Groupe symétrique

« Si ces groupes ont chacun un nombre premier de permutations, l'équation sera résoluble par radicaux ; sinon non. »
E. Galois, lettre à Auguste Chevalier.

Nous avons déjà fait connaissance avec le groupe symétrique lors du dénombrement. Il s'agit simplement de tous les mélanges possibles sur un ensemble fini donné (imaginer un jeu de cartes).
Étudier ce groupe, revient à considérer la succession de plusieurs mélanges différents, ou tris successifs.
Nous verrons par exemple le résultat hautement intuitif selon lequel, on peut trier un jeu de cartes en réalisant simplement des permutations de cartes (échange de deux cartes). De nombreux tris en informatique s'appuient sur cette méthode (il faut tout de même savoir quelles cartes échanger et quand...). On dira que les permutations engendrent le groupe symétrique.

Remarque culturelle :
Le groupe symétrique a un rôle fondamental dans la théorie de Galois pour démontrer qu'il n'existe aucune formule générale qui donne les solutions des équations polynomiales de degré 5 sous forme de radicaux.

Avertissement : Ce chapitre ne propose pas une étude approfondie du groupe symétrique que l'on rencontre souvent en algèbre, mais il donne les quelques définitions nécessaires à la construction du déterminant en algèbre linéaire.

1 Définition

Définition 1.1 *(Permutation)*

Soit E un ensemble fini à n éléments.
Une **permutation de** E est une bijection de E sur lui-même.

Le **groupe symétrique d'ordre** n est l'ensemble des permutations de $[\![1, n]\!]$, muni de la loi de composition. On le note S_n.

On rappelle que le cardinal de S_n est $n!$.

Preuve

On a déjà vu que $(S_n, \circ)$ est un groupe. En effet,

- la composée de deux bijections est une bijection,
- toute bijection admet une réciproque (elle-même bijective),
- l'application identité est une bijection qui est l'élément neutre pour la composition,
- la composition est associative.

■

Remarque : On parlera souvent de produit de permutations au sens de la loi du groupe : il s'agit donc de compositions.

Exemple

1. Montrer que les groupes S_1 et S_2 sont commutatifs.
2. Montrer que pour $n \geqslant 3$, S_n est non commutatif.

Solution :

1. $S_1 = \{\mathrm{Id}\}$: il n'y a qu'un seul élément dans le groupe qui est évidemment commutatif.
   $S_2 = \{\mathrm{Id}, s\}$.
   En effet, pour permuter deux éléments, soit on les conserve, soit on les échange (permutation nommée ici s). Il n'y a pas d'autres solutions.
   Id et s commutent, donc S_2 est commutatif.
2. Soit $n \geqslant 3$.
   On commence par chercher un contre-exemple pour $n = 3$.
   Pour cela on peut définir les permutations
   $$\sigma_1 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} \quad \text{et } \sigma_2 : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases}.$$
   $\sigma_2 \circ \sigma_1(2) = \sigma_2(3) = 3$ mais $\sigma_1 \circ \sigma_2(2) = \sigma_1(1) = 2$.
   Donc $\sigma_2 \circ \sigma_1 \neq \sigma_1 \circ \sigma_2$ et S_3 est non commutatif.
   Pour généraliser à $n \geqslant 3$, on prend les permutations σ_1' et σ_2' dont les restrictions à $[\![1, 3]\!]$ sont égales à σ_1 et σ_2 et sinon égales à l'identité.

Une permutation $\sigma \in S_n$ peut se noter facilement sous la forme

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

Pour que cela représente bien une permutation, il faut et il suffit que chaque entier de $[\![1, n]\!]$ soit écrit une et une seule fois dans la seconde ligne.
Pour chercher l'image, on part simplement de la ligne du haut, vers celle du bas.
Pour obtenir l'inverse, on échange simplement les deux lignes (en réordonnant éventuellement).

Exemple

Pour σ représentée par

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

Il s'agit bien d'une permutation de S_5 car la seconde ligne contient une et une seule fois chaque entier de $[\![1, 5]\!]$.
$\sigma(1) = 2$, $\sigma(2) = 5$,...
On trouve alors facilement

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

De même, on réalise facilement la composition de deux permutations par la lecture successive des deux matrices[1].

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

Dans cet exemple, on voit que la composition n'est pas commutative :

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

Définition 1.2 *(Support)*

Soit $\sigma \in S_n$.
Un **point fixe** de σ est un entier $k \in [\![1, n]\!]$ tel que $\sigma(k) = k$.
Le **support** de σ est l'ensemble $[\![1, n]\!]$ privé des points fixes.

$$\text{supp}(\sigma) = \{k \in [\![1, n]\!],\ \sigma(k) \neq k\}.$$

Deux permutations sont **à supports disjoints**, ou simplement **disjointes** si leurs supports sont disjoints.

On remarque que l'ensemble des points fixes et le support sont complémentaires dans $[\![1, n]\!]$.

1. Le terme matrice désigne ici simplement un tableau de valeurs, sans lien avec l'algèbre linéaire.

Exemple

Le support de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$ est $\{1, 3, 4\}$.

Exemple

Montrer que σ et σ^{-1} ont le même support.
Solution :
Cela revient à montrer, par passage au complémentaires qu'ils ont les mêmes points fixes.
Si $\sigma(k) = k$, alors par application de σ^{-1}, $k = \sigma^{-1}(k)$.
Donc si k est un point fixe de σ, il l'est aussi de σ^{-1}.
L'ensemble des points fixes de σ est donc inclus dans l'ensemble des points fixes de σ^{-1}.
Par symétrie des rôles ($\sigma = \left(\sigma^{-1}\right)^{-1}$), on a également l'autre inclusion.
σ et σ^{-1} ont les mêmes points fixes, donc également le même support.
Le fait qu'une permutation et son inverse aient les mêmes points fixes se voit très bien avec les matrices : si k est au dessus de lui-même, alors, en échangeant les deux lignes, il est encore au dessus de lui-même.

Lemme 1.3

Soit $\sigma \in S_n$ et $k \in [\![1, n]\!]$.
Si $k \in \text{supp}(\sigma)$, alors $\sigma(k) \in \text{supp}(\sigma)$.

Quand on écrit la permutation avec la matrice, ce résultat est très visible.
Par exemple, on commence à écrire

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 4 & 3 & 6 & ? & \cdots & \end{pmatrix}$$

Ici, on a fait en sorte que 1 soit dans le support.
Voyons pourquoi $4 = \sigma(1)$ est également dans le support.
Pour remplir le « ? », on voit que le 4 est déjà utilisé dans la ligne du bas puisque c'est $\sigma(1)$, donc on ne peut le remettre une deuxième fois sans contredire la bijectivité.
Le « ? » ne peut donc pas être remplacé par 4 : $\sigma(4) \neq 4$ ce qui montre que $4 = \sigma(1)$ est aussi dans le support.

Preuve

Pour travailler plutôt avec les points fixes, on prend la contraposée.
Raisonnons par contraposée et supposons que $\sigma(k)$ ne soit pas dans le support de σ, alors c'est un point fixe et $\sigma(\sigma(k)) = \sigma(k)$.
Or σ est une bijection, donc on peut composer avec σ^{-1} et on trouve $\sigma(k) = k$ ce qui est absurde car $k \in \text{supp}(\sigma)$. ■

Remarque : on a aussi la réciproque, σ et σ^{-1} ayant le même support.

Propriété 1.4

Deux permutations à supports disjoints commutent.

Preuve

Soient σ_1 et σ_2 deux permutations de S_n à supports disjoints.
Soit $k \in [\![1, n]\!]$, montrons que $\sigma_1 \circ \sigma_2(k) = \sigma_2 \circ \sigma_1(k)$.

- si $k \in \text{supp}(\sigma_1)$, alors $k \notin \text{supp}(\sigma_2)$ donc $\sigma_2(k) = k$, donc $\sigma_1 \circ \sigma_2(k) = \sigma_1(k) \neq k$.
  Or, d'après le lemme $\sigma_1(k) \in \text{supp}(\sigma_1)$, donc $\sigma_1(k) \notin \text{supp}(\sigma_2)$, donc $\sigma_2(\sigma_1(k)) = \sigma_1(k)$.
  On a donc montré que
  $$\sigma_1 \circ \sigma_2(k) = \sigma_2 \circ \sigma_1(k).$$
- Si $k \notin \text{supp}(\sigma_1)$, alors
  - soit $k \in \text{supp}(\sigma_2)$ auquel cas l'argument précédent est valable en échangeant les rôles.
  - soit $k \notin \text{supp}(\sigma_2)$ et alors
  $$\sigma_1 \circ \sigma_2(k) = k = \sigma_2 \circ \sigma_1(k).$$

Donc $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. ■

⚠ Deux permutations peuvent commuter sans être à supports disjoints, par exemple σ et σ^{-1} (dans le cas d'une permutation différente de l'identité).

Définition 1.5 *(cycle)*

Soit $p \in [\![2, n]\!]$, un **cycle** de longueur p (ou p-cycle) est une permutation σ de S_n dont le support contient exactement p éléments

$$\text{supp}(\sigma) = \{x_1, x_2, \cdots, x_p\}$$

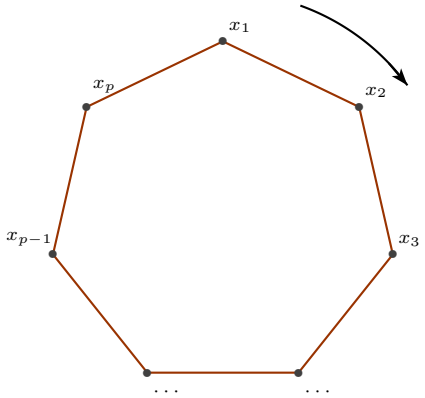
et tel que

$$\sigma(x_1) = x_2,\ \sigma(x_2) = x_3,\ \cdots,\ \sigma(x_p) = x_1.$$

Les x_i ne sont pas nécessairement classés par ordre croissant.
On note ce cycle : $(x_1\ x_2\ \cdots\ x_p)$.

On peut représenter les cycles sous forme de roues (d'où leur appellation), ce qui montre que le cycle n'a pas de « point de départ ».

$$(x_1\ x_2\ \cdots\ x_p) = (x_2\ \cdots\ x_p\ x_1).$$



⚠ $(1\ 3\ 2) \neq (1\ 2\ 3)$.

Exemple

Dans $[\![1, 5]\!]$, on peut considérer le 3-cycle : $(1\ 5\ 3)$. Sa matrice « complète » est alors $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$.

Exemple

Comment lit-on simplement la réciproque d'un cycle ?

Exemple

On considère la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$.
En lisant les éléments successivement, on voit apparaître naturellement un cycle : $1 \to 2 \to 5 \to 3 \to 1$.
Le dernier élément n'est pas dans le support, on peut donc écrire plus simplement : $\sigma = (1\ 2\ 5\ 3\ 1)$.

Exemple

On considère la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}$.
On obtient à présent $1 \to 4 \to 1$ et $2 \to 5 \to 3 \to 2$.
On peut alors écrire σ comme le produit (composition) des deux cycles à support disjoints : $\sigma = (1\ 4)(2\ 5\ 3)$.
L'ordre dans le produit est sans importance car les cycles sont à supports disjoints.
On voit bien qu'en fonction de l'élément dont on cherche l'image, s'il appartient au support de σ, alors il appartient à un seul cycle ce qui permet de lire directement son image en « négligeant » les autres cycles.

Ceci nous amène donc naturellement au théorème qui suit :

Théorème 1.6 *(Décomposition en cycle)*

Toute permutation se décompose de manière unique (à l'ordre près) en produit de cycles à supports disjoints.

Preuve *(Non exigible)*

- *Existence :*
  On remarque que deux éléments sont dans le même cycle si, et seulement s'ils peuvent s'obtenir l'un à partir de l'autre par application d'un certain nombre de fois σ.
  On considère donc la relation d'équivalence correspondante, dont les classes d'équivalence seront les supports des cycles :
  $$\forall (x, x') \in [\![1, n]\!]^2,\ x \sim x' \iff \exists k \in \mathbf{Z},\ x' = \sigma^k(x).$$
  On montre que c'est bien une relation d'équivalence :
  - *Réfexivité :* $\forall x \in [\![1, n]\!],\ x = \sigma^0(x)$.

– *Symétrie :* Si $x = \sigma^k(x')$, alors $x' = \sigma^{-k}(x)$.

– *Transitivité :* Si $x' = \sigma^k(x)$ et $x'' = \sigma^\ell(x')$, alors $x'' = \sigma^{k+\ell}(x)$.

Les classes d'équivalences forment donc une partition de $[\![1, n]\!]$.
⋆ Les classes à un seul élément correspondent aux points fixes.
⋆ Si une classe S_i contient au moins deux éléments, alors on choisit $x \in S_i$, un représentant quelconque.

– $\forall k \in \mathbf{Z}$, $\sigma^k(x) \in S_i$,

– réciproquement, si $x' \in S_i$, alors $x' \sim x$, donc il existe $k \in \mathbf{Z}$ tel que $x' = \sigma^k(x)$.

On a donc

$$S_i = \left\{\sigma^k(x),\ k \in \mathbf{Z}\right\}.$$

Comme cette classe d'équivalence contient un nombre fini d'éléments,
il existe $(k, \ell) \in \mathbf{Z}^2$ avec $k > \ell$ tel que $\sigma^k(x) = \sigma^\ell(x)$ donc $\sigma^{k-\ell}(x) = x$.

Si on considère donc $\left\{k \in \mathbf{N}^*,\ \sigma^k(x) = x\right\}$, alors cet ensemble forme une partie non vide de $\mathbf{N}^*$, donc admet un plus petit élément. Notons le p.

$$p = \min\left\{k \in \mathbf{N}^*,\ \sigma^k(x) = x\right\}.$$

Montrons que $c_i = \left(x\ \sigma(x)\ \cdots\ \sigma^{p-1}(x)\right)$ et un cycle tel que $S_i = \text{supp}(c_i)$.

– *C'est un cycle :*
Montrons que $x, \sigma(x), \cdots, \sigma^{p-1}(x)$ sont deux à deux distincts.
Si par l'absurde il existait $i < j$ dans $[\![0, p-1]\!]$ tels que $\sigma^i(x) = \sigma^j(x)$, alors on aurait $\sigma^{j-i}(x) = x$ avec $j - i \in [\![1, p-1]\!]$ ce qui contredirait la minimalité de p.
De plus, on a bien $\sigma \circ \sigma^{p-1}(x) = \sigma^p(x) = x$.
Donc $\left(x\ \sigma(x)\ \cdots\ \sigma^{p-1}(x)\right)$. forme bien un cycle.

– Soit $x' \in S_i$, alors il existe $k \in \mathbf{Z}$ tel que $x' = \sigma^k(x)$.
On réalise la division euclidienne de k par p et on trouve $k = pq + r$ avec $0 \leqslant r \leqslant p-1$.
Donc $x' = \sigma^{pq+r}(x) = \sigma^r\left((\sigma^p)^q(x)\right)$.
Or, on a vu que $\sigma^p(x) = x$, donc $\sigma^{pq}(x) = x$ donc $x' = \sigma^r(x)$.
Et comme $r \in [\![0, p-1]\!]$, $x' \in \left(x\ \sigma(x)\ \cdots\ \sigma^{p-1}(x)\right)$.

Comme tout élément appartient à une classe d'équivalence, on obtient alors

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_q$$

avec $c_1, c_2 \cdots, c_q$ les supports des cycles correspondant aux classes d'équivalence ayant au moins deux éléments.
Ces cycles étant à support disjoints, ils commutent entre eux et l'ordre est sans importance.

- *Unicité :*
Supposons deux décompositions pour σ : $c_1 c_2 .. c_p = c'_1 c'_2 \cdots c'_q$.
On a alors

$$\text{supp}(\sigma) = \bigsqcup_{i=1}^{p} \text{supp}(c_i) = \bigsqcup_{j=1}^{q} \text{supp}(c'_j).$$

Et ces unions sont disjointes.
Pour $i = 1$, on pose $x \in \text{supp}(c_i)$ et quitte à réordonner les c'_j, on peut dire que $x \in c'_1$.
D'après le lemme 1.3, on a par récurrence immédiate que pour tout $k \in \mathbf{N}$, $c_1^k(x) \in \text{supp}(c'_1)$.
Donc $\text{supp}(c_1) \subset \text{supp}(c'_1)$.
Par symétrie, on a également l'autre inclusion, donc $\text{supp}(c_1) = \text{supp}(c'_1)$.
On obtient donc que $c_i = \sigma_{|\text{supp}(c_i)} = \sigma_{|\text{supp}(c'_i)} = c'_i$ donc les cycles sont égaux.
On fait de même pour tous les supports, et on obtient donc l'égalité deux à deux.
En particulier $p = q$.

■

Définition 1.7 *(transposition)*

Une **transposition**[2] est un cycle de longueur 2.

Théorème 1.8

Les transposition engendrent S_n.
Autrement dit : toute permutation peut s'écrire comme produit de transpositions.

Remarque : on n'a plus l'unicité.

Preuve

D'après le théorème précédent, il suffit de le montrer pour les cycles.
On remarque simplement que

$$(x_1\ x_2\ \cdots\ x_p) = (x_1\ x_2)\,(x_2\ x_3)\cdots(x_{p-1}\ x_p).$$

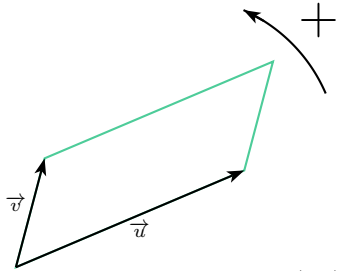
⚠ L'ordre est important. ■

2 Signature

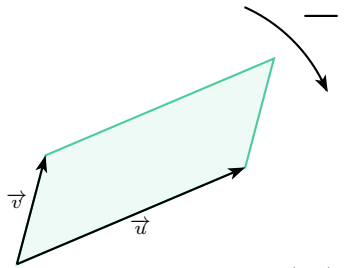
Le but de la signature est de compter le nombre de changements d'ordre entre les éléments.
Par exemple, dans une transposition, on échange l'ordre entre deux éléments ce qui donnera une signature de -1. Si on échange à nouveau l'ordre de deux éléments on retrouvera une signature de 1.
La signature sera donc $\varepsilon(\sigma) = (-1)^k$ avec k le nombre de changements d'ordre.

Cette notion sera importante pour réaliser des calculs de surfaces algébriques. Ainsi, dans un parallélogramme, lorsqu'on échange l'ordre des deux vecteurs, la figure est retournée et l'aire algébrique est multipliée par -1.

2. Contrairement à l'usage courant, le cycle de longueur 2, ou bi-cycle, ne comporte qu'une seule roue.



Aire du parallélogramme orienté $\vec{u}$, $\vec{v}$



Aire du parallélogramme orienté $\vec{v}$, $\vec{u}$

La signature peut également être vue par le nombre de fils qui se croisent lorsque l'on écrit la matrice de la permutation (chaque croisement correspond à une inversion).

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

Ainsi, la signature de la permutation précédente est $(-1)^5 = -1$. On voit en effet que le premier cycle (1 2 3 4 5) présente 4 inversions, et le second (6 7) en présente une seule.

On sait que chaque permutation peut-être écrite comme produit de transpositions, l'idée est donc de définir la signature d'une transposition égale à -1 (il y a une inversion), et de déterminer ensuite le nombre de transpositions nécessaires pour réaliser la permutation de telle sorte que s'il faut un nombre pair de transpositions, la signature sera 1 et s'il en faut un nombre impair, la signature sera -1.
Plus généralement, si on compose deux permutations entre elles, la signature sera égale au produit des deux signatures.

Théorème 2.1 *(Signature)*

Il existe un unique morphisme de groupes $\varepsilon : (S_n, \circ) \to (\{-1, 1\}, \times)$ qui envoie toute transposition sur -1.

En d'autres termes :
Il existe une unique application $\varepsilon : S_n \mapsto \{-1, 1\}$ non constante telle que

- pour toute transposition $\tau \in S_n$, $\varepsilon(\tau) = -1$,
- pour toutes permutations $\sigma_1, \sigma_2 \in S_n$, $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$.

Cette unique application se nomme **signature.**

On peut montrer un résultat plus fort : la signature est le seul morphisme de groupes non constant de $(S_n, \circ)$ dans $(\mathbf{C}^*, \times)$.

Preuve *(Non exigible)*

- *Unicité :*
  Algébriquement, il suffit de voir que l'ensemble des permutations engendre S_n, donc si un tel morphisme existe, alors, il est unique[3].
  Pour les détails : deux applications vérifiant les conditions plus haut.
  Soit σ une permutation, alors on peut décomposer σ en produit de transpositions : $\sigma = \tau_1\tau_2\cdots\tau_p$.
  Par récurrence immédiate, on a donc
  $$\varepsilon(\sigma) = \prod_{i=1}^{p} \varepsilon(\tau_i) = \prod_{i=1}^{p} (-1) = (-1)^p.$$
  On voit que cette quantité est définie de manière unique, ce qui prouve bien l'unicité de la fonction.

- *Existence :*
  On remarque qu'introduire une permutation revient à échanger le signe entre i et j. Dans le cas d'une transposition σ, deux éléments $i \neq j$ restent dans le même ordre si $\frac{\sigma(j)-\sigma(i)}{j-i} = 1$ et sont inversés si $\frac{\sigma(j)-\sigma(i)}{j-i} = -1$.
  On obtient donc naturellement la parité du nombre de transpositions (inversions d'ordre) par le produit
  $$s(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,\,j\}\subset[\![1,\,n]\!]} \frac{\sigma(j)-\sigma(i)}{j-i}.$$
  Montrons que cette application s définie sur S_n vérifie les hypothèses du théorème.

  – Montrons qu'elle vaut -1 pour toute transposition.
  Soit τ une transposition de la forme (a, b) avec $a < b$. Alors
  $$s(\tau) = \prod_{i<j} \frac{\tau(j)-\tau(i)}{j-i}.$$
  On sépare le produit en plusieurs facteurs selon les indices :
  $$\begin{aligned} s(\tau) &= \frac{\sigma(b)-\sigma(a)}{b-a} \prod_{i\notin\{a,\,b\}} \frac{\tau(a)-\tau(i)}{a-i} \prod_{i\notin\{a,\,b\}} \frac{\tau(b)-\tau(i)}{b-i} \prod_{\substack{i,\,j,\\ i\notin\{a,\,b\},\\ j\notin\{a,\,b\}}} \frac{\tau(j)-\tau(i)}{j-i} \\ &= (-1)\left(\prod_{i\notin\{a,\,b\}} \frac{b-i}{a-i}\frac{a-i}{b-i}\right) \times 1 \\ &= -1. \end{aligned}$$

3. C'est le même argument qui assure que les images d'une famille génératrice d'un espace vectoriel donnent l'unicité pour une application linéaire ; mais pas nécessairement l'existence de l'application si la famille n'est pas libre.
La vérification de l'existence d'une telle application doit donc être vérifiée à part.

– Montrons qu'elle est compatible avec le produit.
Soient σ, σ' deux permutations.

$$\begin{aligned} s(\sigma\sigma') &= \prod_{i<j} \frac{\sigma\sigma'(j) - \sigma\sigma'(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma\sigma'(j) - \sigma\sigma'(i)}{\sigma'(j) - \sigma'(i)} \times \prod_{i<j} \frac{\sigma'(j) - \sigma'(i)}{j-i} \\ &= \prod_{i<j} \frac{\sigma(\sigma'(j)) - \sigma(\sigma'(i))}{\sigma'(j) - \sigma'(i)} \times s(\sigma'). \end{aligned}$$

Montrons que le premier produit est égal à $s(\sigma)$.
On remarque que pour $i < j$, en multipliant le numérateur et le dénominateur par -1 dans un facteur on obtient

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

L'ordre entre $\sigma'(j)$ et $\sigma'(i)$ n'a donc pas d'importance pour le produit.
Ainsi, par bijectivité de σ' on voit que les rapports $\dfrac{\sigma(\sigma'(j)) - \sigma(\sigma'(i))}{\sigma'(j) - \sigma'(i)}$ correspondent donc exactement aux rapports $\dfrac{\sigma(\ell) - \sigma(k)}{\ell - k}$ pour $k < \ell$ dans $[\![1, n]\!]$.
On retrouve donc l'expression de $s(\sigma)$. On a donc bien

$$s(\sigma\sigma') = s(\sigma)s(\sigma').$$

– Toute permutation s'écrit comme produit de transposition, donc son image par s s'écrit comme un produit de -1, donc s est à valeurs dans $\{-1, 1\}$.
– Enfin $s \neq \mathrm{Id}$ d'après l'image pour une transposition.

Donc $s = \varepsilon$ qui existe bien.

■

⚠ La décomposition d'une permutation en produit de transpositions n'est pas unique, par contre la signature nous montre que pour deux décompositions différentes, la parité du nombre de transpositions est préservée.

Définition 2.2 *(parité)*

Une permutation est dite paire si sa signature vaut 1 et elle est impaire sinon.

Exemple

Une transposition est impaire, l'identité est paire.

Exemple

L'ensemble des permutations paires de S_n forme un groupe (le groupe alterné). Il correspond au noyau du morphisme signature.

Propriété 2.3 *(Signature d'un cycle)*

La signature d'un cycle de longueur p est $(-1)^{p-1}$.

Remarque : On peut le voir avec les « fils qui se croisent. »

Preuve

Le cycle s'écrit

$$(x_1\ x_2\ \cdots\ x_p) = (x_1\ x_2)(x_2\ x_3)\cdots(x_{p-1}\ x_p).$$

Il y a donc $p-1$ transpositions pour décomposer le cycle, d'où la signature. ■