Chapitre 32

# Groupe symétrique

On se donne dans tout le chapitre un entier $n \geqslant 2$.

Si $n = 1$, alors $S_n = \{\mathrm{Id}\}$ ce qui n'a pas un grand intérêt.

## I Groupe symétrique

### I.1 Définition

**Proposition/Définition.** On note $S_n$ l'ensemble des permutations de $[\![1\,;\,n]\!]$. $S_n$, muni de la composition, est un groupe à $n!$ éléments, non commutatif dès que $n \geqslant 3$, appelé groupe symétrique d'ordre $n$.

On rappelle qu'une permutation est, par définition, une bijection.

Démonstration. Déjà faite dans le chapitre 18.

**Remarques :**

- Certains puristes utilisent le gothique et notent cet ensemble $\mathfrak{S}_n$ (mais la notation $S_n$ est la notation au programme).
- En poussant un peu, on pourrait presque dire que $S_n$ est en fait le groupe des permutations de n'importe quel ensemble fini à $n$ éléments. En effet, on a prouvé dans l'exercice 23 du chapitre 18 que si $E$ et $F$ sont équipotents, c'est-à-dire s'il existe une bijection entre $E$ et $F$, et c'est en particulier le cas si $E$ et $F$ sont finis de même cardinal, alors $S_E$ et $S_F$ sont isomorphes, donc le groupe des permutations de n'importe quel ensemble à $n$ éléments est isomorphe à $S_n$. Cela se voit très bien : si on prend $E$ un ensemble à $n$ éléments qu'on note $\{x_1;\dots;x_n\}$, alors il est intuitif que la bijection $\sigma \in S_n$ est « le même objet » que la fonction

$$\widetilde{\sigma} : \left\{ \begin{array}{ccc} E & \to & E \\ \\ x_i & \mapsto & x_{\sigma(i)} \end{array} \right.$$

Par exemple, il est intuitif que les deux fonctions suivantes représentent le même objet, la même permutation, la même opérations sur les éléments, qu'il s'agisse de $1, 2, 3$ ou de $x_1, x_2, x_3$ :

$$\sigma : \left\{ \begin{array}{ccc} [\![1\,;\,3]\!] & \to & [\![1\,;\,3]\!] \\ \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{array} \right. \qquad \widetilde{\sigma} : \left\{ \begin{array}{ccc} \{x_1;x_2;x_3\} & \to & \{x_1;x_2;x_3\} \\ \\ x_1 & \mapsto & x_3 \\ x_2 & \mapsto & x_1 \\ x_3 & \mapsto & x_2 \end{array} \right.$$

Encore un autre exemple : la permutation ci-dessous

Extraite du numéro de Papoum d'avril 2022... Le groupe symétrique est abordable dès 1 an !

peut être identifiée à la permutation

$$\sigma : \begin{cases} [\![1\,;4]\!] & \to & [\![1\,;4]\!] \\ \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 2 \end{cases}$$

C'est pour cela qu'on se contente d'étudier l'ensemble des permutations de $[\![1\,;n]\!]$ : connaître $S_n$ permet de connaître le groupe des permutations de n'importe quel ensemble à $n$ éléments (puisque ces deux groupes sont isomorphes).

- $S_n$ est un groupe non abélien dès que $n \geqslant 3$. Plus fort : son centre est réduit à Id, c'est-à-dire que l'identité est le seul élément qui commute avec tout le monde (cf. exercice 24 du chapitre 18).

## I.2 Notation

Une première façon de noter les éléments de $S_n$ est de les noter sous forme de tableau à 2 lignes et $n$ colonnes, les entiers de 1 à $n$ sur la première ligne, et leurs images respectives sur la deuxième ligne :

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

Une permutation étant, par définition, une bijection, tous les entiers de 1 à $n$ doivent apparaître exactement une fois sur la deuxième ligne.

Par exemple, la permutation $\sigma \in S_3$ ci-dessus se note :

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

**Exemples :**

- Les deux éléments de $S_2$ sont $\mathrm{Id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ : ces deux éléments commutent, on retrouve le fait que $S_2$ est abélien.

Il est de toute façon isomorphe à $\mathbb{Z}/2\mathbb{Z}$, cf. chapitre 18.

- La permutation de Papoum ci-dessus peut s'écrire :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

- Les six éléments de $S_3$ sont :

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- La bijection (exo) de $[\![1\,;n]\!]$ dans lui-même définie par $\sigma(k) = n+1-k$ (c'est la bijection qui consiste à parcourir $[\![1\,;n]\!]$ en sens inverse) s'écrit :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \ldots & 1 \end{pmatrix}$$

## I.3 Composition de permutations

L'ensemble $S_n$ étant un groupe pour la permutation, on peut évidemment composer ces matrices de la même façon qu'on peut composer les bijections correspondantes. Attention, comme pour la composition de fonction, on lit de la droite vers la gauche, c'est-à-dire que, comme lorsqu'on calcule $f \circ g$, on applique d'abord $g$ puis $f$, lorsqu'on compose deux permutations, on applique d'abord celle de droite puis on applique celle de gauche. De plus,

On parlera parfois de produit de permutations, mais c'est juste qu'on note la loi multiplicativement : il ne faut pas perdre de vue qu'on compose des bijections !

la loi étant évidemment la composition, on pourra se dispenser d'écrire le $\circ$, c'est-à-dire qu'on pourra écrire $\sigma\sigma'$ au lieu de $\sigma \circ \sigma'$, mais attention à ne pas croire qu'on fait un produit de matrices, produit qui n'aurait aucun sens à cause de la dimension des matrices.

**Exemple :**

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

Pour calculer la composée des deux permutations, il suffit de se demander : quelle est l'image de 1 par la première transposition ? puis l'image de son image ? et de recommencer avec 2 puis 3 etc. Ici, l'image de 1 par la première est 3 et l'image de 3 est 1 donc l'image de 1 par la composée est 1.

**Remarque :** La loi étant dans tout le chapitre la composition, quand on parlera de puissances, ce sera évidemment pour la composition, c'est-à-dire que pour tout $k \geqslant 1$,

$$\sigma^k = \underbrace{\sigma \circ \cdots \circ \sigma}_{k \text{ fois}}$$

Cette notation a bien un sens car la composition est associative (cf. chapitre 18). De plus, elle vérifie les propriétés habituelles des puissances, par exemple : $\sigma^2 \circ \sigma^3 = \sigma^5$.

**Exemple :**

$$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}^2 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

## I.4 Inverse d'une permutation

Il suffit de lire la matrice du bas vers le haut, en remettant les termes dans l'ordre.

**Exemple :** $\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}^{-1} = \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}$

**Remarques :**

- Là aussi, l'inverse représente la bijection réciproque, rien à voir avec un quelconque inverse qu'on obtiendrait avec le pivot de Gauß : les matrices ne sont même pas carrées !
- Cela permet (comme dans le chapitre 18) de définir $\sigma^k$ lorsque $k$ est un entier négatif : on note $\sigma^0 = \mathrm{Id}$ par convention, et pour tout $k \leqslant 1$ (et donc $-k \geqslant 1$) :

$$\sigma^k = \underbrace{\sigma^{-1} \circ \cdots \circ \sigma^{-1}}_{-k \text{ fois}}$$

Par exemple, $\sigma^{-3} = \sigma^{-1} \circ \sigma^{-1} \circ \sigma^{-1}$. Là aussi, cette notation vérifie les propriétés habituelles des puissances : par exemple, $\sigma^{-2} \circ \sigma^4 = \sigma^2$.

## I.5 Support d'une permutation

**Définition.** Soit $\sigma \in S_n$. On appelle support de $\sigma$ l'ensemble des éléments de $[\![1\,;n]\!]$ qui ne sont pas invariants par $\sigma$ i.e. $\mathrm{supp}(\sigma) = \{x \in [\![1\,;n]\!] \,|\, \sigma(x) \neq x\}$.

En d'autres termes, le support de $\sigma$ est le complémentaire de l'ensemble de ses points fixes.

**Exemples :**

- Le support de l'identité de $[\![1\,;n]\!]$ est l'ensemble vide. Plus précisément, une permutation a un support vide si et seulement si elle est égale à l'identité.
- le support de $\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}$ est $\{2;3\}$.

**Proposition.** Soient $\sigma$ et $\tau$ deux éléments de $S_n$. Alors $\mathrm{supp}(\sigma\circ\tau) \subset \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$. En particulier, $\mathrm{supp}(\sigma^2) \subset \mathrm{supp}(\sigma)$.

On généralise aisément à un nombre quelconque de permutations.

Démonstration. Soit $x \notin \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$. Alors $x \notin \mathrm{supp}(\sigma)$ et $x \notin \mathrm{supp}(\tau)$, c'est-à-dire que $x$ est laissé fixe par $\sigma$ et $\tau$ donc par $\sigma \circ \tau$ si bien que $x \notin \mathrm{supp}(\sigma \circ \tau)$, d'où le résultat par contraposée.

**Corollaire.** Si $\sigma$ et $\tau$ sont à supports disjoints alors, pour tout $k \in \mathbb{N}^*$, il en est de même pour $\sigma^k$ et $\tau^k$.

Démonstration. Découle du fait que $\text{supp}(\sigma^k) \subset \text{supp}(\sigma)$ et $\text{supp}(\tau^k) \subset \text{supp}(\tau)$.

**Remarque :** En général, il n'y a pas égalité dans l'inclusion de la proposition : une des deux permutations peut remettre à sa place un élément dérangé par l'autre, si bien que cet élément sera laissé stable par la composition des deux, et donc ne sera pas dans le support de $\sigma \circ \tau$ alors qu'il sera dans l'union des deux supports.

**Exemple :** Notons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Alors :

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \text{et} \qquad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Alors :

$$\text{supp}(\sigma \circ \tau) = \{2;3;4\} \neq \text{supp}(\sigma) \cup \text{supp}(\tau) = \{1;2;3;4\}$$

Si on veut l'égalité, il faut une condition supplémentaire.

**Proposition.** Soient $\sigma$ et $\tau$ deux éléments de $S_n$ à supports disjoints. Alors $\sigma$ et $\tau$ commutent, et $\text{supp}(\sigma \circ \tau) = \text{supp}(\sigma) \cup \text{supp}(\tau)$, cette union étant disjointe.

Quand on dit qu'ils commutent, c'est évidemment pour la loi $\circ$ évidemment, c'est-à-dire que $\sigma \circ \tau = \tau \circ \sigma$.

Rappelons qu'un élément qui n'est pas dans le support est un point fixe.

**Remarque :** Cela se voit très bien : $\sigma$ et $\tau$ ne vont « pas toucher aux mêmes éléments » donc peuvent agir chacune de leur côté dans l'ordre qu'elles veulent, cela ne changera rien.

Démonstration. Soit $x \in [\![1\,;n]\!]$. Tout d'abord, prouvons que : $x \in \text{supp}(\sigma) \iff \sigma(x) \in \text{supp}(\sigma)$. Il est équivalent de prouver que : $x \notin \text{supp}(\sigma) \iff \sigma(x) \notin \text{supp}(\sigma)$, c'est-à-dire que : $\sigma(x) = x \iff \sigma(\sigma(x)) = \sigma(x)$. Cette dernière équivalence est immédiate : si $\sigma(x) = x$ alors $\sigma(\sigma(x)) = \sigma(x) = x$, et réciproquement, si $\sigma(\sigma(x)) = \sigma(x)$, par injectivité de $\sigma$, on en déduit que $\sigma(x) = x$. En d'autres termes, un élément est laissé stable par $\sigma$ si et seulement si son image l'est aussi.

Prouvons à présent que $\sigma \circ \tau(x) = \tau \circ \sigma(x)$ en distinguant les cas :

- Supposons que $x \notin \text{supp}(\sigma)$ et $x \notin \text{supp}(\tau)$. Alors $\tau(x) = x$ et $\sigma(x) = x$. On en déduit que $\sigma \circ \tau(x) = \tau \circ \sigma(x) = x$ (et $x$ n'est pas dans le support de $\sigma \circ \tau$).
- Supposons que $x \notin \text{supp}(\sigma)$ et $x \in \text{supp}(\tau)$. Alors $\sigma(x) = x$ si bien que $\tau \circ \sigma(x) = \tau(x)$. Or, $x \in \text{supp}(\tau)$ donc $\tau(x) \in \text{supp}(\tau)$ donc n'appartient pas à $\text{supp}(\sigma)$ puisque les deux supports sont distincts. On en déduit que $\tau(x)$ est un point fixe de $\sigma$ donc $\sigma \circ \tau(x) = \tau(x)$ (et en particulier $x$ est dans le support de $\sigma \circ \tau$).
- Par symétrie des rôles, le résultat est encore valable si $x \in \text{supp}(\sigma)$ et $x \notin \text{supp}(\tau)$ (et là aussi $x$ est dans le support de $\sigma \circ \tau$).
- Enfin, les deux supports étant disjoints, le cas $x \in \text{supp}(\sigma)$ et $x \in \text{supp}(\tau)$ ne peut pas se produire.

L'égalité $\text{supp}(\sigma \circ \tau) = \text{supp}(\tau \circ \sigma)$ découle de l'étude ci-dessus : $x$ est dans le support de $\sigma \circ \tau$ si et seulement s'il est dans celui de $\sigma$ ou celui de $\tau$.

**Remarque :** Là aussi, on généralise aisément à un nombre quelconque de permutations à supports (deux à deux) disjoints, c'est-à-dire que le support de la composée est l'union des supports. Donnons un exemple d'application de ce résultat (exemple fréquent, voir par exemple les exercices 6 et 8).

**Exemple :** Soient $\sigma_1, \ldots, \sigma_k$ des permutations à supports disjoints et $\sigma = \sigma_1 \circ \cdots \circ \sigma_n$. Que dire si $\sigma^2 = \text{Id}_{[\![1\,;n]\!]}$ ?

Les $\sigma_i$ étant à supports disjoints, elles commutent deux à deux donc $\sigma^2 = {\sigma_1}^2 \circ \cdots \circ {\sigma_n}^2 = \text{Id}_{[\![1\,;n]\!]}$. Les $\sigma_i$ étant à supports disjoints, c'est également le cas des ${\sigma_i}^2$ donc :

$$\text{supp}(\sigma^2) = \varnothing = \bigcup_{i=1}^{n} \text{supp}({\sigma_i}^2)$$

Dès lors, tous les supports des ${\sigma_i}^2$ sont vides (une union est vide si et seulement si tous les ensembles sont vides) ce qui implique que tous les ${\sigma_i}^2$ sont égaux à $\text{Id}_{[\![1\,;n]\!]}$.

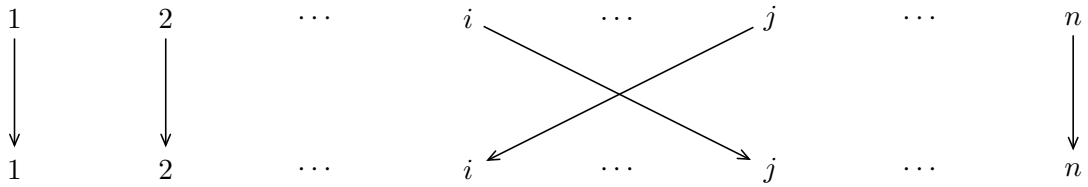
Le support d'une permutation est vide si et seulement si cette permutation est égale à Id.

## I.6 Permutations remarquables, notation cyclique

**Définition.** On appelle transposition une permutation qui échange deux éléments de $[\![1\,;n]\!]$

Et laisse les autres invariants, donc.

**Remarque :** Une transposition n'est rien d'autre qu'une interversion de deux éléments de $[\![1\,;n]\!]$. Ci-dessous on a relié chaque élément de $[\![1\,;n]\!]$ à son image par la transposition qui échange deux éléments $i$ et $j$ :




**Proposition.** Soit $\tau \in S_n$ une transposition. Alors $\tau^2 = \text{Id} : \tau = \tau^{-1}$, $\tau$ est sa propre inverse.

Démonstration. Immédiat : $\tau \circ \tau(i) = \tau(j) = i$, $\tau \circ \tau(j) = \tau(i) = j$ et si $k \neq i, j$, alors $k$ n'appartient pas au support de $\tau$ donc est laissé stable par $\tau$ : $\tau \circ \tau(k) = \tau(k) = k$. Finalement, $\tau^2 = \text{Id}$.

**Définition.** Soit $p \in [\![2\,;n]\!]$. Soit $\sigma \in S_n$. On dit que $\sigma$ est un $p$-cycle s'il existe $x_1, \ldots, x_p \in [\![1\,;n]\!]$ deux à deux distincts tels que :

- $\text{supp}(\sigma) = \{x_1; \ldots; x_p\}$.
- $\forall i \in [\![1\,;p-1]\!]$, $\sigma(x_i) = x_{i+1}$.
- $\sigma(x_p) = x_1$.

Et laisse les autres invariants, donc.

**Proposition.** Si $\sigma$ est un $p$-cycle alors $\sigma^p = \text{Id}$. En particulier, l'inverse de $\sigma$ est $\sigma^{p-1}$.

Il découle même de la démonstration que $p$ est le plus petit indice $k \geqslant 1$ tel que $\sigma^k = \text{Id}$ : on dit que $\sigma$ est d'ordre $p$, si bien que l'ordre d'un cycle est égal à sa longueur, cf. exercice 8.

Démonstration. Avec les notations de la définition, $\sigma^2(x_1) = x_3$, $\sigma^3(x_1) = x_4$ etc. jusque $\sigma^{p-1}(x_1) = x_p$ (récurrence finie immédiate : $\sigma^{k-1}(x_1) = x_k$ pour tout $k \in [\![2\,;p]\!]$) et donc $\sigma^p(x_1) = x_1$. Soit $k \in [\![2\,;p]\!]$. Alors $\sigma^{k-1}(x_1) = x_k$. Par conséquent, $\sigma^{p-k+1}(x_k) = \sigma^p(x_1) = x_1$ et en composant encore par $\sigma^{k-1}$, il vient : $\sigma^p(x_k) = \sigma^{k-1}(x_1) = x_k$.

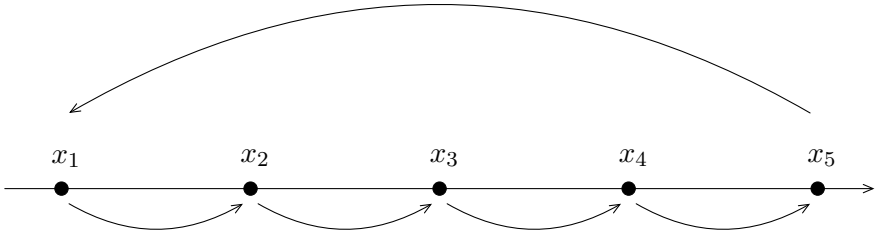
**Remarques :**

- Une transposition est un 2-cycle.
- On a prouvé que les éléments du cycle sont, dans l'ordre, $x_1, \sigma(x_1), \ldots, \sigma^{p-1}(x_1)$ donc :

$$\text{supp}(\sigma) = \{x_1; \sigma(x_1); \cdots; \sigma^{p-1}(x_1)\}$$

  L'élément $x_1$ servant de point de départ étant arbitraire (voir ci-dessous), une permutation est un cycle lorsqu'en partant d'un élément arbitraire du support et en appliquant successivement $\sigma$, on finit par revenir sur cet élément en passant par tous les autres éléments du support. Si, en revenant sur $x_1$, il reste des éléments du support qui n'ont pas été « visités », c'est que la permutation n'est pas un cycle mais la composée de plusieurs cycles : voir paragraphe II.1.

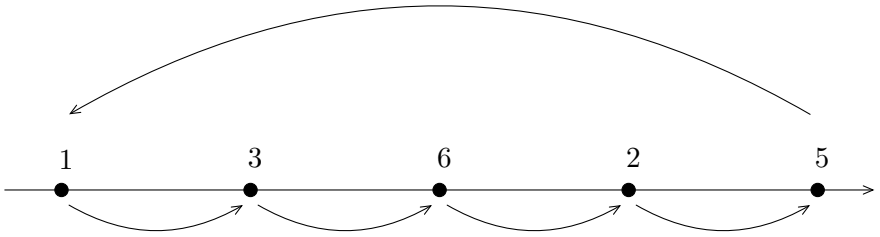
- Pour faire simple, un $p$-cycle est une permutation qui agit uniquement sur $p$ éléments (et qui laisse donc les autres invariants), et qui agit de manière circulaire : le premier sur le deuxième, le deuxième sur le troisième, etc. et le dernier sur le premier. Ci-dessous un 5-cycle :



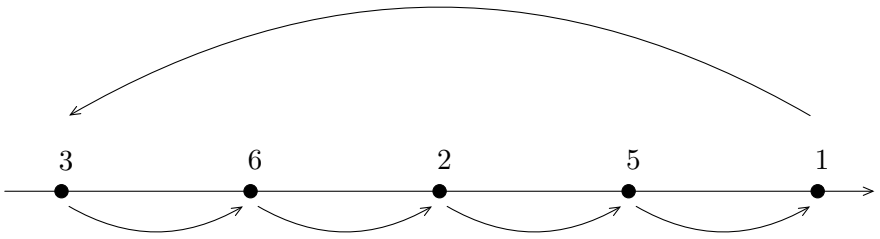

- Cela va sans dire mais je le dis quand même : quand on parle du premier, du deuxième etc., on ne parle pas des éléments rangés dans l'ordre croissant mais dans l'ordre dans lequel les éléments $x_1, x_2, \ldots, x_n$ sont numérotés, indicés i.e. envoyés les uns sur les autres par $\sigma$. Par exemple,

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

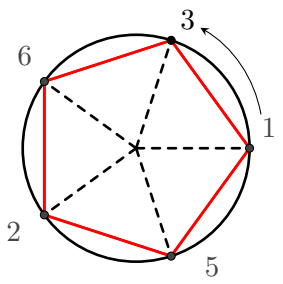
  est un 5-cycle qu'on peut représenter de la façon suivante :




- Le fait de choisir 1 comme point de départ est totalement arbitraire : on aurait tout aussi bien pu représenter ce cycle de la façon suivante :




- En fait, une représentation circulaire est beaucoup plus adaptée (c'est pour ça qu'on appelle ce type de permutation un cycle) :



- Certaines permutations ne sont pas des cycles ! Par exemple, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ n'est pas un cycle : $\sigma(1) \neq 1$ et $\sigma^2(1) = 1$ donc, si $\sigma$ est un cycle, c'est un 2-cycle de support $\{1; \sigma(1)\} = \{1; 4\}$ ce qui est absurde car 2 et 3 appartiennent aussi au support. Cependant, $\sigma$ est la composition des transpositions (ou 2-cycles) qui consistent à échanger 1 et 4 et qui consistent à échanger 2 et 3. Nous verrons dans le paragraphe II.2 qu'on peut généraliser cette notion.

**Notation :** Avec les notations de la définitions, on note $\sigma = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{p-1} & x_p \end{pmatrix}$. Plus précisément, cette notation signifie que $x_1$ est envoyé sur $x_2$, $x_2$ sur $x_3$ etc. $x_{p-1}$ sur $x_p$, $x_p$ sur $x_1$, tous les autres éléments de $[\![ 1 ; n ]\!]$ étant laissés invariants par $\sigma$.

**Exemple :** $\sigma = \begin{pmatrix} 1 & 5 & 9 \end{pmatrix}$ est la permutation envoyant 1 sur 5, 5 sur 9 et 9 sur 1 et les autres éléments invariants : c'est donc un 3-cycle.

**Remarques :**

- Cette notation permet de noter beaucoup plus simplement une transposition. Plus précisément, la transposition qui échange $i$ et $j$ est notée $\begin{pmatrix} i & j \end{pmatrix}$ (encore une fois, les autres éléments sont laissés invariants).

  En particulier, les transpositions $\begin{pmatrix} i & j \end{pmatrix}$ et $\begin{pmatrix} j & i \end{pmatrix}$ sont égales, même si on met en général le plus petit en premier dans l'écriture de la transposition.
- Quand on écrit une transposition ou un cycle, contrairement à la notations comme matrice à deux lignes vue au paragraphe I.2, le $n$ n'apparaît pas : on note de la même façon le 3-cycle $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ dans $S_5$ que dans $S_n$. C'est parce qu'en fait cela n'a aucune importance : tous les éléments n'apparaissant pas sont laissés fixes, donc cela n'est pas très grave s'ils n'apparaissent pas. Cependant, en pratique, on s'arrangera toujours pour que le $n$ soit sous-entendu.
- Une composée de $p$-cycles n'est pas forcément un $p$-cycle, et une puissance d'un $p$-cycle n'en est pas forcément un. Par exemple, si on note $\sigma = \begin{pmatrix} 2 & 5 & 3 & 1 & 7 & 9 \end{pmatrix}$ un 6-cycle de $S_9$, alors :

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

  Alors $\sigma^2$ n'est pas un 6-cycle car $\sigma(1) = 9, \sigma^2(1) = 5, \sigma^3(1) = 9$ donc, si c'est un cycle, c'est le 3-cycle $(1\,9\,5)$ ce qui est absurde puisque $\sigma^2(2) = 3$. Plus précisément, $\sigma$ est la composée de deux 3-cycles à supports disjoints :

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

- Il n'y a pas unicité de l'écriture d'un cycle : le cycle qui envoie $x_1$ sur $x_2$, …, $x_p$ sur $x_1$ peut s'écrire :

  $\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{p-1} & x_p \end{pmatrix}, \begin{pmatrix} x_2 & x_3 & \cdots & x_p & x_1 \end{pmatrix}, \begin{pmatrix} x_3 & x_4 & \cdots & x_p & x_1 & x_2 \end{pmatrix}, \ldots$

  L'élément qu'on met au début est totalement arbitraire (on est sur un cercle). Par exemple : $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix}$.

  Plus précisément, il y a $p$ façons d'écrire un même $p$-cycle : il ne faut donc pas oublier de diviser par $p$ si on veut connaître le nombre de $p$-cycles, cf. exercice 11.

# II Décomposition d'une permutation

L'idée (comme pour les polynômes ou les entiers) consiste à écrire une permutation comme « produit » de permutations plus simples : on va s'intéresser à l'écriture comme produit de cycles ou comme produit de transpositions, chacune ayant ses avantages et ses inconvénients.

On garde en tête que le produit est en fait la composition de bijections.

## II.1 Décomposition en produit de cycles à supports disjoints

**Théorème.** Toute permutation de $S_n$ peut s'écrire comme produit de cycles à supports disjoints. De plus, cette écriture est unique à l'ordre près des termes.

En effet, ces cycles étant à supports disjoints, ils commutent deux à deux (cf. paragraphe I.5) donc on peut écrire ces cycles dans l'ordre qu'on veut sans changer la permutation.

**Exemple :** La permutation de Papoum peut s'écrire $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}$ : le titre de ce numéro aurait donc pu être : Papoum et les produits de cycles à supports disjoints.

Démonstration. **Existence :** Notons $\sim$ la relation sur $[\![1\,;n]\!]$ définie par : $x \sim y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$. Montrons que c'est une relation d'équivalente.

- Soit $x \in [\![1\,;n]\!]$. Alors $\sigma^0 = \mathrm{Id}$ donc $\sigma^0(x) = x : x \sim x$, $\sim$ est réflexive.
- Soient $x$ et $y$ dans $[\![1\,;n]\!]$ tels que $x \sim y$. Il existe $k \in \mathbb{Z}$ tel que $y = \sigma^k(x)$, si bien que $x = \sigma^{-k}(y)$ (rappelons que $\sigma$ est une bijection). En d'autres termes, $y \sim x$ donc $\sim$ est symétrique.
- Soient $x, y, z$ dans $[\![1\,;n]\!]$ tels que $x \sim y$ et $y \sim z$ : il existe $k_1$ et $k_2$ tels que $y = \sigma^{k_1}(x)$ et $z = \sigma^{k_2}(y)$, si bien que $z = \sigma^{k_1}(\sigma^{k_2}(x)) = \sigma^{k_1+k_2}(x) : x \sim z$, $\sim$ est transitive.

Par conséquent, les classes d'équivalence forment une partition de $[\![1\,;n]\!]$. De plus, la classe d'équivalence de $x$ est un singleton si et seulement si $x$ est laissé invariant par $\sigma$. En effet, si $x$ n'est pas invariant, alors $\sigma(x) \neq x$ donc $\mathrm{cl}(x)$ a au moins deux éléments, et si $x$ est laissé invariant par $\sigma$, alors il est facile de prouver que tous les $\sigma^k$, pour $k \in \mathbb{Z}$, sont tous égaux à $x$, si bien que $\mathrm{cl}(x) = \{x\}$. En d'autres termes, les classes d'équivalences non réduites à un élément forment une partition du support de $\sigma$.

Les classes d'équivalence forment une partition donc deux classes d'équivalence sont soit disjointes soit confondues.

Notons $m$ le nombre de classes d'équivalences disjointes qui ne soient pas des singletons : notons-les $C_1, \dots, C_m$, c'est-à-dire que $\mathrm{supp}(\sigma) = C_1 \cup \cdots \cup C_m$, cette union étant disjointe.

Soit $i \in [\![1\,;m]\!]$, soit $x \in C_i$ si bien que $C_i = \mathrm{cl}(x)$. Par définition :

$$\mathrm{cl}(x) = \{\sigma^k(x) \,|\, k \in \mathbb{Z}\}$$

L'ensemble $[\![1\,;n]\!]$ étant fini, par principe des tiroirs, il existe $k_1 < k_2$ dans $\mathbb{N}$ tels que $\sigma^{k_1}(x) = \sigma^{k_2}(x)$. En composant par $\sigma^{-k_1}$, il vient : $\sigma^{k_2-k_1}(x) = x$. Notons dès lors $p = \min\{k \in \mathbb{N}^* \,|\, \sigma^k(x) = k\}$ et montrons que :

Un tel $p$ existe car minimum d'une partie non vide (car contient $k_2 - k_1$) de $\mathbb{N}$, et il est supérieur strict à 1 puisque $\sigma(x) \neq x$ car on a pris $x$ qui n'est pas dans le support.

$$\mathrm{cl}(x) = \{x; \sigma(x); \dots; \sigma^{p-1}(x)\}$$

L'inclusion $\{x; \sigma(x); \dots; \sigma^{p-1}(x)\} \subset \mathrm{cl}(x)$ est évidente par définition de $\mathrm{cl}(x)$. Réciproquement, soit $y \in \mathrm{cl}(x)$ : il existe donc $k \in \mathbb{Z}$ tel que $y = \sigma^k(x)$. Faisons la division euclidienne de $k$ par $p$ : il existe $q \in \mathbb{Z}$ et $r \in [\![0\,;p-1]\!]$ tels que $k = pq + r$ donc :

$$\begin{aligned} y &= \sigma^{pq+r}(x) \\ &= \sigma^r \circ \sigma^{pq}(x) \end{aligned}$$

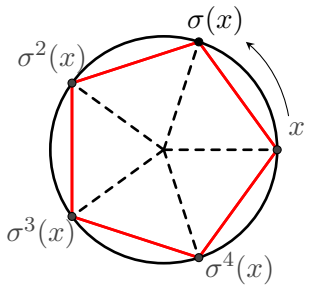
Or, $\sigma^p(x) = x$ donc

$$\begin{aligned} \sigma^{2p}(x) &= \sigma^p(\sigma^p(x)) \\ &= \sigma^p(x) \\ &= x \end{aligned}$$

Par une récurrence immédiate, $\sigma^{pq}(x) = x$ pour tout $q \in \mathbb{N}$. De plus, $\sigma^p(x) = x$ donc, en composant par $\sigma^{-p}$, $x = \sigma^{-p}(x)$ et, de même, pour tout $q \in \mathbb{N}$, $\sigma^{-pq}(x) = x$. Finalement, pour tout $q \in \mathbb{Z}$, qu'il soit positif ou négatif, on a $\sigma^{pq}(x) = x$ si bien que $y = \sigma^r(x)$. En d'autres termes, $y \in \{x; \sigma(x); \dots; \sigma^{p-1}(x)\}$, d'où l'inclusion réciproque, d'où l'égalité voulue.

Notons $\sigma_i = \begin{pmatrix}x & \sigma(x) & \cdots & \sigma^{p-1}(x)\end{pmatrix}$ le $p$-cycle formé par les éléments de $\mathrm{cl}(x) = C_i$.

Rappelons que $x$ est un élément quelconque de $C_i$.




Le support de $\sigma_i$ est $C_i$ : les cycles $\sigma_1, \dots, \sigma_m$ ont donc pour supports respectifs les classes d'équivalence $C_1, \dots, C_m$ qui sont disjointes donc ces cycles sont bien à supports disjoints. Il suffit donc de prouver que $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$ pour conclure.

Soit $x \in [\![ 1\,;\, n ]\!]$. Si $x \notin \text{supp}(\sigma)$ alors $\sigma(x) = x$ et $x$ n'appartient à aucune $C_i$ donc est laissé stable par tous les $\sigma_i$ donc :

$$\sigma_1 \circ \cdots \circ \sigma_n(x) = x = \sigma(x)$$

Supposons à présent que $x \in \text{supp}(\sigma)$. Soit $i \in [\![ 1\,;\, m ]\!]$ tel que $\text{cl}(x) = C_i$. D'après ce qui précède (on avait pris un élément quelconque de $C_i$), $\sigma_i(x) = \sigma(x)$ (rappelons que $\sigma_i = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{p-1}(x) \end{pmatrix}$). De plus, si $j \neq i$, alors $x$ et $\sigma(x)$ n'appartiennent pas à $C_j$ qui est le support de $\sigma_j$ donc $\sigma_j(x) = x$ et $\sigma_j(\sigma(x)) = \sigma(x)$. Par conséquent, quand on applique $\sigma_1 \circ \cdots \circ \sigma_n$ à $x$, toutes les permutations laissent invariants $x$ et $\sigma(x)$, sauf $\sigma_i$ qui envoie $x$ sur $\sigma(x)$. Finalement, $x$ est envoyé sur $\sigma(x)$ par l'un des cycles et les autres ne changent rien. Finalement :

$$\sigma_1 \circ \cdots \circ \sigma_n(x) = \sigma(x)$$

$x$ étant quelconque, $\sigma = \sigma_1 \circ \cdots \circ \sigma_n$. D'où l'existence.

**Unicité :** Supposons que $\sigma$ s'écrive comme un produit de cycles à supports disjoints notés $\tau_1, \dots, \tau_p$. On sait (cf. paragraphe I.5) que $\text{supp}(\sigma)$ est l'union disjointe des $\text{supp}(\tau_i)$. Soit $x \in \text{supp}(\sigma)$.

D'une part, il existe $j \in [\![ 1\,;\, n ]\!]$ tel que $x \in C_j$ (les classes d'équivalence vues plus haut) et on a alors vu qu'il existe $p \geqslant 1$ tel que $C_j = \{x; \sigma(x); \cdots; \sigma^{p-1}(x)\}$.

D'autre part, il existe $i \in [\![ 1\,;\, p ]\!]$ tel que $x \in \text{supp}(\tau_i)$. Tout d'abord :

$$\sigma = \tau_1 \circ \cdots \circ \tau_p$$

$x \in \text{supp}(\tau_i)$ et les supports sont disjoints donc $x \notin \text{supp}(\tau_j)$ pour tout $j \neq i$. Il en découle que $x$ est laissé stable par tous les $\tau_j$, $j \neq i$. Par conséquent, $\sigma(x) = \tau_i(x)$ car tous les autres laissent $x$ invariant. Il en découle que $\sigma(x) \in \text{supp}(\tau_i)$. On a donc montré que, si on a un élément de $\text{supp}(\tau_i)$, son image par $\tau_i$ est égale à $\sigma(x)$ et que cette image par $\sigma$ est encore dans le support : puisque $\sigma(x) \in \text{supp}(\tau_i)$, alors $\sigma^2(x) \in \tau_i(x)$. Par récurrence immédiate, $\sigma^k(x) \in \text{supp}(\tau_i)$ pour tout $k \in \mathbb{N}$. En particulier, $C_j \subset \text{supp}(\tau_i)$. En particulier, l'union des $C_j$ est incluse dans l'union des $\text{supp}(\tau_i)$. Or, dans les deux cas, cette union est disjointe et égale à $\text{supp}(\sigma)$. On en déduit qu'il y a autant d'éléments dans les deux unions, c'est-à-dire que $n = p$, et que, dans tous les cas, l'inclusion $C_j \subset \text{supp}(\tau_i)$ est en fait une égalité. On a déjà vu que, sur $\text{supp}(\tau_i)$, $\tau_i$ coïncide avec $\sigma$ et est un cycle, donc un cycle de longueur $p$ puisque son support est $C_j$. Finalement,

$$\tau_i = \begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{p-1}(x) \end{pmatrix} \qquad \square$$

c'est-à-dire que $\tau_i = \sigma_i$. D'où l'unicité. Ouf !

**Remarque :** La technicité de cette démonstration ne doit pas cacher l'idée générale qui est très simple : les différents cycles de cette écriture sont obtenus en prenant des éléments non équivalents, c'est-à-dire qu'on ne peut pas passer de l'un à l'autre en appliquant $\sigma$, et les cycles sont simplement obtenus en prenant leurs images successives par $\sigma$. Cela nous donne un algorithme constructif assez simple :

- On prend le premier élément $x$ du support de $\sigma$ (1 si 1 est dans le support, sinon 2 etc.).
- On prend ses images successives par $\sigma$. On finit par retomber sur $x$ lui-même : les images distinctes forment une classe d'équivalence, et cela nous donne un premier cycle.
- Si on a obtenu le support de $\sigma$, on arrête là, sinon on recommence avec un élément du support que nous n'avons pas encore « visité », cela donnera une autre classe d'équivalence, et donc un autre cycle.
- On recommence jusqu'à obtenir le support de $\sigma$ en entier. Cet algorithme termine puisque le support est un ensemble fini, et on retire au moins un élément à chaque fois, donc le cardinal des éléments restants diminue strictement donc il finit par être nul.

**Exemple :** Décomposons en produit de cycles à supports disjoints la permutation de $S_{15}$ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

Commençons par 1 qui est dans le support : ses images successives par $\sigma$ sont $4, 12$ et $5$ si bien qu'on a un premier cycle : $\begin{pmatrix} 1 & 4 & 12 & 5 \end{pmatrix}$. Le prochain élément du support que nous n'avons pas visité est 3 : ses images successives par $\sigma$ sont $8, 10, 9, 11, 13$ et on retombe sur 3 si bien qu'on a un deuxième cycle : $\begin{pmatrix} 3 & 8 & 10 & 9 & 11 & 13 \end{pmatrix}$. Ensuite, au tour de 6 : son image est 7 et on revient ensuite sur 6, cela donne un cycle (en fait une transposition) $\begin{pmatrix} 6 & 7 \end{pmatrix}$. On a pris tous les éléments du support, donc finalement :

$$\sigma = \begin{pmatrix} 1 & 4 & 12 & 5 \end{pmatrix} \begin{pmatrix} 3 & 8 & 10 & 9 & 11 & 13 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$$

**Remarque :** On a supposé sans le dire dans la démonstration que $\sigma$ n'était pas l'identité car on a construit les cycles à partir des éléments du support, sous-entendu : il est non vide. Le but d'une permutation étant d'être connue, ce résultat est inutile pour l'identité car on la connaît très bien, et donc on ne cherchera jamais à l'écrire sous une forme comme celle-ci. Néanmoins, on peut vouloir le faire tout de même, ne serait-ce que pour que le théorème soit correct car on a dit que « toute » permutation pouvait être écrite sous cette forme. Le résultat est encore valable pour l'identité en disant que Id est un produit... vide de cycles à supports disjoints.

## II.2 Décomposition en produit de transpositions

**Proposition.** Toute permutation de $S_n$ peut s'écrire comme produit de transpositions.

Là aussi, pour l'identité, ce résultat est toujours valable : soit on prend un produit vide, soit on remarque que $\mathrm{Id} = \sigma \circ \sigma$ avec $\sigma$ une transposition quelconque.

**Remarque :** Cette écriture n'est pas forcément unique, même à l'ordre près des termes. Par exemple :

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

De plus, les supports ne sont pas disjoints : les transpositions ne commutent pas !

Démonstration. Soit $\sigma$. Donnons deux démonstrations de ce résultat.

- **Première démonstration :** Puisque $\sigma$ est produit de cycles (à supports disjoints), alors il suffit de prouver le résultat pour un cycle : en effet, si $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$ avec les $\sigma_i$ des cycles, s'ils sont produits de transpositions, $\sigma$ l'est aussi.

  Il suffit ensuite de voir que, pour tous $a_1, \ldots, a_m$ deux à deux distincts :

  $$\begin{pmatrix} a_1 & a_2 & \ldots & a_m \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_2 & a_3 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}$$

  Notons en effet $\tau$ le produit de droite. Alors $\tau(a_1) = a_2$ puisque $a_1$ se trouve uniquement dans le support de la dernière transposition, donc est laissé invariant par les autres, et la dernière transposition l'envoie sur $a_2$. De plus, $\tau(a_2) = a_3 : a_2$ est laissé stable par toutes sauf les deux dernières, l'avant-dernière l'envoie sur $a_3$, et la dernière laisse $a_3$ invariant, et ainsi de suite : pour tout $k \leqslant m-1$, $a_k$ est laissé invariant par toutes les transpositions avant $\begin{pmatrix} a_k & a_{k+1} \end{pmatrix}$ qui l'envoie sur $a_{k+1}$ mais $a_{k+1}$ n'apparaît pas dans le support des transpositions qui suivent donc est laissé stable si bien que $\tau(a_k) = a_{k+1}$. Enfin, la dernière transposition envoie $a_m$ sur $a_{m-1}$, celle d'avant envoie $a_{m-1}$ sur $a_{m-2}$ etc. et la dernière envoie $a_2$ sur $a_1$ si bien que $\tau(a_m) = a_1$.

  En conclusion, $\sigma = \tau$ : tout cycle est produit de transpositions ce qui permet de conclure.

- **Deuxième démonstration :** Par récurrence sur $n \geqslant 2$. Le résultat est évident si $n = 2$ car $S_2$ contient l'identité et la permutation $\begin{pmatrix} 1 & 2 \end{pmatrix}$ donc tout élément de $S_2$ est produit de transpositions. Soit $n \geqslant 2$. Supposons le résultat vrai au rang $n$ et montrons qu'il est vrai au rang $n+1$. Soit donc $\sigma \in S_{n+1}$. Si $\sigma(n+1) = n+1$, posons $s = \sigma$. Supposons que $\sigma(n+1) \neq n+1$. Notons $\tau = \begin{pmatrix} n+1 & \sigma(n+1) \end{pmatrix}$. Alors

  $$\tau \circ \sigma(n+1) = n+1 \qquad \square$$

  Posons alors $s = \tau \circ \sigma$. Dans tous les cas, $s$ est une permutation de $[\![ 1 ; n+1 ]\!]$ avec $s(n+1) = n+1$ donc $s$ peut être vue comme une permutation de $[\![ 1 ; n ]\!]$ donc, par hypothèse de récurrence, est un produit de transpositions $\tau_1 \circ \cdots \circ \tau_p$. Il en découle que $s = \tau_1 \circ \cdots \circ \tau_p$. Si $\sigma(n+1) = n+1$, alors $s = \sigma = \tau_1 \circ \cdots \circ \tau_p$, et sinon, alors $s = \tau \circ \sigma$ donc, en composant par $\tau^{-1} = \tau$ à gauche, il vient : $\sigma = \tau \circ \tau_1 \circ \cdots \tau_p$ : dans tous les cas, $\sigma$ est un produit de transpositions, ce qui clôt la récurrence.

**Remarques :**

- En adaptant un peu la récurrence, on prouve que tout élément de $S_n$ s'écrit comme un produit d'au plus $n-1$ transpositions. On ne peut pas faire mieux : on peut montrer (cf. exercice 20) que les $n$-cycles ne peuvent pas s'écrire comme un produit de $n-2$ transpositions.
- Tout élément de $S_n$ peut s'écrire comme un produit de transpositions. On peut montrer (cf. exercice 19) que tout élément de $S_n$ peut s'écrire comme produit de transpositions du type $\begin{pmatrix} 1 & j \end{pmatrix}$, ou comme produit de transpositions du type $\begin{pmatrix} i & i+1 \end{pmatrix}$.
- Un des avantages de ces deux types de décomposition (comme produit de cycles ou comme produit de transpositions) est que si on veut prouver un résultat pour toutes les permutations, il suffit de le prouver pour les transpositions ou les cycles, et c'est souvent plus facile.
- Les deux démonstrations ci-dessus donnent un moyen simple de donner explicitement une telle écriture, i.e. une décomposition de $\sigma$ en produit de transpositions. Dans le cas où $\sigma$ est sous forme d'un produit de cycles à supports disjoints, on écrit chaque cycle comme produit de transpositions en prenant chaque élément de chaque cycle et son successeur. Par exemple, si on reprend $\sigma$ la permutation de $[\![ 1 ; 15 ]\!]$ ci-dessus :

  $$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 4 & 12 & 5 \end{pmatrix} \begin{pmatrix} 3 & 8 & 10 & 9 & 11 & 13 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 4 & 12 \end{pmatrix} \begin{pmatrix} 12 & 5 \end{pmatrix} \begin{pmatrix} 3 & 8 \end{pmatrix} \begin{pmatrix} 8 & 10 \end{pmatrix} \begin{pmatrix} 10 & 9 \end{pmatrix} \begin{pmatrix} 9 & 11 \end{pmatrix} \begin{pmatrix} 11 & 13 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix} \end{aligned}$$

Cette méthode est assez simple mais nécessite de connaître la décomposition de $\sigma$ en produit de cycles à supports disjoints. Celle-ci n'est pas très difficile à obtenir, mais on aimerait une méthode directe : c'est là que la seconde démonstration entre en oeuvre.

- Reprenons les notations de l'hérédité et supposons que $\sigma(n+1) \neq n+1$ et on pose $s = \tau \circ \sigma$ avec $\tau = \begin{pmatrix} n+1 & \sigma(n+1) \end{pmatrix}$ c'est-à-dire que $\tau$ échange $n+1$ et son image par $\sigma$. On pose alors $s = \tau \circ \sigma$ si bien que $\sigma = \tau \circ s$ avec $s$ la permutation obtenue à partir de $\sigma$ en intervertissant $n+1$ et $\sigma(n+1)$ dans la ligne du bas (voir ci-contre pour une démonstration propre).

  Ensuite, on applique l'hypothèse de récurrence à $s$ c'est-à-dire qu'on recommence : si $s(n) \neq n$, on compose par la permutation $t = \begin{pmatrix} n & s(n) \end{pmatrix}$ c'est-à-dire qu'on échange $n$ et son image, ce qui a pour effet de fixer $n$, et ensuite on recommence jusqu'à tomber sur l'identité (l'algorithme termine forcément puisque le dernier élément qui n'est pas fixe diminue de 1 à chaque étape donc il finira par ne plus y avoir de points fixes i.e. on tombera forcément sur l'identité). On aura alors $\sigma = \tau \circ t \circ \cdots$ un produit de transpositions. Illustrons par un exemple.

Notons $y$ l'unique antécédent de $n+1$ par $\sigma$. $s(n+1) = \tau(\sigma(n+1)) = n+1$ donc $s$ fixe $n+1$. De plus, $\tau(\sigma(y)) = \tau(n+1) = \sigma(n+1)$. Enfin, si $x \neq y, n+1$, alors $\sigma(x) \neq n+1, \sigma(n+1)$ par injectivité de $\sigma$ donc $\tau(\sigma(x)) = \sigma(x)$. En résumé : $s$ est la permutation obtenue à partir de $\sigma$ en intervertissant $n+1$ et $\sigma(n+1)$ dans la ligne du bas : en effet, $s(y) = \sigma(n+1)$ et $s(n+1) = n+1$ alors que pour $\sigma, \sigma(y) = n+1$ et $\sigma(n+1) = \sigma(n+1)$, et les autres éléments sont inchangés. Puisque $s = \tau \circ \sigma$ et que $\tau$ est son propre inverse, alors $\sigma = \tau \circ s$ : en d'autres termes, on met à gauche la permutation qui échange $n+1$ et $\sigma(n+1)$, et $s$ est la permutation obtenue en échangeant $n+1$ et son image sur la ligne du bas. On passe de

$$\begin{pmatrix} y & \dots & n+1 \\ n+1 & \dots & \sigma(n+1) \end{pmatrix}$$

à $\begin{pmatrix} n+1 & \sigma(n+1) \end{pmatrix} \circ$

$$\begin{pmatrix} y & \dots & n+1 \\ \sigma(n+1) & \dots & n+1 \end{pmatrix}$$

**Exemple :** Donnons encore la décomposition en produit de transpositions de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

Appliquons l'algorithme : on a $\sigma = \tau \circ s$ avec $\tau$ qui échange le dernier élément qui n'est pas fixé et son image (et donc $s$ est obtenu en intervertissant, dans la ligne du bas, cet élément et son image), et on recommence. Ici, le dernier élément non fixe est 13 et son image est 3 : on a donc

$$\sigma = \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 3 & 5 & 13 & 14 & 15 \end{pmatrix}$$

Ensuite, le dernier élément non fixé est 12 : on échange donc 12 et son image, à savoir 5 (on peut même arrêter d'écrire les derniers éléments : s'ils n'apparaissent pas, ils sont considérés comme fixes, ce qui est cohérent avec « l'identification » dont on parle ci-dessous).

$$\sigma = \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 2 & 8 & 5 & 1 & 7 & 6 & 10 & 11 & 9 & 3 \end{pmatrix}$$

Et ainsi de suite, on s'arrête quand tous les points sont fixes, quand on tombe sur l'identité. On trouve finalement :

$$\begin{aligned}
\sigma &= \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 3 & 11 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 5 & 1 & 7 & 6 & 10 & 3 & 9 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 3 & 11 \end{pmatrix} \begin{pmatrix} 9 & 10 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 8 & 5 & 1 & 7 & 6 & 9 & 3 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 3 & 11 \end{pmatrix} \begin{pmatrix} 9 & 10 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 8 & 5 & 1 & 7 & 6 & 3 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 3 & 11 \end{pmatrix} \begin{pmatrix} 9 & 10 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix} \begin{pmatrix} 3 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 1 & 7 & 6 \end{pmatrix}
\end{aligned}$$

et ainsi de suite jusqu'à obtenir :

$$\sigma = \begin{pmatrix} 3 & 13 \end{pmatrix} \begin{pmatrix} 5 & 12 \end{pmatrix} \begin{pmatrix} 3 & 11 \end{pmatrix} \begin{pmatrix} 9 & 10 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix} \begin{pmatrix} 3 & 8 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix} \begin{pmatrix} 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 4 \end{pmatrix}$$

On remarque une fois encore qu'il n'y a pas unicité.

**Remarque :** Dans la (deuxième) démonstration ci-dessus, nous avons écrit que $s$ fixait $n+1$ donc pouvait être considérée comme appartenant à $S_n$. Ce genre de raisonnement

Justification à retenir !

est assez fréquent (typiquement, comme ci-dessus, lors d'une hérédité) : par exemple, on pourra dire que les permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

sont égales, alors qu'elles n'appartiennent pas au même ensemble, mais cela se comprend bien car elles permutent uniquement les entiers $1, 2, 3, 4$, et ce de la même façon. Plus généralement, on identifie une permutation de $[\![ 1 ; n ]\!]$ avec la permutation de $[\![ 1 ; n+1 ]\!]$ qui coïncide avec elle sur $[\![ 1 ; n ]\!]$ et qui envoie $n+1$ sur $n+1$, c'est-à-dire qu'on identifie

$$\alpha = \begin{pmatrix} 1 & \dots & n \\ \alpha(1) & \dots & \alpha(n) \end{pmatrix}$$

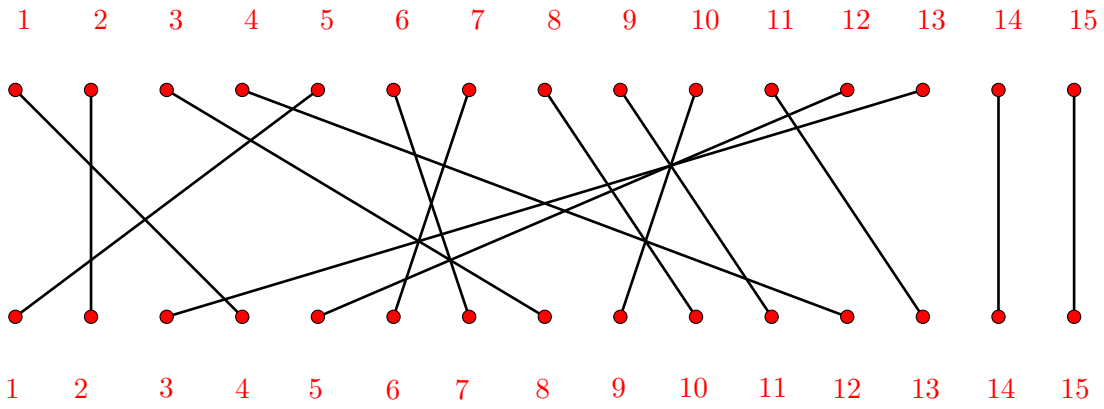
et

$$\alpha' = \begin{pmatrix} 1 & \dots & n & n+1 \\ \alpha(1) & \dots & \alpha(n) & n+1 \end{pmatrix}$$

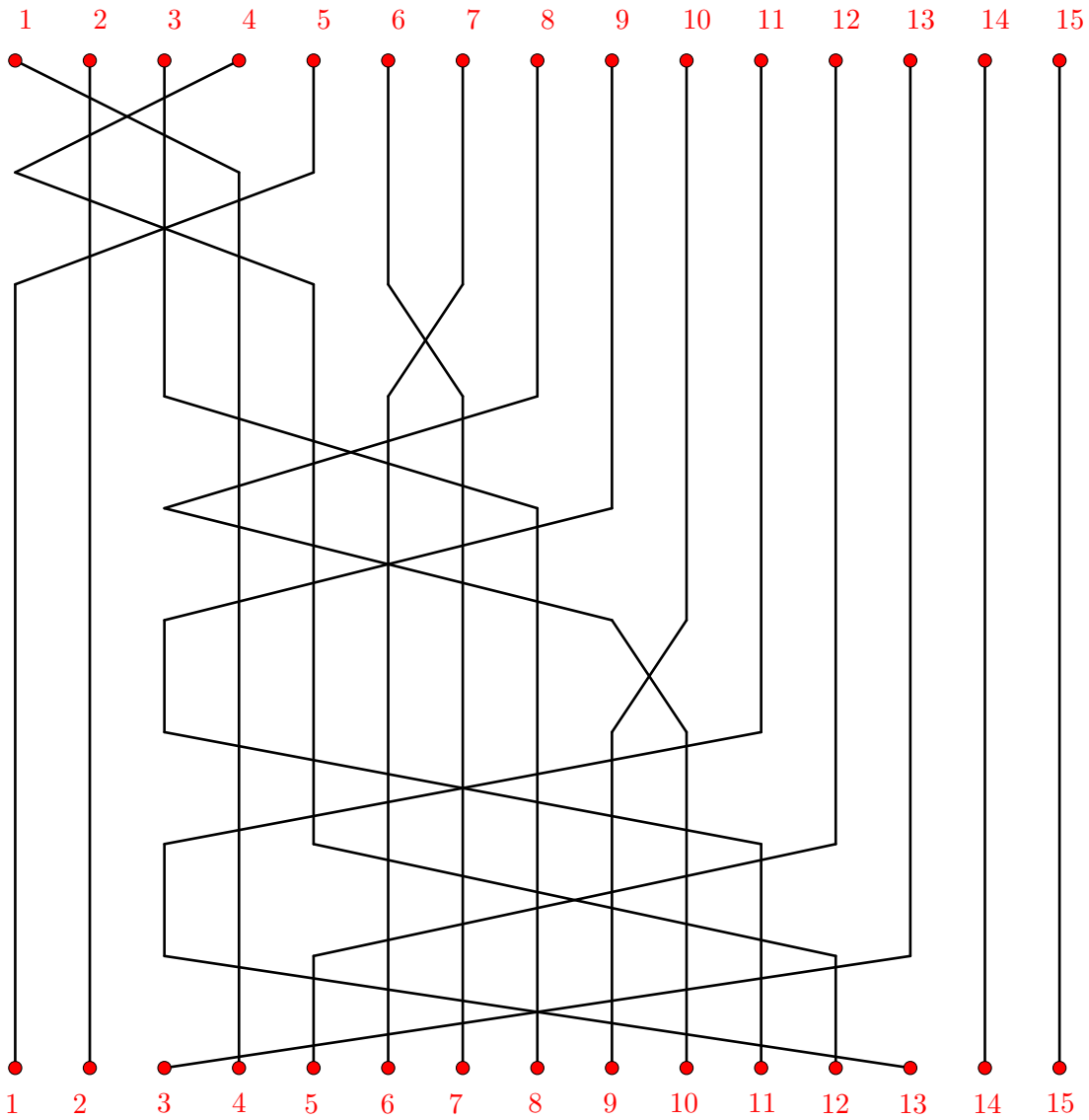
Ce ne sont pas des éléments du même ensemble (la première appartient à $S_n$ et la deuxième à $S_{n+1}$) mais cet abus de langage se comprend assez bien, et il peut être justifié tout à fait rigoureusement en prouvant (ce qui est immédiat) que la fonction qui va de $S_n$ dans $S_{n+1}$ et qui à une permutation $\alpha$ associe $\alpha'$ définie comme ci-dessus est injective (on dit que $S_n$ s'injecte dans $S_{n+1}$, ce qu'on note $S_n \hookrightarrow S_{n+1}$) donc est un isomorphisme entre $S_n$ et son image, c'est-à-dire entre $S_n$ et l'ensemble des permutations de $[\![ 1 ; n+1 ]\!]$ qui laissent $n+1$ invariants, et comme au chapitre 18, deux groupes isomorphes peuvent être considérés comme étant « le même » groupe (donc on peut dire que $S_{n+1}$ contient « une copie conforme de $S_n$ »), et donc on peut identifier leurs éléments.

## III Signature

**Remarque :** On peut (c'est rare) représenter une permutation comme une tresse, c'est-à-dire qu'on relie par des traits chaque élément de $[\![ 1 ; n ]\!]$ (en haut) à son image (en bas). Ci-dessous la permutation de $S_{15}$ vue au paragraphe précédent.

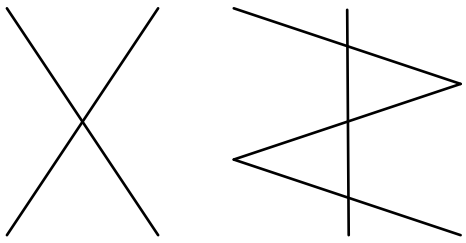



Si on écrit $\sigma$ comme un produit de transpositions, on peut l'écrire comme une succession de tresses où l'on échange à chaque fois deux fils. Ci-dessous la deuxième écriture de cette permutation comme produit de transpositions (on n'oublie pas qu'on va de la droite vers la gauche) :




C'est tout l'intérêt de l'écriture comme un produit de transpositions : on met les éléments $[\![ 1 ; n ]\!]$ dans un ordre quelconque, et on y arrive en échangeant deux éléments, puis encore deux autres etc.

On cherche un moyen de savoir combien on a effectué d'échanges dans une permutation. En d'autres termes, on cherche combien on a effectué de transpositions dans une permutation. On l'a vu, il n'y a pas unicité des transpositions qui interviennent dans le produit du paragraphe précédent, ni même unicité de leur nombre (on a écrit une transposition comme un produit de trois transpositions) mais on peut montrer qu'il y a unicité de la parité du nombre de transpositions, ce qui est intuitif : il peut y avoir quelques « errements », quelques zigzags, mais on arrive toujours à bon port. Ci-dessous, on échange deux éléments : à gauche on les échange directement, à droite on se balade un peu mais on finit par les échanger, à gauche il y a un échange, à droite il y en a trois. À chaque fois un nombre impair !



Tout ça pour dire que les transpositions « rajoutées » sont compensées par d'autres si bien que la différence entre deux produits de transpositions qui donnent la même permutations est forcément un nombre pair. Nous le prouvons rigoureusement ci-dessous.

**Proposition/Définition.** Il existe un unique morphisme de groupe de $S_n$ dans $\{\pm 1\}$ qui envoie toutes les transpositions sur $-1$. Ce morphisme est noté $\varepsilon$, il est appelé signature et il est défini par :

$$\varepsilon : \begin{cases} S_n & \to & \{\pm 1\} \\ \sigma & \mapsto & \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{cases}$$

Rappelons que $\{\pm 1\}$ est un groupe à deux éléments quand on le munit de la multiplication (il est alors isomorphe à $\mathbb{Z}/2\mathbb{Z}$, comme tout groupe à deux éléments d'ailleurs).

Démonstration. L'unicité est immédiate : si deux morphismes coïncident sur toutes les transpositions, ils sont égaux (sur $S_n$ tout entier) puisque toute permutation s'écrit comme produit de transpositions. Plus précisément, soient $f$ et $g$ deux morphismes de $S_n$ qui coïncident en toutes les transposition. Soit $\sigma \in S_n$. Il existe $\tau_1, \dots, \tau_p$ transpositions telles que

$$\sigma = \tau_1 \circ \cdots \circ \tau_p$$

$f$ et $g$ étant des morphismes qui coïncident en $\tau_1, \dots, \tau_p$ :

$$\begin{aligned} f(\sigma) &= f(\tau_1) \times \cdots \times f(\tau_p) \\ &= g(\tau_1) \times \cdots \times g(\tau_p) \\ &= g(\tau_1 \circ \cdots \circ \tau_p) \\ &= g(\sigma) \end{aligned}$$

c'est-à-dire que $f = g$. D'où l'unicité. Prouvons à présent l'existence. Prouvons que

$$\varepsilon : \begin{cases} S_n & \to & \{\pm 1\} \\ \sigma & \mapsto & \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{cases}$$

Plus fort : la signature est même l'unique morphisme non trivial (c'est-à-dire non constant égal à 1) de $S_n$ dans $\mathbb{C}^*$ : cf. exercice 18.

Montrons que $\varepsilon$ convient.

- Soit $\sigma \in S_n$. Tout d'abord :

$$\begin{aligned} \varepsilon(\sigma)^2 &= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \times \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \times \prod_{1 \leqslant j < i \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \prod_{1 \leqslant i \neq j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

Indices muets.

Or, $\sigma$ est une bijection donc, au numérateur, on a le produit de tous les $a - b$ possibles avec $a \neq b$, et aussi au dénominateur (les indices sont muets). En d'autres termes, $\varepsilon(\sigma)^2 = 1$ : $\varepsilon$ est bien à valeurs dans $\{\pm 1\}$.

- Soient $\sigma_1$ et $\sigma_2$ appartenant à $S_n$. Montrons que $\varepsilon(\sigma_1\circ\sigma_2) = \varepsilon(\sigma_1)\times\varepsilon(\sigma_2)$ (c'est-à-dire que $\varepsilon$ est bien un morphisme de groupes). Tout d'abord :

$$\begin{aligned}
\varepsilon(\sigma_1\circ\sigma_2) &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{i-j} \\
&= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} \times \frac{\sigma_2(i)-\sigma_2(j)}{i-j} \\
&= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} \times \prod_{1\leqslant i<j\leqslant n} \frac{\sigma_2(i)-\sigma_2(j)}{i-j} \\
&= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} \times \varepsilon(\sigma_2)
\end{aligned}$$

Les dénominateurs sont non nuls puisque $\sigma_2$ est injective.

Il suffit donc de prouver que le premier produit est égal à $\varepsilon(\sigma_1)$. $\sigma_2$ étant bijective, en faisant les changements d'indices $u=\sigma_2(i)$ et $v=\sigma_2(j)$, on obtient :

$$\prod_{1\leqslant i<j\leqslant n} \frac{\sigma_1\circ\sigma_2(i)-\sigma_1\circ\sigma_2(j)}{\sigma_2(i)-\sigma_2(j)} = \prod_{1\leqslant \sigma_2^{-1}(u)<\sigma_2^{-1}(v)\leqslant n} \frac{\sigma_1(u)-\sigma_1(v)}{u-v}$$

Le problème est qu'on n'a pas forcément $u<v$. L'avantage est que cela n'a aucune importance ! En effet, si $u<v$, alors c'est bon, et si $v<u$, le terme du produit est égal à

$$\frac{\sigma_1(u)-\sigma_1(v)}{u-v} = \frac{\sigma_1(v)-\sigma_1(u)}{v-u}$$

et l'indice est muet donc on peut très bien échanger les noms de $u$ et $v$. En d'autres termes, que $u$ soit strictement inférieur à $v$ ou le contraire (dans ce cas il suffit d'échanger les deux lettres ce qui ne change pas la valeur du quotient), le produit ci-dessus est en fait le produit de tous les termes de la forme

Penser à truc < machin.

$$\frac{\sigma_1(u)-\sigma_1(v)}{u-v}$$

avec $u<v$, c'est-à-dire que ce produit est bien égal à $\varepsilon(\sigma_1)$.

- Soit $\tau$ une transposition. Montrons enfin que $\varepsilon(\tau)=-1$. Notons $\tau = \begin{pmatrix} a & b \end{pmatrix}$ avec $a<b$. Il suffit d'examiner tous les termes du produit. Rappelons que $\tau(a)=b, \tau(b)=a$ et $\tau(x)=x$ si $x\neq a,b$.
  - ⋆ Si ni $i$ ni $j$ ne valent $a$ ou $b$, alors :

$$\frac{\tau(i)-\tau(j)}{i-j} = \frac{i-j}{i-j} = 1$$

  - ⋆ Si $i=a$ et $j\neq b$, alors :

On a aussi $a<j$.

$$\frac{\tau(i)-\tau(j)}{i-j} = \frac{b-j}{a-j}$$

  - ⋆ Si $j=a$ alors $i\neq a,b$ (puisque $i<a$) donc :

$$\frac{\tau(i)-\tau(j)}{i-j} = \frac{i-b}{i-a} = \frac{b-i}{a-i}$$

L'indice étant muet, ces deux derniers cas de figure donnent tous les quotients du type $\dfrac{b-k}{a-k}$ avec $k\neq a,b$ (le premier cas pour $k>a$ et le deuxième pour $k<a$).

⋆ Si $i = b$, alors $j \neq a, b$ (puisque $j > b$) donc :

$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{a - j}{b - j}$$

⋆ Si $j = b$ et $i \neq a$, alors :

On a aussi $i < b$.

$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{i - a}{i - b} = \frac{a - i}{b - i}$$

L'indice étant muet, ces deux cas de figure donnent tous les quotients du type $\frac{a-k}{b-k}$ avec $k \neq a, b$ (le premier cas pour $k > b$ et le deuxième pour $k < b$).

⋆ Enfin, si $i = a$ et $j = b$ :

$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{b - a}{a - b} = -1$$

En d'autres termes, parmi tous les termes constitutifs du produit qui définit $\varepsilon(\tau)$, on trouve :

⋆ Un seul terme égal à $-1$.

⋆ Des termes égaux à 1.

⋆ Le produit :

$$\prod_{k \neq a,b} \frac{b-k}{a-k} \times \prod_{k \neq a,b} \frac{a-k}{b-k} = 1$$

ce qui permet de conclure. Ouf ! □

**Corollaire.** Soit $\sigma \in S_n$. Si $\sigma$ est le produit de $N$ permutations, alors $\varepsilon(\sigma) = (-1)^N$.

**Remarques :**

- Pour la seule et unique fois de l'année, utilisons la définition de $\varepsilon$ pour calculer la signature de

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

Par définition de $\varepsilon$, on trouve :

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

et on trouve finalement $\varepsilon(\sigma) = -1$.

- C'est tout de même fastidieux... sans compter que c'était un cas tout de même assez simple : on a pris $n = 4$ ! C'est la raison pour laquelle, en pratique, on utilisera simplement le corollaire ci-dessus : quand on voudra donner la signature d'une permutation, on commencera par l'écrire comme un produit de transpositions, et ensuite le corollaire permettra de donner la signature directement. Par exemple, si

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

alors

$$\sigma = (3 \quad 13)(5 \quad 12)(3 \quad 11)(9 \quad 10)(3 \quad 9)(3 \quad 8)(6 \quad 7)(1 \quad 5)(1 \quad 4)$$

donc $\varepsilon(\sigma) = (-1)^9 = -1$. C'est tout de même plus rapide !

- On a vu que l'écriture en produit de transposition n'était pas du tout unique, mais la parité du nombre de transposition est fixe, comme on l'a vu plus haut, car la valeur de la signature d'une permutation est la même peu importe quelle écriture comme produit de transpositions on choisit.
- Pour faire simple (si on représente une permutation sous forme de tresse comme ci-dessus) : à chaque échange, on multiplie par $-1$.
- On peut aussi vouloir donner la signature d'une permutation écrite comme produit de cycles à supports disjoints. Pour cela, on dispose du résultat suivant :

**Proposition.** Soit $p \geqslant 2$ et soit $\sigma$ un $p$-cycle. Alors $\varepsilon(\sigma) = (-1)^{p-1}$.

Démonstration. On a vu au paragraphe II.2 (dans la première démonstration) qu'un $p$-cycle est produit de $p-1$ transpositions.