Théorème :

Toute permutation σ de $\mathfrak{S}_n$ se décompose en un produit de cycles de supports disjoints.
De plus cette décomposition est unique à l'ordre près des facteurs.

Lemme :

Pour tout $\sigma \in \mathfrak{S}_n$ et tout $i \in \{1,2,...,n\}$ il existe $p \in \mathbb{N}^*$ tel que :
$i, \sigma(i), ..., \sigma^{p-1}(i)$ soient deux à deux distincts et $\sigma^p(i) = i$.

Démonstration du lemme :

L'application $\varphi : \mathbb{N} \to \{1,2,...,n\}$ définie par $\varphi(k) = \sigma^k(i)$ ne peut-être injective car $\mathbb{N}$ est un ensemble infini.

Par suite, $\exists k \neq \ell \in \mathbb{N}$ tel que $\sigma^k(i) = \sigma^\ell(i)$ et on peut supposer $k < \ell$.

On a alors $\sigma^{\ell-k}(i) = \sigma^{-k} \circ \sigma^\ell(i) = i$ avec $\ell - k \in \mathbb{N}^*$.

Considérons maintenant $A = \{q \in \mathbb{N}^* / \sigma^q(i) = i\}$.

D'après l'étude précédente on peut affirmer que A est une partie non vide de $\mathbb{N}^*$, elle possède donc un plus petit élément p.

Pour celui-ci on a $\sigma^p(i) = i$.

De plus les $i, \sigma(i), ..., \sigma^{p-1}(i)$ sont nécessairement deux à deux distincts.

En effet s'il existait $0 \leq k < \ell \leq p-1$ tels que $\sigma^k(i) = \sigma^\ell(i)$ alors on aurait $\sigma^{\ell-k}(i) = i$ avec $0 < \ell - k < p$.

Or ceci contredit la définition de p.

Le lemme est donc démontré.

Démonstration du théorème :

Existence :

Procédons par récurrence sur $n \geq 2$.

Pour $n = 2$, les permutations éléments de $\mathfrak{S}_2$ sont Id et $(1,2)$ ce qui permet de conclure.

Supposons l'existence établie au rang $n \geq 2$.

Soit $\sigma \in \mathfrak{S}_{n+1}$.

Si $\sigma(n+1) = n+1$.

Considérons la restriction σ' de σ à $\{1,2,...,n\}$.

σ' réalise une permutation de $\{1,2,...,n\}$ car σ est une permutation de $\{1,2,...,n+1\}$ qui laisse $n+1$ fixe.

En appliquant l'hypothèse de récurrence à σ' on peut décomposer cette dernière en produit de cycles de $\mathfrak{S}_n$.

Cette décomposition de σ' dans $\mathfrak{S}_n$ se prolonge en une décomposition de σ en cycles de $\mathfrak{S}_{n+1}$.

Si $\sigma(n+1) \neq n+1$.

Considérons $p \in \mathbb{N}^*$ tel que $n+1, \sigma(n+1), ..., \sigma^{p-1}(n+1)$ soient deux à deux distincts et $\sigma^p(n+1) = n+1$.

Formons le cycle $c = (n+1, \sigma(n+1), ..., \sigma^{p-1}(n+1))$.

La permutation $c^{-1} \circ \sigma$ laisse, par construction, invariants les éléments $n+1, \sigma(n+1), ..., \sigma^{p-1}(n+1)$.

Comme $n+1$ est invariant, on peut par l'étude précédente, décomposer $c^{-1} \circ \sigma$ en $c_1 \circ c_2 \circ ... \circ c_r$ produit de cycles de supports disjoints.

De plus les supports de $c_1, c_2, ..., c_r$ sont disjoints de $\{n+1, \sigma(n+1), \ldots, \sigma^{p-1}(n+1)\}$ car ces éléments sont invariants par $c^{-1} \circ \sigma$.

L'écriture $\sigma = c \circ c_1 \circ c_2 \circ ... \circ c_r$ apparaît alors comme étant une décomposition de c en produit de cycles de supports disjoints.

Récurrence établie

Unicité :

Supposons que σ présente deux décompositions de la forme voulue :

$\sigma = c_1 \circ c_2 \circ ... \circ c_r$ et $\sigma = d_1 \circ d_2 \circ ... \circ d_s$.

On peut supposer $r \geq s$.

Si $r = 0$ alors $s = 0$.

Sinon, considérons i un élément du support de c_r.

Par le lemme, il existe $p \in \mathbb{N}^*$ tel que $i, \sigma(i), ..., \sigma^{p-1}(i)$ soient deux à deux distincts et $\sigma^p(i) = i$.

Or $\sigma(i) = c_r(i), \sigma^2(i) = c_r^2(i), ..., \sigma^{p-1}(i) = c_r^{p-1}(i)$ et $\sigma^p(i) = c_r^p(i) = i$ ceci car les éléments $i, c_r(i), c_r^2(i), ..., c_r^{p-1}(i)$ évoluent dans le support du cycle c_r.

Par suite $c_r = (i, \sigma(i), \sigma^2(i), ..., \sigma^{p-1}(i))$.

Comme i est modifié par $\sigma = d_1 \circ d_2 \circ ... \circ d_s$, il existe t entre 1 et s tel que i appartient au support de d_t.

Quitte à réorganiser l'ordre de la décomposition $\sigma = d_1 \circ d_2 \circ ... \circ d_s$ on peut supposer $t = s$.

En suivant la même démarche que ci-dessus on obtient $d_s = (i, \sigma(i), \sigma^2(i), ..., \sigma^{p-1}(i))$ puis $d_s = c_r$.

Après simplification on obtient la relation $c_1 \circ c_2 \circ \ldots \circ c_{r-1} = d_1 \circ d_2 \circ \ldots \circ d_{s-1}$

Il suffit alors de réitérer ce processus pour conclure.

Théorème :

L'application signature est un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ sur $(\{1, -1\}, \times)$.

Démonstration :

Soit σ et σ' deux éléments de $\mathfrak{S}_n$.

Soit (i, j) un couple avec $1 \leq i < j \leq n$.

$\sigma' \circ \sigma$ réalise une inversion sur (i, j) si et seulement si :

σ réalise une inversion sur (i, j) et σ' ne réalise pas d'inversion sur $(\sigma(j), \sigma(i))$

ou σ ne réalise pas d'inversion sur (i, j) mais σ' en réalise une sur $(\sigma(i), \sigma(j))$.

En sommant $I(\sigma)$ et $I(\sigma')$ on dénombre les cas précédemment étudiés ainsi que deux fois les cas où il y a à la fois inversion sur (i, j) et sur $(\sigma(j), \sigma(i))$.

Par suite $I(\sigma' \circ \sigma)$ à même parité que $I(\sigma) + I(\sigma')$,

puis $\varepsilon(\sigma' \circ \sigma) = (-1)^{I(\sigma' \circ \sigma)} = (-1)^{I(\sigma) + I(\sigma')} = \varepsilon(\sigma')\varepsilon(\sigma)$.

Ainsi ε est un morphisme de groupes.