2- Signature d'une permutation:

Def: $\mathcal{S}(n) = \{ \sigma : \{1 - n\} \longrightarrow \{1, -, n\} \text{ bijectives} \}$.

- On appelle les éléments de $\mathcal{S}(n)$ des permutations.
- $(\mathcal{S}(n), \circ)$ est un groupe de cardinal $n!$.
- Pour $\sigma \in \mathcal{S}(n)$, on définit $Supp(\sigma) := \{ i \,/\, \sigma(i) \neq i \}$
- On note $\sigma = \begin{pmatrix} 1 & 2 & & n \\ \sigma(1), & \sigma(2), & \dots, & \sigma(n) \end{pmatrix}$
- Une transposition est une permutation de type échange de deux éléments. Elle s'écrit $\begin{pmatrix} 1 & 2 - i - j - n \\ 1 & 2 - j - i - n \end{pmatrix}$
- Un cycle est une permutation du type $i_1 \longrightarrow i_2 \longrightarrow i_3 \longrightarrow i_4 \dots \longrightarrow i_k \rightarrow i_1$.
  On la note $(i_1, -, i_k)$.
  k est la longueur du cycle.
  Une transposition est donc un cycle de longueur 2.

Lemme:
- $\sigma(Supp\, \sigma) = Supp(\sigma)$
- $Supp(\sigma^{-1}) = Supp\, \sigma$
- Si $Supp\, \sigma_1 \cap Supp\, \sigma_2 = \phi$ alors $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Preuve:
- Si $i \in Supp(\sigma)$: $\sigma(i) \neq i$. Comme σ est une bijection, σ est injective donc $\sigma(\sigma(i)) \neq \sigma(i)$ (sinon $\sigma(i)$ aurait deux antécédents différents i et $\sigma(i)$)
  Donc $\sigma(i) \in Supp(\sigma)$

  Donc $\sigma(Supp\, \sigma) \subset Supp\, \sigma$.
  Mais σ injective, $Supp\, \sigma$ est fini donc $\sigma(Supp\, \sigma) = Supp\, \sigma$.

- Si $i \in Supp\, \sigma$: $\sigma(i) \neq i$. On $\sigma^{-1}(\sigma(i)) = i$ donc $\sigma(i) \in Supp\, \sigma^{-1}$

  et $\sigma^{-1}(Supp\, \sigma^{-1}) = Supp\, \sigma^{-1}$ donc $i = \sigma^{-1}(\sigma(i)) \in Supp\, \sigma^{-1}$.

  Donc $Supp\, \sigma \subset Supp\, \sigma^{-1}$. Mais $(\sigma^{-1})^{-1} = \sigma$ Donc $Supp\, \sigma^{-1} \subset Supp\, \sigma$.

- Si $Supp\, \sigma_1 \cap Supp\, \sigma_2 = \phi$: Soit $i \in \{1, -, n\}$

  → Soit $i \in Supp\, \sigma_1$. Alors $\sigma_1(i) \in Supp\, \sigma_1$ et $\{i, \sigma_1(i)\} \cap Supp\, \sigma_2 = \phi$.

  Donc $\sigma_1 \circ \sigma_2(i) = \sigma_1(i) = \sigma_2 \circ \sigma_1(i)$.

  → Si $i \in Supp\, \sigma_2$, c'est pareil

  → Si $i \notin Supp\, \sigma_1 \cup Supp\, \sigma_2$: $\sigma_1 \circ \sigma_2(i) = \sigma_2(i) = i = \sigma_2 \circ \sigma_1(i)$

Finalement, $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ $\square$.

Theorem : Toute permutation se décompose en

① . Produits de cycles à supports disjoints

② . Produits de transpositions (à support non disjoint).

Preuve : ①

Exemple : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 6 & 1 \end{pmatrix}$. On a $1 \to 3 \to 5 \to 6 \to 1$
$2 \to 4 \to 2$

Donc $\sigma = (1\ 3\ 5\ 6) \circ (2\ 4)$

Preuve : On raisonne par récurrence sur le cardinal du support de σ.

H_j : " $\forall \sigma \in \mathfrak{S}(n)$, $\exists \tau_1, \dots, \tau_\ell$ cycles à supports disjoints inclus ds Supp σ tq $\sigma = \tau_1 \circ \dots \circ \tau_\ell$. "

- Si $\#\mathrm{Supp}\,\sigma = 0$ alors $\sigma = id$ OK : (H_0) vraie.
- Sinon : Soit $i_1 \in \mathrm{Supp}\,\sigma$. $i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} i_3 \to \dots$

→ Comme $\{1, \dots, n\}$ est fini, il existe $k \leq n$ tel que $i_k \xrightarrow{\sigma} \{i_1, \dots, i_{k-1}\}$. On prend k le premier comme ça, $k \neq 1$ puisque $\sigma(i_1) \neq i_1$.

→ Comme σ est injective, on doit avoir $\sigma(i_k) = i_1$.

En effet, sinon $\sigma(i_k) = i_j$ aurait 2 antécédents : i_k et i_{j-1}.

→ Donc $i_1 \xrightarrow{\sigma} i_2 \to \dots \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1$.

Soit alors $\tau_0 := (i_1, \dots, i_k)$ (cycle de longueur $k \geq 2$).

On a $\tau_0^{-1} \circ \sigma\,(i_1) = \tau^{-1}(i_2) = i_1 \dots$ Donc

$\mathrm{Supp}\,(\tau_0^{-1} \circ \sigma) \cap \{i_1, \dots, i_k\} = \emptyset$.

De plus si $i \notin \mathrm{Supp}\,\sigma$, $i \notin \mathrm{Supp}\,\tau_0^{-1}$ car $\mathrm{Supp}\,\tau_0^{-1} = \{i_1 \dots i_k\} \subset \mathrm{Supp}\,\sigma$.

Donc $\tau_0^{-1} \circ \sigma\,(i) = \tau_0^{-1}(i) = i$.

Donc finalement, $\mathrm{Supp}\,(\tau_0^{-1} \circ \sigma) \subset \mathrm{Supp}\,\sigma \setminus \{i_1 \dots i_k\} = \mathrm{Supp}\,\sigma \setminus \mathrm{Supp}\,\tau_0$

Donc $\#\,\mathrm{Supp}\,(\tau_0^{-1} \circ \sigma) < \#\,\mathrm{Supp}\,\sigma$.

Par hypothèse de récurrence, $\tau_0^{-1} \circ \sigma = \tau_1 \circ \dots \circ \tau_\ell$ où τ_i sont des cycles à supports disjoints inclus dans $\mathrm{Supp}\,(\tau_0^{-1} \circ \sigma)$.

Puisque $\mathrm{Supp}\,\tau_0^{-1} \circ \sigma \subset \mathrm{Supp}\,\sigma \setminus \mathrm{Supp}\,\tau$, $\mathrm{Supp}\,\tau_0 \cap \mathrm{Supp}\,\tau_i = \emptyset$.

Donc $\sigma = \tau_0 \circ \tau_1 \circ \dots \circ \tau_\ell$ où $\mathrm{Supp}\,\tau_i$ st disjoints, inclus ds $\mathrm{Supp}\,\sigma$. ☐

② Il suffit à présent de montrer que tout cycle est un produit de transpositions. On le démontre par récurrence sur la longueur du cycle. Soit σ un cycle.

→ Si $\ell(\sigma) = 2$: σ est une transposition.

→ Si $\ell(\sigma) > 2$: $\sigma = (i_1\ i_2\ i_3, \dots, i_k)$

Alors. $\mathrm{Supp}\, (i_1, i_2)\circ\sigma \subset \{i_2 \longrightarrow i_k\}$.

- $(i_1, i_2)\circ\sigma(i_1) = (i_1, i_2)\,(i_2) = i_1$
- $(i_1\ i_2)\circ\sigma(i_k) = (i_1\ i_2)\,(i_1) = i_2$
- $\forall j \neq 1, k$: $(i_1\ i_2)\circ\sigma\,(i_j) = (i_1\ i_2)\underbrace{(i_{j+1})}_{\notin\{i_1, i_2\}} = i_{j+1}$.

Donc $(i_1\ i_2)\circ\sigma = \underbrace{(i_2\ i_3\ \dots\ i_k)}_{\text{lgueur } = k-1 < k}$.

Par hypothèse de récurrence : $(i_1 i_2)\circ\sigma = \tau_1\circ\dots\circ\tau_\ell$, τ_i = transpositions.

Donc $\sigma = (i_1\ i_2)\circ\tau_1\circ\dots\circ\tau_\ell$ = produit de transpositions. □.

<u>Def (Signature d'une permutation)</u>: Soit $\sigma \in \mathfrak{S}(n)$. On définit sa signature par $$\varepsilon(\sigma) := \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\substack{i<j \\ i,j\in \mathrm{Supp}\,\sigma}} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

<u>Ex</u>: $\varepsilon(i\ j) = \frac{i-j}{j-i} = -1$. $\varepsilon(1, 2, 3) = \frac{3-2}{2-1}\ \frac{1-2}{3-1}\ \frac{1-3}{3-2} = 1$.

- Remarquons que $\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(i)-\sigma(j)}{i-j}$. Donc la condition $i<j$ n'est pas très pertinente. Introduisons alors
  $$\mathcal{P}_2^{\neq}(n) := \{\{i, j\},\ i, j \in \{1, \dots, n\},\ i \neq j\}.$$
  Ce sont les parties à 2 éléments différents de $\{1, \dots, n\}$.
  Alors si $\{i, j\} \in \mathcal{P}_2^{\neq}(n)$, on peut définir $\frac{\sigma(j)-\sigma(i)}{j-i}$ puisque cette valeur ne dépend pas de si on met i ou j en premier.
- Remarquons aussi que $\{\{i, j\},\ i<j\} = \mathcal{P}_2^{\neq}(n)$.

On obtient donc la formule alternative suivante :
$$\varepsilon(\sigma) = \prod_{\{i,j\}\in\mathcal{P}_2^{\neq}(n)} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Theoreme : ε est un morphisme de groupe de $(\mathfrak{S}(n),\circ)$ vers $(\{-1,1\},\times)$.

Preuve : . Montrons d'abord que $\varepsilon : (\mathfrak{S}(n),\circ) \longrightarrow (\mathbb{R}^*,\cdot)$ morphisme.

$\rightarrow \varepsilon(\sigma\circ\tau) = \prod_{\{i,j\}\in\mathcal{P}_2^*(n)} \frac{\sigma\circ\tau(j)-\sigma\circ\tau(i)}{j-i} = \prod_{\mathcal{P}_2^*(n)} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{\mathcal{P}_2^*(n)} \frac{\tau(j)-\tau(i)}{j-i}$

$= \varepsilon(\tau)\cdot \prod_{\{i,j\}\in\mathcal{P}_2^*(n)} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}$

Puisque τ est une bijection, $\tau^{\otimes 2} : \mathcal{P}_2^*(n) \longrightarrow \mathcal{P}_2^*(n)$
$\{i,j\} \longmapsto \{\tau(i),\tau(j)\}$

est une bijection (d'inverse $\{\tau^{-1}(k),\tau^{-1}(\ell)\}$).

Alors : $\varepsilon(\sigma) = \prod_{\{i,j\}\in\mathcal{P}_2^*(n)} \frac{\sigma(j)-\sigma(i)}{j-i}$

$= \prod_{\substack{\tau^{\otimes 2}(\{i,j\}) \\ \{i,j\}\in\mathcal{P}_2^*(n)}} \frac{\sigma(j)-\sigma(i)}{j-i}$

$= \prod_{\{i,j\}\in\mathcal{P}_2^*(n)} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}$

Finalement, $\varepsilon(\sigma\circ\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$.

$\rightarrow$ $\varepsilon(id) = 1$ evident.

$\rightarrow$ ε à valeurs ds $\mathbb{R}^*$ car si $j\neq i$, $\sigma(j)\neq\sigma(i)$ (injection).

Donc $\varepsilon : (\mathfrak{S}(n),\circ) \longrightarrow (\mathbb{R}^*,\cdot)$ morphisme de groupe.

$\rightarrow$ Finalement, on a vu que si τ est une transposition $\varepsilon(\tau)=-1$. Et que
$\forall\sigma$, $\exists\,\tau_1,\dots,\tau_\ell$ des transpositions telles que $\sigma = \tau_1\circ\dots\circ\tau_\ell$.

Donc $\varepsilon(\sigma) = \varepsilon(\tau_1\circ\dots\circ\tau_\ell) = \prod\varepsilon(\tau_i) = (-1)^\ell$.

Donc $\varepsilon : (\mathfrak{S}(n),\circ) \longrightarrow (\{-1,1\},\cdot)$ morphisme de groupe. $\square$

Corollaire : La decomposition de σ n'est pas unique mais la parité du nbre de transpositions dans ces décomposition est fixe.

Preuve : Si $\tau_1\circ\dots\circ\tau_\ell = \tau'_1\circ\dots\circ\tau'_{\ell'}$, On a

$(-1)^\ell = \varepsilon(\tau_1\circ\dots\circ\tau_\ell) = \varepsilon(\tau'_1\circ\dots\circ\tau'_{\ell'}) = (-1)^{\ell'}$

Donc $\ell = \ell'\ [2]$. $\square$

Exercices : $\rightarrow$ Decomposit° en $\times$ de cycles algorithique
$\rightarrow$ transposit°
$\rightarrow$ Calcul de la signature.

$\rightarrow$ Calcul de $(1\,2)(2\,3)(3\,4)\cdots(i-1,i)$.