{ si } x \in O_{\sigma,i} \\ \gamma_i(x) = x \ sinon \end{cases}$ $(*)$

Remarquons que dans le cas d'une orbite de taille 1, nous avons $\gamma_i(x) = \ \sigma(x) = x$

γ_i est un cycle de longueur k_i et peut se noter $(x_i, \sigma(x_i) , \sigma^2(x_i), \dots \ \sigma^{k_i-1}(x_i))$

En effet :

- si $x \notin O_{\sigma,i} \ \gamma_i(x) = x$
- si $x \in O_{\sigma,i} \ alors \ x = \sigma^p(x_i) \ avec \ 0 \leq p \leq k_i - 1$. $\gamma_i(x) = \sigma(x) = \sigma^{p+1}(x_i)$
  γ_i est donc un cycle de longueur k_i

Nous avons : $\boldsymbol{\sigma = \prod_{j=1}^{p} \gamma_j}$

En effet, soit $x \in [\![1, n]\!]$. $\exists i \ tq \ x \in O_{\sigma,i}$

Dans ce cas $\gamma_j(x) = x$ pour $j \neq i$ et $\gamma_i(x) = \sigma(x)$.

Les γ_j étant à support disjoints, ils commutent. Nous pouvons donc écrire $\prod_{j=1}^{p} \gamma_j = \gamma_i o \prod_{\substack{j=1 \\ (j \neq i)}}^{p} \gamma_j$

$$\prod_{j=1}^{p} \gamma_j \ (x) = \gamma_i o \prod_{\substack{j=1 \\ (j \neq i)}}^{p} \gamma_j \ (x) = \gamma_i(x) = \sigma(x)$$

Nous avons donc montré que $\forall x \in [\![1, n]\!] \ \prod_{j=1}^{p} \gamma_j \ (x) = \ \sigma(x) \Longrightarrow \boldsymbol{\sigma = \prod_{i=1}^{p} \gamma_i}$

Montrons maintenant l'unicité d'une telle décomposition à l'ordre des cycles près.

Supposons qu'il existe une deuxième décomposition $\sigma = \prod_{i=1}^{p'} \gamma_i'$

Soient $O'_1, O'_2, \dots . O'_p$, les supports respectifs disjoints de ces cycles.

Soit $x \in [\![1,n]\!]$. $\exists i \; tq \; x \in O_{\sigma,i}$ et $\exists j \; tq \; x \in O'_j$

Nous avons déjà vu que $x \in O_{\sigma,i} \Longrightarrow O_{\sigma,i} = \{x, \sigma(x), \sigma^2(x), \dots \sigma^{k_i-1}(x)\}$

Nous savons que $\sigma(x) = \prod_{i=1}^{p'} \gamma'_i = \gamma'_j o \prod_{\substack{i=1 \\ i\neq j}}^{p'} \gamma'_i \,(x) = \gamma'_j(x)$

Donc si $p \in \mathbb{N}, \sigma^p(x) = \gamma_j'^p(x) \Longrightarrow \sigma^p(x) \in O'_j$. Tous les membres de $O_{\sigma,i}$ appartiennent à O'_j. Donc $O_{\sigma,i} \subset O'_j$

Réciproquement $x \in O'_j$. Soit k'_j la taille du cycle γ'_j. $O'_j = \{x, \gamma'_j(x), \gamma_j'^2(x), \dots \gamma_j^{\prime(k'_j-1)}(x)\}$

Or $\gamma'_j(x) = \sigma(x)$ Donc $O'_j \subset O_{\sigma,i}$

Nous avons donc $\boldsymbol{O'_j = O_{\sigma,i}}$.

$O_{\sigma,i}$ définit le cycle γ_i $\left(voire\ (*)\right)$ et O'_j définit le cycle γ'_j donc $\gamma_i = \gamma'_j$

A chaque γ'_j de la décomposition $\sigma = \prod_{i=1}^{p'} \gamma'_i$ correspond un γ_i qui lui est égal dans la décomposition $\sigma(x) = \prod_{j=1}^{p} \gamma_j \,(x)$. Les γ'_j commutant entre eux, de même que les γ_i nous en déduisons que la décomposition est identique.

Exemple	La permutation σ définie par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 6 & 2 & 1 & 7 \end{pmatrix}$ peut se décomposer ainsi : $\sigma = (1\ 3\ 4\ 6) o (2\ 5)$
Propriété	Toute permutation peut se décomposer en un produit de transpositions.

Preuve

Nous avons déjà vu que toute permutation peut se décomposer en un produit de cycles.
Tout cycle $(x_1\ x_2\ x_3\ \dots\ x_p)$ peut se décomposer ainsi $(x_1\ x_2) o (x_2\ x_3) o (x_3\ x_4) o \dots . (x_{p-1}\ x_p)$
Donc toute permutation peut se décomposer en un produit de transpositions.

Exemple	Reprenons la permutation σ donnée plus haut. $\sigma = (1\ 3\ 4\ 6) o (2\ 5) = (1\ 3) o (3\ 4) o (4\ 6) o (2\ 5)$
Remarque	La décomposition d'une permutation en produit de transpositions n'est pas unique. $(1\ 2\ 3) = (1\ 2) o (2\ 3) = (2\ 3) o (1\ 3)$
Définition	Pour toute permutation σ, nous noterons $\mu(\sigma)$ le nombre de $\sigma - orbites$ disjointes. (Attention, là encore une $\sigma - orbite$ être de taille 1) Nous appelons **signature** d'une permutation le nombre $\boldsymbol{\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}}$
Exemple	• Considérons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 6 & 2 & 1 & 7 \end{pmatrix}$ dont nous avons vu que la décomposition en produit de cycles disjoints est égale à $(1\ 3\ 4\ 6) o (2\ 5) o (7)$. Il y a donc 3 orbites disjointes ce qui nous amène à $\varepsilon(\sigma) = (-1)^{7-3} = 1$ • La signature de l'identité est égale à $(-1)^{n-n} = (-1)^0 = 1$ • Pour une transposition nous avons une orbite de taille 2 et $(n-2)$ orbites de taille 1. Donc la signature d'une transposition est égale à $(-1)^{n-[n-2+1]} = (-1)$ • Pour un cycle de longueur p, nous avons une orbite de taille p et $n-p$ orbites de taille 1. La signature d'un tel cycle est donc égale à $(-1)^{n-[1+(n-p)]} = (-1)^{p-1}$
Propriété	Pour toute permutation σ et toute transposition τ nous avons $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$

Preuve

Soient $O_{\sigma,1}, O_{\sigma,2} \dots O_{\sigma,p}$ les orbites de σ de taille non réduites à un élément et soit $\tau = \tau_{i,j}$ avec $(i,j) \in [\![1,n]\!]^2$

- 1er cas : $\{i,j\} \cap \cup_{j=1}^{p} O_{\sigma,p} = \emptyset$. i et j correspondent donc à des points fixes de σ
  $\tau\sigma$ possède donc une orbite de taille 2 de plus que σ et deux orbites de taille 1 en moins. Nous en déduisons $\mu(\tau\sigma) = \mu(\sigma) - 2 + 1 = \mu(\sigma) - 1 \Longrightarrow \varepsilon(\tau\sigma) = (-1)^{n-\mu(\tau\sigma)} = (-1)^{n-(\mu(\sigma)-1)} = (-1)(-1)^{n-\mu(\sigma)} = (-1)\varepsilon(\sigma)$
- 2eme cas : $i \in \cup_{j=1}^{p} O_{\sigma,p} \; et \; j \notin \cup_{j=1}^{p} O_{\sigma,p}$. j correspond donc à un point fixe de σ
  Soit k tel que $i \in O_{\sigma,k}$ et soit t_k la taille de cette orbite.
  Nous avons $O_{\sigma,k} = \{i, \sigma(i), \sigma^2(i), \dots \sigma^{t_k-1}(i)\}$
  Soient $c_1, c_2 \dots ., c_p$ les cycles définis par les orbites $O_{\sigma,1}, O_{\sigma,2}, \dots O_{\sigma,p}$
  (Rappel : $c_p(x) = \sigma(x)$ si $x \in O_{\sigma,p}$ et $c_p(x) = x$ sinon). Nous avons $\sigma = c_1 o c_2 \dots . o c_p$
  Nous avons $\sigma = c_1 o c_2 \dots . o c_p = c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j \Longrightarrow \tau_{i,j} o \sigma = \tau_{i,j} o c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$

$$\tau_{i,j} o c_k = (i\ \ j)(i\ \ \sigma(i)\ \ \sigma^2(i)\ \ \dots \sigma^{t_k-1}(i)) = (j\ \ i\ \ \sigma(i)\ \ \sigma^2(i)\ \ \dots \sigma^{t_k-1}(i)) = c'_k$$

$\sigma = c'_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$, c'_k étant à support disjoint de tous les c_j

$\tau\sigma$ possède donc un point fixe de moins que σ et un nombre d'orbites de taille > 1 égal à celui de σ.

Nous en déduisons $\mu(\tau\sigma) = \mu(\sigma) - 1 \Longrightarrow \varepsilon(\tau\sigma) = (-1)^{n-(\mu(\sigma)-1)} = -(-1)^{n-(\mu(\sigma))} = -\varepsilon(\sigma)$

- 3eme cas : (Très similiaire au deuxième) $i \notin \cup_{j=1}^{p} O_{\sigma,p}$ et $j \in \cup_{j=1}^{p} O_{\sigma,p}$. i correspond donc à un point fixe de σ

  Soit k tel que j $\in O_{\sigma,k}$ et soit t_k la taille de cette orbite.

  Nous avons $O_{\sigma,k} = \{j, \sigma(j), \sigma^2(j), \dots \sigma^{t_k-1}(j)\}$

  Soient $c_1, c_2 \dots, c_p$ les cycles définis par les orbites $O_{\sigma,1}, O_{\sigma,2}, \dots O_{\sigma,p}$

  (Rappel : $c_p(x) = \sigma(x)$ si $x \in O_{\sigma,p}$ et $c_p(x) = x$ sinon). Nous avons $\sigma = c_1 o c_2 \dots . o c_p$

  Nous avons $\sigma = c_1 o c_2 \dots . o c_p = c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j \Longrightarrow \tau_{i,j} o \sigma = \tau_{i,j} o c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$

  $$\tau_{i,j} o c_k = (i \;\; j)(j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_k-1}(j)) = (i \;\; j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_k-1}(j)) = c'_k$$

  $\sigma = c'_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$, c'_k étant à support disjoint de tous les c_j

  $\tau\sigma$ possède donc un point fixe de moins que σ et un nombre d'orbites de taille > 1 égal à celui de σ.

  Nous en déduisons $\mu(\tau\sigma) = \mu(\sigma) - 1 \Longrightarrow \varepsilon(\tau\sigma) = (-1)^{n-(\mu(\sigma)-1)} = -(-1)^{n-(\mu(\sigma))} = -\varepsilon(\sigma)$

- 4eme cas : i et j appartiennent à la même orbite $O_{\sigma,k}$ de taille t_k. $O_{\sigma,k} = \{i, \sigma(i), \sigma^2(i), \dots \sigma^{t_k-1}(i)\}$

  $$\sigma = c_1 o c_2 \dots . o c_p = c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j \Longrightarrow \tau_{i,j} o \sigma = \tau_{i,j} o c_k o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$$

  $$\tau_{i,j} o c_k = (i \;\; j)(i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \dots \sigma^{t_k-1}(i))$$

  En appelant $i = x_1$, $\sigma(i) = x_2$, $\dots . \sigma^{t_k-1}(i) = x_{t_k-1}$, Nous avons

  $$\tau_{i,j} o c_k = (x_1 \;\; j)(x_1 \;\; x_2 \;\; \dots . x_{t_k-1})$$

  Or j est un des x_l avec $t_k - 1 \geq l \geq 2$. Supposons $j = x_p$

  $$(x_1 \;\; x_p)(x_1 \;\; x_2 \;\; \dots \;\; x_p \;\; \dots \;\; x_{t_k-1}) = (x_1 \;\; x_2 \;\; \dots \;\; x_{p-1})(x_p \;\; \dots \;\; x_{t_k-1})$$

  $$\tau_{i,j} o c_k = c'_k o c''_k$$, c'_k et c''_k étant deux cycles à support disjoints.

  $$\tau_{i,j} o \sigma = c'_k o c''_k \; o \prod_{\substack{j=1 \\ (j\neq k)}}^{p} c_j$$

  $\tau\sigma$ possède donc une orbite de plus de taille > 1 que σ. On en déduit $\mu(\tau\sigma) = \mu(\sigma) + 1 \Longrightarrow$

  $$\varepsilon(\tau\sigma) = (-1)^{n-(\mu(\sigma)+1)} = -(-1)^{n-(\mu(\sigma))} = -\varepsilon(\sigma)$$

- 5eme cas : $i \in O_{\sigma,k}$ de taille t_k et $j \in O_{\sigma,l}$ de taille t_l.

  $O_{\sigma,k} = \{i, \sigma(i), \sigma^2(i), \dots \sigma^{t_k-1}(i)\}$ et $O_{\sigma,l} = \{j, \sigma(j), \sigma^2(j), \dots \sigma^{t_l-1}(j)\}$

  $$\sigma = c_1 o c_2 \dots . o c_p = c_k o c_l o \prod_{\substack{j=1 \\ (j\neq k) \\ (j\neq l)}}^{p} c_j \Longrightarrow \tau_{i,j} o \sigma = \tau_{i,j} o c_k o c_l o \prod_{\substack{j=1 \\ (j\neq k) \\ (j\neq l)}}^{p} c_j$$

  $$\tau_{i,j} o c_k o c_l = (i \;\; j)\big(i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \dots \sigma^{t_k-1}(i)\big)(j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_l-1}(j))$$

  $$\tau_{i,j} o c_k o c_l = (j \;\; i)\big(i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \dots \sigma^{t_k-1}(i)\big)(j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_l-1}(j))$$

  $$\tau_{i,j} o c_k o c_l = (i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \dots \sigma^{t_k-1}(i) \;\; j)(j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_l-1}(j))$$

  $$\tau_{i,j} o c_k o c_l = \big(i \;\; \sigma(i) \;\; \sigma^2(i) \;\; \dots \sigma^{t_k-1}(i) \;\; j \;\; \sigma(j) \;\; \sigma^2(j) \;\; \dots \sigma^{t_l-1}(j)\big) = c'_k$$

  Donc $\tau_{i,j} o \sigma = c'_k \; o \prod_{\substack{j=1 \\ (j\neq k) \\ (j\neq l)}}^{p} c_j$

  $\tau\sigma$ possède donc une orbite de moins de taille > 1 que σ. On en déduit $\mu(\tau\sigma) = \mu(\sigma) - 1 \Longrightarrow \varepsilon(\tau\sigma) = (-1)^{n-(\mu(\sigma)-1)} = -(-1)^{n-(\mu(\sigma))} = -\varepsilon(\sigma)$

  Dans tous les cas nous avons bien $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$

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

Preuve

Par recurrence :

- Le cas où $p = 1$ est évident
- Supposons que si $\sigma = \prod_{i=1}^{p} \tau_i$ alors $\varepsilon(\sigma) = (-1)^p$

  Soit σ' un produit de $p + 1$ transpositions. $\sigma' = \prod_{i=1}^{p+1} \tau'_i = \tau'_1 o \prod_{i=2}^{p+1} \tau'_i = \tau'_1 o \tilde{\sigma}$ où $\tilde{\sigma}$ est le produit de p transpositions.

  Nous avons donc $\varepsilon(\sigma') = \varepsilon(\tau'_1 o \tilde{\sigma}) = -\varepsilon(\tilde{\sigma}) = -(-1)^p = (-1)^{p+1}$

Propriété	La signature et l'application constante égale à 1 sont les seuls morphismes de groupe allant du groupe (S, o) vers le groupe $(\{-1; +1\},*)$ où S symbolise le groupe des permutations de $[\![1, n]\!]$.

Preuve

Nous avons déjà vu que (S, o) était un groupe dans le chapitre sur les groupes.
Soient σ_1 et σ_2 deux permutations de $[\![1, n]\!]$. Nous avons déjà vu que toute permutation pouvait se décomposer en un produit de p transpositions. Supposons que σ_1 se décompose en un produit de p transpositions et σ_2 se décompose en un produit de m transpositions. $\sigma_1 = \prod_{i=1}^{p} \tau_i$ et $\sigma_2 = \prod_{i=1}^{m} \tau_i{}'$
D'après la propriété précédente $\varepsilon(\sigma_1 o \sigma_2) = \varepsilon\left(\prod_{i=1}^{p} \tau_i \, o \prod_{i=1}^{m} \tau_i{}' \right) = (-1)^{m+p} = (-1)^m(-1)^p = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$
Donc ε est bien un morphisme. Nous admettrons l'unicité.

Définition	Nous appellerons permutation paire toute permutation dont la signature vaut 1. Nous appellerons permutation impaire toute permutation dont la signature vaut 1.
Exemple	Reprenons la permutation citée plus haut $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 6 & 2 & 1 & 7 \end{pmatrix}$ Nous avons vu que $\sigma = (1\ 3\ 4\ 6) o (2\ 5) = \gamma o \tau$ avec $\gamma = (1\ 3\ 4\ 6)$ et $\tau = (2\ 5)$ $\varepsilon(\sigma) = \varepsilon(\gamma\ \tau) = \varepsilon(\gamma)\varepsilon(\tau) = (-1)^3(-1) = 1$ Donc σ est une permutation paire.