Groupe symétrique.

Motivation

Rappel :

$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = \underbrace{a_{1,1}a_{2,2}}_{\mathrm{id}} - \underbrace{a_{2,1}a_{1,2}}_{\tau_{1,2}}$$

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = \underbrace{a_{11}a_{22}a_{33}}_{\mathrm{id}} + \underbrace{a_{21}a_{32}a_{13}}_{c} + \underbrace{a_{31}a_{12}a_{23}}_{c^{-1}} - \underbrace{a_{21}a_{12}a_{33}}_{\tau_{1,2}} - \underbrace{a_{31}a_{22}a_{13}}_{\tau_{1,3}} - \underbrace{a_{11}a_{32}a_{23}}_{\tau_{2,3}}$$

On verra dans le prochain chapitre : $\begin{vmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{vmatrix} = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$

Objectif principal de ce chapitre : comprendre ce qu'est ε.

I Rappels sur S_n

I.1 Définition

Rappel :

1. S_n est l'ensemble des bijections de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, n\}$.
2. $(S_n, \circ)$ forme un groupe.
3. $|S_n| = n!$.

Exemples 1

1. Pour $n = 0$, $S_0 = \{\mathrm{id}\}$.
2. Pour $n = 1$, $S_1 = \{\mathrm{id}\}$.
3. Pour $n = 2$, $S_2 = \{\mathrm{id}, \tau_{12}\}$.
4. Pour $n = 3$, $S_3 = \{\mathrm{id}, c, c^{-1}, \tau_{12}, \tau_{13}, \tau_{23}\}$.

Exemple 2 Si $1 \leqslant i \neq j \leqslant n$ on peut considérer la permutation $\tau_{i,j} \in S_n$ suivante, appelée transposition :
$\tau_{i,j} : \left\{ \begin{array}{ccc} \{1, \dots, n\} & \to & \{1, \dots, n\} \\ k & \mapsto & \left\{ \begin{array}{l} j \text{ si } k = i \\ i \text{ si } k = j \\ k \text{ sinon} \end{array} \right. \end{array} \right.$.

Notation : Une permutation σ de S_n pourra être notée $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.

Exemple 3 Pour $n = 4$, la permuation $\tau_{1,2} \circ \tau_{3,4}$ peut s'écrire :

$$\tau_{12} \circ \tau_{34} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Définition 1 .
On appelle <u>support</u> d'une permutation σ l'ensemble des éléments de $\{1, \ldots, n\}$ qui ne sont pas fixés par σ.
(Le support est "là où il se passe quelque chose".)

Exemple 4 Supports de $\tau_{1,2}$, $\tau_{3,4}$ et $\tau_{1,2} \circ \tau_{3,4}$ dans S_n ?

τ_{12} $\{1, 2\}$

τ_{34} $\{3, 4\}$

$\tau_{12} \circ \tau_{34}$ $\{1, 2, 3, 4\}$

Définition 2 .
Étant donné $\sigma \in S_n$ on appelle <u>inversion</u> de σ un couple $(i, j) \in \{1, 2, \ldots, n\}$ tel que $i < j$ et $\sigma(i) > \sigma(j)$

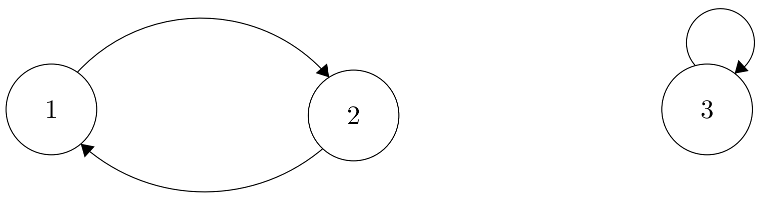
Exemples 5

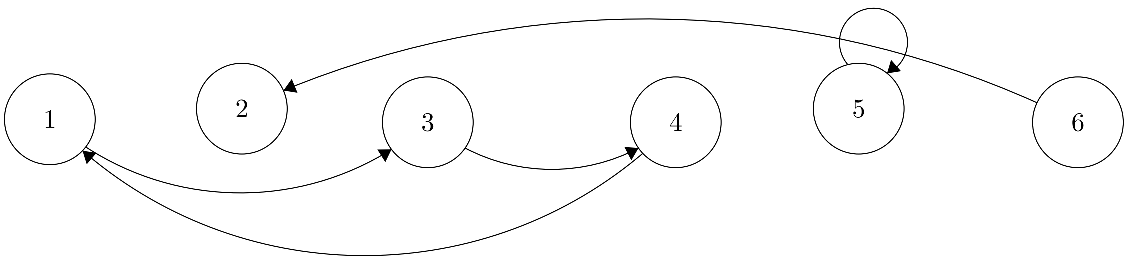
1. L'identité a 0 inversion(s).
2. Dans S_3, la transposition $\tau_{1,2}$ a 1 inversion : $\{(1, 2)\}$.
3. Dans S_3, la transposition $\tau_{1,3}$ a 3 inversion(s) : $\{(1, 3), (2, 3), (1, 2)\}$.
4. Dans S_3, le cycle $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ a $\{(1, 3), (2, 3)\}$ inversion(s).

I.2 Représentation schématique

On peut représenter une permutation par un graphe orienté dont les sommets sont les éléments de $\{1, 2, \ldots, n\}$ et pour lequel il existe un arc de i vers j si et seulement si $\sigma(i) = j$.

Exemples 6
Dans S_3 puis S_6





I.3 Transpositions

<u>Rappel</u> :

1. Une <u>transposition</u> est une permutation de la forme $\tau_{i,j}$ (voir plus haut).
2. $\tau_{i,j}^{-1} = \tau_{ij}$ c'est-à-dire $\tau_{i,j}^2 = \text{id}$. On dit qu'une transposition est une permutation d'ordre 2.

3. $\tau_{j,i} = \tau_{i,j}$.

Corollaire 1 : du troisième point.

Il y a $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions.

I.4 Structure

Rappel : Pour $n \leqslant m$ toute permutation de S_n peut être vue comme une permutation de S_m (qui laisse fixe les éléments $\{n+1, \cdots, m\}$).

Théorème 1 : Rappel.

1. $S_0 \simeq S_1 \simeq \{e\}$ (le groupe trivial)
2. $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$
3. pour $n \geqslant 3$, S_n est non commutatif car $\tau_{12} \circ \tau_{23} = c^{-1} \neq c = \tau_{23} \circ \tau_{12}$

Par commodité, on parlera de multiplication et de produit pour la composition des permutations et la composée de permutations. On s'autorisera aussi à noter $\sigma\sigma'$ pour $\sigma \circ \sigma'$.

Remarque 1

Pour tout $\sigma \in S_n$, il existe un plus petit entier $p > 0$ tel que $\sigma^p = \mathrm{id}$. Cet entier p est appelé l'ordre de la permutation.

Démonstration. Par l'absurde :
$\{\sigma, \sigma^2, \ldots, \sigma^i, \ldots, \sigma^j\}$ est fini donc il existe $i < j$ tel que $\sigma^i = \sigma^j$ d'où $\mathrm{id} = \sigma^{j-i}$ □

Exemple 7 La permutation $c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ est d'ordre 3 En effet : $c^2 = c^{-1}; c^3 = \mathrm{id}$

II Parité d'une permutation

II.1 Décomposition en transpositions

Remarque 2

On peut décomposer $c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ en produit de transpositions : $c_1 = \tau_{2,3} \circ \tau_{1,3} = \tau_{1,2} \circ \tau_{2,3}$.

Exemple 8 Pour $n = 2k$, la permutation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ n & n-1 & \cdots & k+1 & k & \cdots & 1 \end{pmatrix}$ peut se décomposer :

$\sigma = \bigcirc_{i=0}^{k} \tau_{i,i+1}$.

Les optionnaires info connaissent bien le **tri par sélection** (et pour les autres, c'est au programme en seconde année). Pour trier une liste Python L de longueur n :

- On détermine l'élément maximal parmi L[0], ..., L[n-1] ;
- On permute cet élément avec L[n-1] (sauf si c'est L[n-1]) ;
- On recommence sur L[0], ..., L[n-2] ; etc.

À la fin, on obtient une liste triée. Ceci peut se reformuler de la façon suivante sur les permutations :

Théorème 2 .

Toute permutation peut se décomposer comme produit de transpositions.

On dit que les transpositions engendrent S_n.

DÉMONSTRATION. En notant L_k la liste Python obtenue à l'issue de la k^e itération de boucle, un invariant de boucle est clairement "les éléments de L_k sont les éléments de L et $L_k[0], \cdots, L_k[n-k] \leqslant L_k[n-k+1] \leqslant \cdots \leqslant L_k[n]$".
Ceci montre que le tri par sélection est correct. Par ailleurs il est clair qu'il termine (on imbrique simplement deux boucles for).
Le rapport ? En notant τ_{i_1,j_1}, τ_{i_2,j_2}, ..., τ_{i_k,j_k} les permutations effectuées au cours de l'algorithme ($k \leqslant n-1$), on a id = ... **et donc** $\sigma =$ .... □

Remarque 3

Cette démonstration est constructive, elle donne un mode d'emploi pour trouver **une** décomposition d'une permutation !

Exemple 9 Décomposons $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

$$\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \\
\sigma \circ \tau_{45} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \\
\sigma \circ \tau_{45} \circ \tau_{14} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \\
\sigma \circ \tau_{45} \circ \tau_{14} \circ \tau_{23} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathrm{id}
\end{aligned}$$

Exercice 1. Pour les option info : quel énoncé mathématique tirer de la terminaison et correction du tri à bulles ? (Les autres : vous le ferez quand même en TD, vous ne saurez simplement pas qu'il s'agit d'un corollaire du tri à bulles.)

II.2 Parité d'une permutation

/!\ La décomposition n'est jamais unique pour $n \geqslant 2$! Par contre : il y en a au plus $n-1$

Théorème 3 : (admis).

La parité du nombre de transpositions dans une décomposition est toujours la même.

Idée d'une démonstration possible :

1. On montre que la parité du nombre d'inversions change lorsqu'on compose une permutation par une transposition.
2. On déduit facilement le résultat par l'absurde.

Définition 3 .

Une permutation est dite paire lorsqu'elle peut s'écrire comme produit d'un nombre pair de transpositions. Elle est dite impaire sinon.

Exemples 10

1. La permutation $c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ est paire car il y a deux permutations
2. Une transposition $\tau_{i,j}$ est toujours impaire
3. L'identité est toujours paire

Définition 4 : signature.

Soit $\sigma \in S_n$. On appelle signature de σ le nombre .

$$\begin{aligned}\varepsilon(\sigma) &= \begin{cases} 1 \text{ si } \sigma \text{ est paire} \\ -1 \text{ si } \sigma \text{ est impaire} \end{cases} \\ &= (-1)^{\text{nombre de permutations dans la décomposition}}\end{aligned}$$

Exemple 11 La signature de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ est $\varepsilon(\sigma) = (-1)^3 = -1$

III Orbites. Cycles

III.1 Orbites

Définition 5 .

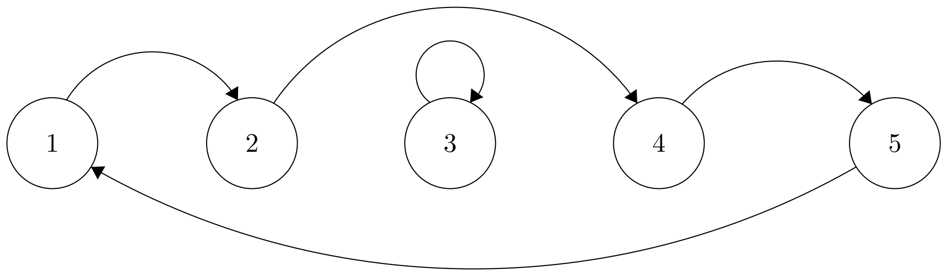
Soit $\sigma \in S_n$ et $k \in \{1, 2, \cdots, n\}$.

On appelle orbite de k sous σ (ou simplement orbite de k lorsque le contexte le permet) l'ensemble

$$O_\sigma(k) = \{k, \sigma(k), \cdots, \sigma^n(k), \cdots\} \subset \{1, 2, \cdots, n\}$$

Exemples 12

1. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \in S_5$, les orbites sont :



$$\begin{aligned} O(1) = \{1, 2, 4, 5\} = O(2) = O(4) &= O(5) \\ O(3) &= \{3\} \end{aligned}$$

2. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_6$, les orbites sont :

Remarque 4

On a déjà vu que, d'après le principe des tiroirs, la suite $\left(\sigma^i(k)\right)_{i \in \mathbb{N}}$ est périodique. Toute orbite est donc de la forme $O_\sigma(k) = \{k, \sigma(k), \cdots, \sigma^{n_k}(k)\}$.

Théorème 4 .

Les orbites sous σ forment toujours une partition de $\{1, 2, \cdots, n\}$.

Démonstration. D'après la propriété fondamentale sur les relations d'équivalences, il suffit de montrer que la relation "être dans la même orbite que" est une relation d'équivalence.

Tout est évident. □

III.2 Cycles

Exemple 13 Dans S_n avec $n \geqslant 3$, $c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $c_2 = c_1^2 = c_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ sont des 3-cycles.

Définition 6 .

1. Une permuation σ est appelée un cycle lorsqu'elle a exactement une orbite non réduite à un élément.
2. Un p-cycle est un cycle d'ordre p.

Exemple 14 Illustrons l'exemple précédent dans les cas $n = 3$ et $n = 5$.

1. Dans S_3 : une seule orbite $\{1, 2, 3\}$
2. Dans S_5 : trois orbites $\{1, 2, 3\}$, $\{4\}$ et $\{5\}$ mais une seule non réduite à un seul élément.

On a bien une seule orbite **non réduite à un seul élément**.

Exemple 15 Dans S_4, $\tau_{1,2} \circ \tau_{3,4}$ n'est pas un cycle.
Il y a deux orbites : $\{1, 2\}$ et $\{3, 4\}$
`/!\` id n'est pas un cycle car il y deux orbites non-réduites a un élément

Remarque 5

Le support d'un cycle (rappel : "là où il se passe quelque chose") est donc son unique orbite non réduite à un élément.

Proposition 1 .
Le support d'un p-cycle est de cardinal p.

Théorème 5 .
La signature d'un p-cycle est $(-1)^{p-1}$.

Démonstration. $(i_1 i_2 i_3 \dots i_p) := \begin{pmatrix} \dots & i_1 \dots & i_2 \dots & i_{p-1} \dots & i_p \dots \\ \dots & i_2 \dots & i_3 \dots & i_p \dots & i_1 \dots \end{pmatrix}$
$\tau_{ij} = (ij)$

$$(i_1 i_2 \dots i_p) = \tau_{p-1,p} \circ \dots \circ \tau_{i_2 i_p} \circ \tau_{i_1 i_p}$$

□

III.3 Décomposition en cycles

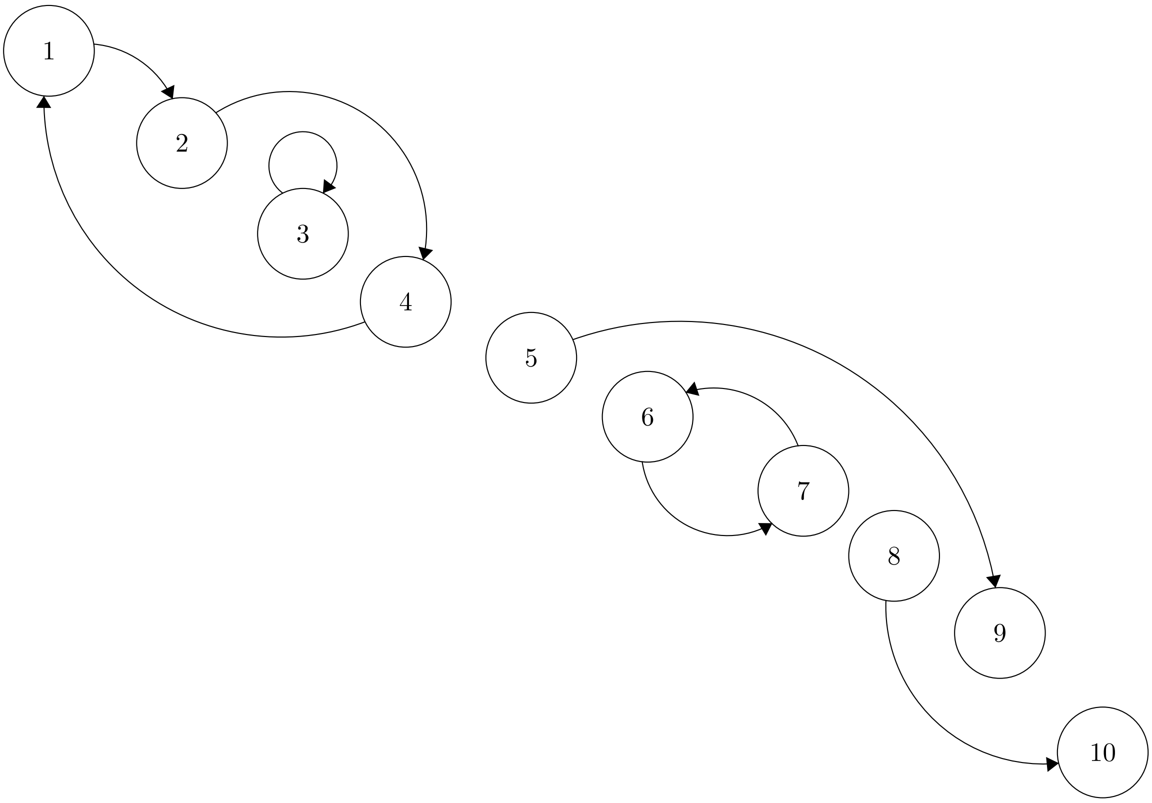
Remarque 6

Deux cycles à supports disjoints commutent.

Théorème 6 .
Toute permutation peut s'écrire comme produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près.

Démonstration. C'est une reformulation du fait que les orbites forment une partiton de $\{1, \dots, n\}$ □

Exemples 16



$$\sigma = (1\ 2\ 4) \circ (5\ 9) \circ (6\ 7) \circ (8\ 10)$$

1. Décomposons en cycles la permutation $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 & 6 \end{pmatrix} = (1\ 4\ 5) \circ (2\ 7\ 9\ 6\ 8\ 3)$.
2. Décomposons en cycles la permutation $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 4 & 3 & 2 & 9 & 7 & 6 & 8 \end{pmatrix} = (1\ 5\ 2) \circ (3\ 4) \circ (6\ 9\ 8)$.

III.4 Calcul de l'ordre d'une permutation

Exemple 17 Calculons l'ordre de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$.

On décompose en produit de cycles

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

TABLE 1 – Autocompositions de σ

σ	$(1\ 2\ 4) \circ (3\ 5)$
σ^2	$(1\ 4\ 2) \circ \mathrm{id} = (1\ 4\ 2)$
σ^3	$\mathrm{id} \circ (3\ 5)$
σ^4	$(1\ 2\ 4) \circ \mathrm{id} = (1\ 2\ 4)$
σ^5	$(1\ 2\ 4) \circ (3\ 5)$
σ^6	$\mathrm{id} \circ \mathrm{id} = \mathrm{id}$

Proposition 2 .
Si c_1 et c_2 sont deux cycles à supports disjoints, alors l'ordre de $c_1 \circ c_2$ est le PPCM des ordres

Méthode générale pour le calcul d'un ordre :

1. Décomposer σ en produit de cycles à support disjoints.
2. Déterminer l'ordre de chaque cycle à l'aide du support.
3. Utiliser la proposition précédente.

IV Compléments sur la signature

IV.1 Calcul pratique d'une signature

Théorème 7 .

$\varepsilon : \left\{ \begin{array}{ccc} (S_n, \circ) & \to & (\{\pm 1\}, \times) \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array} \right.$ est un morphisme de groupe.

Rappel : cela signifie

Démonstration.

$$\begin{aligned} \text{pair} + \text{pair} = \text{impair} + \text{impair} &= \text{pair} \\ \text{pair} + \text{impair} = \text{impair} + \text{pair} &= \text{pair} \end{aligned}$$

□

Méthode pratique pour calculer la signature d'une permutation σ :

1. On décompose σ en produit de cycles disjoints.
2. On utilise que ε est un morphisme de groupe.
3. On utilise le résultat sur la signature d'un p-cycle.

Exemples 18 Reprenons les exemples précédents :

1. $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 & 6 \end{pmatrix}$

$$\begin{aligned} \varepsilon(\sigma) &= \varepsilon((1\ 5\ 2))\varepsilon((3\ 4))\varepsilon((6\ 9\ 8)) \\ &= 1 \cdot -1 \cdot 1 \\ &= -1 \end{aligned}$$

2. $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 4 & 3 & 2 & 9 & 7 & 6 & 8 \end{pmatrix}$

$$\begin{aligned} \varepsilon(\sigma) &= \varepsilon((1\ 4\ 5)) \cdot \varepsilon((2\ 7\ 9\ 8\ 6\ 3)) \\ &= 1 \cdot -1 \\ &= -1 \end{aligned}$$

Remarque 7

On a exactement deux morphismes de groupe $(S_n, \circ) \to (\{\pm 1\}, \times)$: la signature et le morphisme trivial $1 : \left\{ \begin{array}{ccc} S_n & \to & \{\pm 1\} \\ \sigma & \mapsto & 1. \end{array} \right.$

Démonstration. Exercice du TD ! □

IV.2 Expressions équivalentes

Proposition 3 .

On dispose des trois caractérisations équivalentes suivantes de la signature :

1. $\varepsilon(\sigma) = (-1)^{\left|\left\{(i,j),\ i<j \text{ et } \sigma(i)>\sigma(j)\right\}\right|}$.
2. $\varepsilon(\sigma) = \prod_{i<j} \dfrac{i-j}{\sigma(i)-\sigma(j)} = \prod_{i<j} \dfrac{\sigma(i)-\sigma(j)}{i-j}$.
3. $\varepsilon(\sigma) = (-1)^{n-m}$ où $\begin{cases} n \text{ est l'indice de } S_n \\ m \text{ est le nombre d'orbites de } \sigma. \end{cases}$

Démonstration. Exercice, pas facile. □

IV.3 Groupe alterné

Proposition-Définition 7 .

L'ensemble des permutations paires forment un sous-groupe de S_n.

On l'appelle groupe alterné et on le note $\mathcal{A}_n$ ou $\mathcal{U}_n$.

Démonstration. $\mathcal{U}_n = \mathrm{Ker}(\varepsilon)$ □

Exemples 19

1. Pour $n = 0$ et $n = 1$, on a $\mathcal{U}_3 = \{\mathrm{id}, c, c^{-1}\}$
2. Pour $n = 2$, on a ....
3. Pour $n = 3$, on a ....

Exemple 20 Décrivons S_4 en détails pour obtenir $\mathcal{U}_4$.

Théorème 8 .

Pour $n \geqslant 2$, on a $|\mathcal{U}_n| = \dfrac{n!}{2}$.

Démonstration.

□