Géométrie 1

École Centrale de Pékin

Cours de mathématiques du cycle préparatoire

6 septembre 2020

Table des matières

Chapitre 1 Le groupe symétrique

Table des matières du chapitre

1.1 Permutations

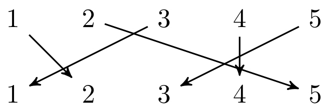
On étudie ici les permutations : j'ai n cartes numérotées dans l'ordre de 1 à n ; une permutation consiste à mélanger les cartes. Je change l'ordre des cartes, mais je garde toutes les cartes. C'est une opération très courante en mathématique et en informatique. Combien a-t-on de permutations ? Comment les distinguer ?
Nous utiliserons souvent dans la suite de ce cours des permutations. On a besoin de très peu de connaissance.

Définition 1
Soit $n \in \mathbb{N}^*$. Une ***permutation*** \置换\ *de $[\![1,n]\!]$ est une application σ de $[\![1,n]\!]$ vers $[\![1,n]\!]$ telle que si $k,\ k' \in [\![1,n]\!]$, $k \neq k'$, alors $\sigma(k) \neq \sigma(k')$. L'ensemble des permutations de $[\![1,n]\!]$ est appelé le* ***groupe symétrique*** *d'ordre n* \$n$阶对称群\ *et est noté S_n.*

On note
$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$
la permutation $\sigma \in S_n$ définie par : $\forall i \in [\![1,n]\!]$, $\sigma(i) = a_i$. Les a_i appartiennent à $[\![1,n]\!]$ et sont distincts deux à deux.

Exemple 2 —

1. *La figure ci-dessous représente une permutation $\sigma_1 \in S_5$.*



Cette permutation est la bijection $\sigma_1 : [\![1,5]\!] \to [\![1,5]\!]$ définie par
$$\sigma_1(1) = 2 \quad , \quad \sigma_1(2) = 5 \quad , \quad \sigma_1(3) = 1 \quad , \quad \sigma_1(4) = 4 \quad \text{et} \quad \sigma_1(5) = 3.$$
et notée $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$.

2. *L'application $[\![1,n]\!] \to [\![1,n]\!]$, $k \mapsto k$ s'appelle permutation identité et est notée $\mathrm{Id}_{[\![1,n]\!]}$ ou plus simplement* Id. *Par exemple,* $\mathrm{Id}_{[\![1,5]\!]} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

3. *L'ensemble $S_1 = \{\mathrm{Id}\}$, $S_2 = \{\mathrm{Id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$.*

Exercice 3 — *Décrire les éléments de S_3.*

PROPOSITION 4
L'ensemble S_n possède $n!$ éléments.

Preuve — On énumère toutes les permutations σ :

1) à 1 je peux associer n'importe quel élément $\sigma(1)$ de $[\![1, n]\!]$, il y a n possibilités.
ii) puis à 2 je peux associer n'importe quel élément de $[\![1, n]\!]$ sauf $\sigma(1)$, il y a $n-1$ possibilités.
$\vdots$
n) enfin à n je peux associer n'importe quel élément de $[\![1, n]\!]$ sauf $\sigma(1), \cdots, \sigma(n-1)$, il ne reste plus qu'une seule possibilité.

On en déduit que S_n contient $n \times (n-1) \times \cdots \times 1 = n!$ éléments. □

REMARQUE 5 — *Il résulte de la démonstration que pour tout $j \in [\![1, n]\!]$, il existe un unique $i \in [\![1, n]\!]$ tel que $\sigma(i) = j$.*

PROPOSITION 6
La composée de deux permutations de $[\![1, n]\!]$ est aussi une permutation de $[\![1, n]\!]$.

Preuve — Soit σ et σ' deux permutations de $[\![1, n]\!]$. Alors $\sigma \circ \sigma' : [\![1, n]\!] \to [\![1, n]\!]$, $k \mapsto \sigma(\sigma'(k))$. De plus si $k, l \in [\![1, n]\!]$ et $\sigma(\sigma'(k)) = \sigma(\sigma'(l))$, alors $\sigma'(k) = \sigma'(l)$ car σ est une permutation. Enfin, comme σ' est une permutation, on en déduit que $k = l$. Par contraposée, nous avons montré que si $k \neq l$, alors $\sigma(\sigma'(k)) \neq \sigma(\sigma'(l))$. □

EXEMPLE 7 — *Si*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} \quad \textit{et} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix},$$

alors

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \quad \textit{et} \quad \sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

Dans cet exemple, $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$: on dit que la composition n'est pas commutative.

DÉFINITION 8 (et proposition)
Soit $\sigma \in S_n$. Il existe une unique permutation notée σ^{-1} et appelée permutation réciproque telle que

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}.$$

Preuve — On définit la permutation σ^{-1} de la manière suivante : d'après la remarque 5, pour tout $j \in [\![1, n]\!]$, il existe un unique $i \in [\![1, n]\!]$, tel que $\sigma(i) = j$. On pose $\sigma^{-1}(j) = i$. Par définition, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$ et $\sigma^{-1}(j) = \sigma^{-1}(j')$ si et seulement $j = j'$. □

EXEMPLE 9 — *Par exemple,* $\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix}$.

DÉFINITION 10
Soient $n \in \mathbb{N}^*$ et une permutation $\sigma \in S_n$. L'ensemble des éléments k de $[\![1, n]\!]$ tels que $\sigma(k) \neq k$ est appelé le ***support*** *de la permutation σ. Si un élément x n'appartient pas au support de σ, alors $\sigma(x) = x$ et on dit que x est un élément* ***invariant*** *ou un* ***point fixe****.*

EXEMPLE 11 —

1. *Le support de la permutation σ_1 est $\{1, 2, 3, 5\}$ et le support de $\mathrm{Id}_{[\![1,5]\!]}$ est $\emptyset$.*
2. *Existe-t-il une permutation $\sigma \in S_n$ telle que le support de σ a un seul élément ?*

REMARQUE 12 — *Quand on représente une permutation, il suffit d'écrire les éléments du support : par exemple on peut écrire $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 5 \\ 2 & 5 & 1 & 3 \end{pmatrix}$. Il faut comprendre qu'une telle écriture ne permet pas de connaître la valeur de n telle que $\sigma_1 \in S_n$. On a certainement $n \geq 5$. On va en fait réduire encore l'écriture des permutations.*

Proposition 13
Si les supports de deux permutations $\sigma \in S_n$ et $\sigma' \in S_n$ sont disjoints, alors elles commutent : $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Preuve — Soient $A := \{a_1, \dots, a_p\}$ et $A' := \{a'_1, \dots, a'_{p'}\}$ les supports de σ et σ'. On suppose que $A \cap A' = \emptyset$.

Soit x appartenant à $[\![1, n]\!]$.

Si x appartient à A, alors $\sigma(x)$ appartient à A. D'où x et $\sigma(x)$ n'appartiennent pas à A'. Donc $\sigma \circ \sigma'(x) = \sigma(x) = \sigma' \circ \sigma(x)$.

Si x appartient à A', alors $\sigma(x)$ appartient à A'. D'où x et $\sigma(x)$ n'appartiennent pas à A. Donc $\sigma' \circ \sigma(x) = \sigma'(x) = \sigma \circ \sigma'(x)$.

Si x n'appartient pas à $A \cup A'$, alors $\sigma(x) = \sigma'(x) = x$. Donc $\sigma \circ \sigma'(x) = \sigma(x) = x = \sigma'(x) = \sigma' \circ \sigma(x)$. □

1.2 Transpositions

Définition 14
*Soit $n \in \mathbb{N}^*$. On dit qu'une permutation $\tau \in S_n$ est une **transposition** \对换\ s'il existe deux éléments distincts a et b de $[\![1, n]\!]$ tels que*

$$\tau(a) = b \quad , \quad \tau(b) = a \quad \text{et} \quad \forall x \notin \{a, b\},\ \tau(x) = x.$$

On la note alors $\tau = \begin{pmatrix} a & b \end{pmatrix}$.

La transposition $\tau = \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} b & a \end{pmatrix}$ échange les deux éléments a et b. Sa réciproque est elle-même : $\tau^{-1} = \tau$. Par exemple, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ est la transposition $\begin{pmatrix} 1 & 3 \end{pmatrix} \in S_4$.

Proposition 15
Soit $n \geq 2$. Toute permutation de $[\![1, n]\!]$ est la composée de transpositions.

Preuve — Par récurrence sur n : la propriété est vraie au rang $n = 2$ car toute permutation de $[\![1, 2]\!]$ est, ou bien une transposition, ou bien l'identité $\mathrm{Id}_{[\![1,2]\!]} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix}$.

Supposons que la propriété est vraie au rang n. Soit $\sigma \in S_{n+1}$:
- ou bien $\sigma(n+1) = n+1$. La restriction de σ à $[\![1, n]\!]$ appartient alors à S_n. D'où cette restriction est la composée de transpositions $\begin{pmatrix} a_i & a_j \end{pmatrix} \in S_n$. Donc σ est la composée des mêmes transpositions $\begin{pmatrix} a_i & a_j \end{pmatrix} \in S_{n+1}$.
- ou bien $\sigma(n+1) = p \leq n$. Alors la permutation $\sigma' = \begin{pmatrix} p & n+1 \end{pmatrix} \circ \sigma$ vérifie $\sigma'(n+1) = n+1$ et on vient de montrer qu'elle est composée de transpositions. Donc $\sigma = \begin{pmatrix} p & n+1 \end{pmatrix} \circ \sigma'$ est aussi composée de transpositions.

La propriété est donc vraie au rang $n+1$. □

Méthode 16 — *On décompose la permutation $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ en transpositions :*

$\sigma_3 = \begin{pmatrix} 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 5 \end{pmatrix}$ *car*

$$\begin{array}{cccccc|l}
1 & 2 & 3 & 4 & 5 & 6 & \\
 & & & & & & \downarrow (15) \\
5 & 2 & 3 & 4 & 1 & 6 & \\
 & & & & & & \downarrow (13) \\
 & & 1 & 4 & 3 & 6 & \\
 & & & & & & \downarrow (46) \\
 & & & 6 & 3 & 4 & \\
5 & 2 & 1 & 6 & 3 & 4 &
\end{array}$$

$\sigma_3 = \begin{pmatrix} 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 4 & 6 \end{pmatrix}$ *car*

$$\begin{array}{cccccc|l}
1 & 2 & 3 & 4 & 5 & 6 & \\
 & & & & & & \downarrow (46) \\
1 & 2 & 3 & 6 & 5 & 4 & \\
 & & & & & & \downarrow (35) \\
1 & 2 & 5 & & 3 & & \\
 & & & & & & \downarrow (15) \\
5 & & 1 & & & & \\
5 & 2 & 1 & 6 & 3 & 4 &
\end{array}$$

Cet exemple montre qu'une décomposition en transpositions n'est pas unique. Le nombre de transpositions n'est pas unique non plus car $\sigma_3 = \begin{pmatrix} 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix}$.

Remarque 17 — *Si on inverse l'ordre des transpositions qui composent une permutation σ, alors on obtient la permutation réciproque σ^{-1}. (Pourquoi ?) Par exemple : $\sigma_3 = \begin{pmatrix} 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 5 \end{pmatrix}$, d'où $\sigma_3^{-1} = \begin{pmatrix} 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 4 & 6 \end{pmatrix}$.*

1.3 Cycles

Définition 18

*Soient $n \geq 2$ et $p \in [\![2, n]\!]$. On dit qu'une permutation σ est un p-**cycle** \\p-轮换\\ ou un **cycle** s'il existe p éléments distincts deux à deux $a_1, \ldots, a_p$ de $[\![1, n]\!]$ tels que*

$$\begin{aligned} \forall x \notin \{a_1, \ldots, a_p\} \quad & \sigma(x) = x \\ \forall i \in [\![1, p-1]\!] \quad & \sigma(a_i) = a_{i+1} \\ & \sigma(a_p) = a_1. \end{aligned}$$

On note alors $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix}$.

$$\begin{tikzcd} a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_p \arrow[lll, bend left] \end{tikzcd}$$

Les 2-cycles sont les transpositions.

Si $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_{p-1} & a_p \end{pmatrix}$, alors $\sigma^{-1} = \begin{pmatrix} a_p & a_{p-1} & \ldots & a_2 & a_1 \end{pmatrix}$. La réciproque d'un p-cycle est donc aussi un p-cycle. Leur support est l'ensemble $\{a_1, \ldots, a_p\}$.

Remarque 19 — *Soient $n \in \mathbb{N}^*$ et une permutation $\sigma \in S_n$.*

1. *On note $\sigma^0 = \mathrm{Id}_{[\![1,n]\!]}$ et, pour tout $k \in \mathbb{N}^*$,*

$$\sigma^k = \underbrace{\sigma \circ \ldots \circ \sigma}_{k \text{ fois}} \quad \text{et} \quad \sigma^{-k} = \underbrace{\sigma^{-1} \circ \ldots \circ \sigma^{-1}}_{k \text{ fois}}.$$

2. *Si σ est un p-cycle $\begin{pmatrix} a_1 & a_2 & \ldots & a_{p-1} & a_p \end{pmatrix}$, alors $\forall k \in [\![2, p]\!]$, $a_k = \sigma^{k-1}(a_1)$.*
   D'où $\sigma = \begin{pmatrix} a_1 & \sigma(a_1) & \cdots & \sigma^{p-1}(a_1) \end{pmatrix}$.
3. *Réciproquement, soit $x \in [\![1, n]\!]$:*
   - *ou bien $\sigma(x) = x$;*
   - *ou bien il existe $p \in [\![2, n]\!]$ tel que $\sigma^p(x) = x$ et $\begin{pmatrix} x & \cdots & \sigma^{p-1}(x) \end{pmatrix}$ est un p-cycle.*

   Preuve — *Si $\sigma(x) \neq x$, alors l'ensemble $\{\sigma^k(x), \quad 0 \leq k \leq n\}$ contient au plus n éléments car il est inclus dans $[\![1, n]\!]$. Il existe donc $(i, j) \in [\![0, n]\!]^2$ tel que $i < j$ et $\sigma^i(x) = \sigma^j(x)$. D'où $\sigma^{j-i}(x) = x$. Soit alors p le plus petit entier non nul tel que $\sigma^p(x) = x$. Les p entiers $x, \sigma(x), \cdots, \sigma^{p-1}(x)$ sont distincts deux à deux (Pourquoi ?).* □

Nous dirons que deux cycles sont disjoints si leurs supports sont disjoints.

Proposition 20

Soit $n \geq 2$. Toute permutation de $[\![1, n]\!]$ différente de l'identité est la composée de cycles disjoints.

Preuve — Soit une permutation $\sigma \neq \mathrm{Id}_{[\![1,n]\!]}$. Nous allons raisonner par récurrence sur le nombre d'éléments du support $A_\sigma := \{x \in [\![1, n]\!] / \sigma(x) \neq x\}$.

Initialisation : si A_σ contient 2 éléments, alors σ est un 2-cycle.

Hérédité : supposons que la propriété est vraie si A_σ contient au plus k éléments. Montrons qu'elle est vraie si A_σ contient $k+1$ éléments. Soit x appartenant à A_σ. Il existe un entier p tel que $\begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{p-1}(x) \end{pmatrix}$ est un cycle. Soit $\sigma' = \begin{pmatrix} \sigma^{p-1}(x) & \sigma^{p-2}(x) & \ldots & \sigma(x) & x \end{pmatrix}$ le cycle réciproque. Le support de $\sigma \circ \sigma'$ est inclus dans $A_\sigma \backslash \{x, \sigma(x), \ldots, \sigma^{p-1}(x)\}$. D'où il existe des cycles disjoints $\sigma_1, \ldots, \sigma_k$ tels que $\sigma \circ \sigma' = \sigma_1 \circ \ldots \circ \sigma_k$. Alors $\sigma = \sigma_1 \circ \ldots \circ \sigma_k \circ (\sigma')^{-1}$ et tous les cycles σ_i sont disjoints du cycle $(\sigma')^{-1}$. □

Remarque 21 —

1. *Les cycles de cette décomposition sont disjoints, donc ils commutent (d'après la proposition 13).*
2. *On peut décomposer tout p-cycle en $p-1$ transpositions :*

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}.$$

(Le vérifier.)

3. *D'après le proposition 20, on peut décomposer toute permutation en cycles. D'après la dernière remarque, on peut décomposer tout cycle en transpositions. On obtient ainsi une seconde preuve de la proposition 15.*

MÉTHODE 22 — *Après la méthode 16, voici donc une seconde méthode pour décomposer une permutation en transpositions : on la décompose d'abord en cycles, puis chaque cycle en transpositions. Par exemple,*

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 \end{pmatrix}.$$

EXERCICE 23 — *Décomposer en cycles disjoints et en transpositions les permutations*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} \quad \textit{et} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 4 & 5 & 6 & 3 & 8 & 2 \end{pmatrix}.$$

DÉFINITION 24
*Soient $n \in \mathbb{N}^*$ et une permutation $\sigma \in S_n$. Pour chaque élément $x \in [\![1, n]\!]$, l'**orbite** \轨道\ de x suivant σ est l'ensemble noté $O_\sigma(x)$ défini par*

$$O_\sigma(x) = \{\sigma^k(x), \quad k \in \mathbb{Z}\}.$$

Les orbites suivant σ forment une partition de l'ensemble $[\![1, n]\!]$.

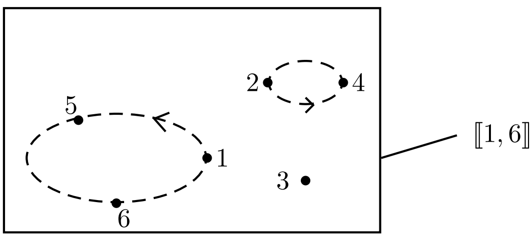
Preuve — Soit $\mathcal{R}$ la relation définie sur $[\![1, n]\!]$ par : $x \mathcal{R} y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$. Cette relation est une relation d'équivalence car :
— (réflexive) $x = \sigma^0(x)$;
— (symétrique) si $y = \sigma^k(x)$, alors $x = \sigma^{-k}(y)$;
— (transitive) si $y = \sigma^k(x)$ et $z = \sigma^\ell(y)$, alors $z = \sigma^{k+\ell}(x)$.

Les orbites suivant σ sont les classes d'équivalence de $\mathcal{R}$. Elles forment donc une partition de l'ensemble $[\![1, n]\!]$. (Voir le cours *Algèbre 1*.) □

Soit $x \in [\![1, n]\!]$:
— si $\sigma(x) = x$, alors l'orbite de x est le singleton $\{x\}$;
— sinon l'orbite de x est le support du p-cycle $\begin{pmatrix} x & \sigma(x) & \cdots & \sigma^{p-1}(x) \end{pmatrix}$, où p est le nombre d'éléments de l'orbite.

Preuve — Si $\sigma(x) \neq x$, alors la permutation σ est différente de l'identité, c'est donc (proposition 20) la composée $\sigma = \sigma_1 \circ \cdots \circ \sigma_k$ de cycles disjoints. L'élément x appartient au support d'un unique cycle σ_i, d'où $\sigma(x) = \sigma_i(x)$. □

EXEMPLE 25 — *La figure ci-dessous représente les orbites $\{1, 5, 6\}$, $\{2, 4\}$ et $\{3\}$ de la permutation σ_4 :*



On en déduit que la décomposition d'une permutation σ en cycles disjoints est unique : les cycles de deux décompositions de σ sont les mêmes, seul l'ordre des cycles peut changer. (Pourquoi ?)

1.4 SIGNATURE

DÉFINITION 26
*Soit σ une permutation. La **signature** \符号\ de σ, notée $\varepsilon(\sigma)$ est égale à*

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

REMARQUE 27 —

1. *On a*
$$\varepsilon(\sigma) = \prod_{\{i,j\}\in\mathcal{P}([\![1,n]\!]),i\neq j} \frac{\sigma(i)-\sigma(j)}{i-j}.$$
2. *On a*
$$\prod_{i<j}\left|\frac{\sigma(i)-\sigma(j)}{i-j}\right| = 1$$
car on multiplie par tous les produits $(\sigma(i)-\sigma(j))$ avec $\sigma(i)\neq\sigma(j)$ et on divise donc par ce même facteur au signe près.

PROPOSITION 28
L'application $\varepsilon : S_n \to \{-1,1\}$, $\sigma \mapsto \varepsilon(\sigma)$ vérifie
$$\varepsilon(\sigma'\circ\sigma) = \varepsilon(\sigma')\varepsilon(\sigma).$$

Preuve — Avec la remarque précédente, on calcule
$$\begin{aligned}\varepsilon(\sigma'\circ\sigma) &= \prod_{i<j}\frac{\sigma'\circ\sigma(i)-\sigma'\circ\sigma(j)}{i-j}\\ &= \prod_{i<j}\frac{\sigma'\circ\sigma(i)-\sigma'\circ\sigma(j)}{\sigma(i)-\sigma(j)}\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}\\ &= \varepsilon(\sigma')\varepsilon(\sigma).\end{aligned}$$
□

COROLLAIRE 29
Si $\sigma = \tau_1\circ\cdots\tau_r$, alors $\varepsilon(\sigma) = (-1)^r$.

Preuve — On vérifie que $\varepsilon(\tau) = -1$: soit $\tau = (i_0, j_0)$ avec $i_0 < j_0$, alors

1. si i et j différents de i_0 et j_0, alors $\tau(i) = i$ et $\tau(j) = j$, donc le couple (i,j) donne le produit $\dfrac{\tau(i)-\tau(j)}{i-j} = 1$.
2. si $k \neq i_0, j_0$, alors $\tau(k) = k$ et $\tau(i_0) = j_0$ et $\tau(j_0) = i_0$, donc les couples (i_0,k) et (j_0,k) donnent le produit $\dfrac{\tau(i_0)-\tau(k)}{i_0-k}\times\dfrac{\tau(j_0)-\tau(k)}{j_0-k} = 1$.
3. le couple (i_0,j_0) donne le produit $\dfrac{\tau(i_0)-\tau(j_0)}{i_0-j_0} = -1$.

D'où le résultat. Puis on applique la proposition précédente. □

REMARQUE 30 — *On en déduit que pour une permutation donnée, le nombre de transpositions nécessaires pour sa décomposition n'est pas fixe mais sa parité l'est et est donnée par la signature.*

DÉFINITION 31
*Soit σ une permutation. Une **inversion** \逆序\ de σ est un couple (i,j) tel que $i<j$ et $\sigma(i)>\sigma(j)$. On note $I(\sigma)$ le **nombre d'inversions** \逆序数\ de σ.*

EXEMPLE 32 —

1. *Le nombre d'inversions de l'identité est* 0.
2. *L'ensemble des inversions de la permutation* $\begin{pmatrix}1&2&3&4&5&6\\3&1&6&2&4&5\end{pmatrix}$ *est* $\{(1,2),(1,4),(3,4),(3,5),(3,6)\}$.
Donc son nombre d'inversions est 5.

PROPOSITION 33
Soit $\sigma\in S_n$. Alors $\varepsilon(\sigma) = (-1)^{I(\sigma)}$

DÉFINITION 34
Une permutation $\sigma \in S_n$ est une permutation paire (resp. impaire) si $\varepsilon(\sigma) = 1$, (resp $\varepsilon(\sigma) = -1$). On appelle groupe alterné l'ensemble A_n des permutations paires de S_n.