Définition 1. *Un groupe est un couple $(G,*)$ où G est un ensemble non vide muni d'une loi de composition interne* $* : \begin{array}{ccc} G\times G & \longrightarrow & G \\ (a,b) & \longmapsto & a*b \end{array}$ *satisfaisant les propriétés suivantes :*

1. *associativité :* $\forall (a,b,c)\in G^3, \quad (a*b)*c = a*(b*c)$,
2. *existence d'un neutre, que l'on notera* e *:* $\exists e\in G, \quad \forall g\in G, \quad g*e = e*g = g$,
3. *tout élément de* G *admet un inverse : pour tout* $g\in G$*, il existe* $h\in G$ *tel que* $g*h = h*g = e$*. On appelle alors* h *l'inverse de* g *dans* $(G,*)$ *et on le note* g^{-1}.

Le groupe $(G,*)$ *est dit commutatif ou abélien si :* $\forall (a,b)\in G^2, \quad a*b = b*a$.

Définition 2. *Soit* $n\in\mathbb{N}^*$*, on définit* $\mathfrak{S}_n$ *comme l'ensemble des bijections de* $[\![1;n]\!]$ *dans lui même. Un élément de* $\mathfrak{S}_n$ *est appelé une permutation.*

Proposition 1. *L'ensemble* $\mathfrak{S}_n$ *muni de la composition est un groupe, d'élément neutre l'identité. On l'appelle le groupe symétrique d'ordre* n*. Pour* $n\geq 3$*, le groupe* $(\mathfrak{S}_n,\circ)$ *n'est pas commutatif.*

Proposition 2. *Le groupe symétrique* $\mathfrak{S}_n$ *est de cardinal* $n!$.

Définition 3. *Un cycle est une permutation* $\sigma\in\mathfrak{S}_n$ *telle qu'il existe* $i_1,\dots,i_p\in[\![1;n]\!]$ *deux à deux distincts (avec* $2\leq p\leq n$*) tels que*

$$\sigma(i_1)=i_2, \quad \sigma(i_2)=i_3, \quad \dots, \quad \sigma(i_{p-1})=i_p, \quad \sigma(i_p)=i_1 \quad \text{et} \quad \forall i\in[\![1;n]\!]\backslash\{i_1,\dots,i_p\}, \quad \sigma(i)=i.$$

On note alors $\sigma=(i_1 i_2\dots i_p)$*. L'entier* p *est appelé la longueur du cycle* σ.

Définition 4. *Les cycles de longueur* 2 *sont appelés des transpositions. Une transposition* $\tau=(ij)$ *a pour effet d'échanger les éléments* i *et* j.

Définition 5. *Soit* $\sigma\in\mathfrak{S}_n$*. On définit le support de* σ *comme l'ensemble*

$$\mathrm{Supp}(\sigma)=\{i\in[\![1;n]\!]\mid\sigma(i)\neq i\}.$$

Proposition 3. *Deux permutations de* $\mathfrak{S}_n$ *à supports disjoints commutent.*

Théorème 1. *Toute permutation se décompose en produits de cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre près des termes.*

Théorème 2. *Toute permutation se décompose en un produit de transpositions.*

Définition 6. *Soit $\sigma \in \mathfrak{S}_n$ et (i,j) un couple tel que $1 \leq i < j \leq n$. On dit que σ réalise une inversion sur le couple (i,j) si $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre de couples (i,j) avec $1 \leq i < j \leq n$ sur lesquels σ réalise une inversion (aussi appelé nombre d'inversions de σ).*

Définition 7. *On appelle signature d'une permutation $\sigma \in \mathfrak{S}_n$ le réel $\varepsilon(\sigma) = (-1)^{I(\sigma)}$, autrement dit, si on désigne par* sgn *la fonction signe,*

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \operatorname{sgn}(\sigma(j) - \sigma(i)).$$

La signature définit une application $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1; 1\}$.

Proposition 4. *La signature d'une transposition vaut -1.*

Proposition 5. *Soit $\sigma \in \mathfrak{S}_n$, la signature de σ est donnée par*

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Proposition 6. *Soient $\sigma, \tau \in \mathfrak{S}_n$, alors $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \times \varepsilon(\tau)$.*

Corollaire 1.

1. *Pour tous $\sigma_1, \ldots, \sigma_p \in \mathfrak{S}_n$, $\varepsilon(\sigma_1 \circ \cdots \circ \sigma_p) = \varepsilon(\sigma_1) \times \cdots \times \varepsilon(\sigma_p)$.*
2. *Pour tout $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.*

Corollaire 2. *Soit c un cycle de longueur p, alors $\varepsilon(c) = (-1)^{p-1}$.*