IV/ *Groupe des permutations d'un ensemble fini*

1. Groupe S_n

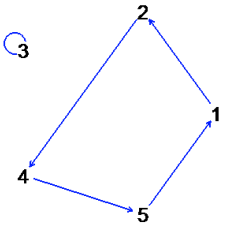
S_n est le groupe des permutations (bijections) de l'ensemble $\{1,2,..,n\}$.
Il est isomorphe au groupe des permutations de n'importe quel ensemble à n éléments.

Exemples
S_2 est composé de l'identité et de la bijection $1 \longleftrightarrow 2$
S_3 est isomorphe au groupe des permutations des sommets d'un triangle équilatéral, et donc aussi au groupe des isométries du plan qui laissent un triangle équilatéral globalement invariant.

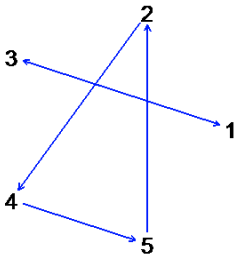
S_n est un groupe d'ordre $n!$

Une permutation σ peut être notée $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$
Cette notation (notation de Gauss) peut être commode pour composer 2 permutations.

Exemple :
pour $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$



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



on écrit $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$ pour voir que $\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$

et $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ pour voir que $\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$

La composée $\sigma_2 \circ \sigma_1$ se note aussi $\sigma_2\sigma_1$; $\sigma \circ \sigma \circ ... \circ \sigma = \sigma^k$, $\sigma^0 = id$ (notation multiplicative).

2. Permutations particulières

Orbite d'un élément sous l'action d'une permutation

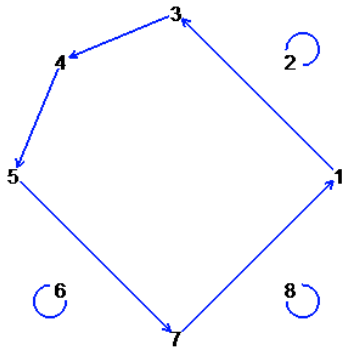
Soit σ une permutation de $\{1,2,..,n\}$ et $x \in \{1,2,..,n\}$.
L'orbite de x sous l'action de σ est l'ensemble $O(x) = \{x, \sigma(x), \sigma^2(x), ..., \sigma^k(x)...\}$

Exemple pour σ_1 : $O(1) = \{1,2,4,5\}, O(2) = O(4) = O(5) = O(1)$ et $O(3) = \{3\}$

- $O(x)$ est un ensemble fini.
- Pour tout x, il existe un entier $k \leqslant n$ tel que $O(x) = \{x, \sigma(x), \sigma^2(x), ..., \sigma^{k-1}(x)\}$ et $\sigma^k(x) = x$
- La relation $y \mathcal{R} x \Leftrightarrow y \in O(x)$ est une relation d'équivalence. Les orbites sont donc disjointes 2 à 2.

p-cycle

Une permutation σ de $\{1,2,..,n\}$ est un p-cycle (ou cycle d'ordre p) si toutes les orbites sont réduites à un élément, sauf une seule, qui a p éléments.



Dans ce cas, pour tout x élément de cette orbite, $O(x)=\{x,\sigma(x),\sigma^2(x),...,\sigma^{p-1}(x)\}$

Le p-cycle σ est alors noté $(x,\sigma(x),\sigma^2(x),...,\sigma^{p-1}(x))$

L'ensemble des éléments de l'orbite (sans tenir compte de l'ordre) est appelé le support du cycle.

Exemples σ_1 est un 4-cycle noté $(1,2,4,5)$ ou $(2,4,5,1)$ ou... mais pas $(1,4,2,5)$.

Son support est $\{1,2,4,5\}=\{1,4,2,5\}=...$

σ_2 n'est pas un cycle.

Transposition

Une transposition est un 2-cycle.

La transposition (i,j) dans $\boldsymbol{S_n}$ échange i et j et laisse invariant pous les autres éléments de $\{1,2,..,n\}$

Remarque :

Pour i, j, k distincts 2 à 2, le produit des transpositions (i,j) et (j,k) est un 3-cycle : $(i,j)(j,k)=(i,j,k)$

↑°→	id	(1,2)
id	id	(1,2)
(1,2)	(1,2)	id

Table du groupe S_2

↑°→	id	(1,2,3)	(1,3,2)	(1,2)	(2,3)	(1,3)
id	id	(1,2,3)	(1,3,2)	(1,2)	(2,3)	(1,3)
(1,2,3)	(1,2,3)	(1,3,2)	id	(1,3)	(1,2)	(2,3)
(1,3,2)	(1,3,2)	id	(1,2,3)	(2,3)	(1,3)	(1,2)
(1,2)	(1,2)	(2,3)	(1,3)	id	(1,2,3)	(1,3,2)
(2,3)	(2,3)	(1,3)	(1,2)	(1,3,2)	id	(1,2,3)
(1,3)	(1,3)	(1,2)	(2,3)	(1,2,3)	(1,3,2)	id

Table du groupe S_3

3. Décomposition en cycles, en transposititon

Théorème 1 :

- Toute permutation se décompose en produit de cycles de supports disjoints.
- Cette décomposition est unique à l'ordre près.
- Tous ces cycles commutent

Théorème 2 :

- Toute permutation se décompose en produit de transpositions.
- Cette décomposition n'est pas unique

Exemple

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix} = (1,\,3,\,6)(2,\,10,\,9,\,8,\,5) = (1,\,3)(3,\,6)(2,\,10)(10,\,9)(9,\,8)(8,\,5)$$

↑°→	id	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)	(1,2)(3,4)	(1,4)(2,3)	(2,4)	(1,3)
id	id	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)	(1,2)(3,4)	(1,4)(2,3)	(2,4)	(1,3)
(1,2,3,4)	(1,2,3,4)	(1,3)(2,4)	(1,4,3,2)	id	(1,3)	(2,4)	(1,2)(3,4)	(1,4)(2,3)
(1,3)(2,4)	(1,3)(2,4)	(1,4,3,2)	id	(1,2,3,4)	(1,4)(2,3)	(1,2)(3,4)	(1,3)	(2,4)
(1,4,3,2)	(1,4,3,2)	id	(1,2,3,4)	(1,3)(2,4)	(2,4)	(1,3)	(1,4)(2,3)	(1,2)(3,4)
(1,2)(3,4)	(1,2)(3,4)	(2,4)	(1,4)(2,3)	(1,3)	id	(1,3)(2,4)	(1,2,3,4)	(1,4,3,2)
(1,4)(2,3)	(1,4)(2,3)	(1,3)	(1,2)(3,4)	(2,4)	(1,3)(2,4)	id	(1,4,3,2)	(1,2,3,4)
(2,4)	(2,4)	(1,4)(2,3)	(1,3)	(1,2)(3,4)	(1,4,3,2)	(1,2,3,4)	id	(1,3)(2,4)
(1,3)	(1,3)	(1,2)(3,4)	(2,4)	(1,4)(2,3)	(1,2,3,4)	(1,4,3,2)	(1,3)(2,4)	id

Table du sous-groupe de S_4 *engendré par le cycle* $(1,2,3,4)$ *et la transposition* $(1,3)$

Application :
Pour prouver qu'une expression utilisant *n* variable est symétrique, c'est-à-dire invariante par toute permutation des variables, il suffit de démontrer qu'elle est ne change pas quand on échange 2 des *n* variables.
Exemples :
le polynôme $P(X,Y,Z) = (X+Y+Z)\text{^}3 - X^2Y - X^2Z - XY^2 - ZY^2 - XZ^2 - YZ^2 + XYZ$ est symétrique.
le polynôme $Q(X,Y,Z) = X^2\left(Y^2+Z^2\right) + Y^2\left(X^2+Z^2\right) + XYZ$ ne l'est pas (échanger X et Z).

4. Signature

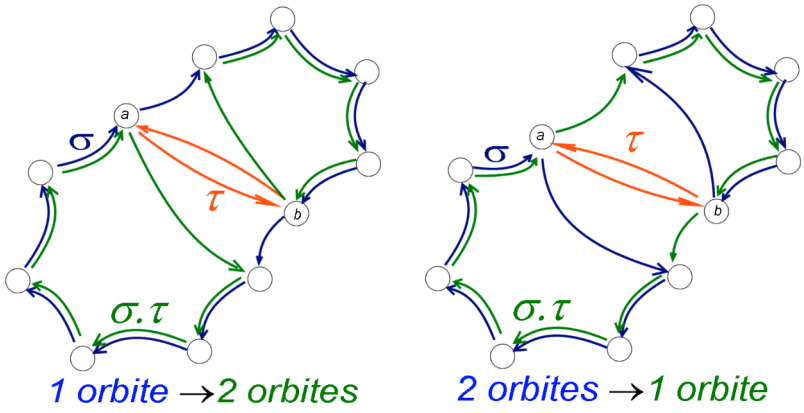
Pour toute permutation σ de S_n, on détermine le nombre m d'orbites distinctes sous l'action de σ.

On définit alors sa <u>signature</u> $\varepsilon(\sigma)$ comme étant égale à 1 si $n-m$ est pair et -1 sinon : $\varepsilon(\sigma)=(-1)^{n-m}$

- La signature de l'identité est $+1$
- La signature d'une transposition est -1
- La signature d'un 3-cycle est $+1$

Théorème 3 :

- Pour toute permutation σ de S_n et toute transposition τ, $\varepsilon(\sigma\tau)=-\varepsilon(\sigma)$
- Pour toutes permutations σ_1 et σ_2 de S_n, $\varepsilon(\sigma_1\sigma_2)=\varepsilon(\sigma_1)\varepsilon(\sigma_2)$:
  La fonction $\varepsilon : S_n \longrightarrow \{-1,+1\}$ est un morphisme de groupes
- Si une permutation σ de S_n se décompose en produit de k transpositions, alors $\varepsilon(\sigma)=(-1)^k$



Théorème 4 :

Pour toute permutation σ de S_n, sa signature est égale à $\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}$,

c'est-à-dire à +1 si le nombre de "dérangements" de la liste $[1,2,...,n]$ est pair, et à -1 sinon.

Démonstration : Notons $s(\sigma)=\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}=\frac{\prod_{i<j}(\sigma(i)-\sigma(j))}{\prod_{i<j}(i-j)}$.

1° $s(\sigma)=\prod_{i<j}\frac{\sigma(i)-\sigma(j)}{i-j}=\prod_{i<j}\frac{\sigma(j)-\sigma(i)}{j-i}$ donc $(s(\sigma))^2=\frac{\prod_{i<j}(\sigma(i)-\sigma(j))(\sigma(j)-\sigma(j))}{\prod_{i<j}(i-j)(j-i)}$

Comme σ est une permutation, chaque facteur $a-b$ (avec $a<b$ ou $b<a$) se trouve une fois et une seule au numérateur. Donc $(s(\sigma))^2=1$ et $s(\sigma)=\pm 1$. Il n'y a plus qu'à trouver son signe !

2° Si σ est une transposition (a,b) (avec $a<b$),
Pour i et j donnés (avec $i<j$),

- si $i\neq a$ et $j\neq b$, $\sigma(i)=i$, $\sigma(j)=j$ donc $\frac{\sigma(i)-\sigma(j)}{i-j}=1$

- si $i=a$ et $j\neq b$, $\sigma(i)=b$, $\sigma(j)=j$ donc $\dfrac{\sigma(i)-\sigma(j)}{i-j}=\dfrac{b-j}{a-j}$,
  ce qui est négatif si et seulement si $a<j<b$, ce qui fait $b-a-1$ cas
- De même si $i\neq a$ et $j=b$, $\dfrac{\sigma(i)-\sigma(j)}{i-j}=\dfrac{i-a}{i-b}<0\Leftrightarrow a<i<b$, ce qui fait encore $b-a-1$ cas
- Enfin si $i=a$ et $j=b$ $\dfrac{\sigma(i)-\sigma(j)}{i-j}=\dfrac{b-a}{a-b}<0$

Il y a donc $(b-a+1)+(b-a+1)+1$ facteurs négatifs dans $s(\sigma)$ donc $s(\sigma)<0$ et $s(\sigma)=-1$

3° Soient maintenant 2 permutations σ_1 et σ_2.

Comme σ_2 est une permutation, $s(\sigma_1)=\prod_{i<j}\dfrac{\sigma_1(i)-\sigma_1(j)}{i-j}=\prod_{i<j}\dfrac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{\sigma_2(i)-\sigma_2(j)}$

(c'est seulement un changement de l'ordre des facteurs). Donc

$$s(\sigma_1).s(\sigma_2)=\prod_{i<j}\left(\frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{\sigma_2(i)-\sigma_2(j)}.\frac{\sigma_2(i)-\sigma_2(j)}{i-j}\right)=\prod_{i<j}\frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{i-j}=s(\sigma_1\circ\sigma_2).$$

4° Toute permutation peut se décomposer en produit de transpositions.

Si σ est le produit de k transpositions $\sigma=\tau_1\circ\tau_2\circ\ldots\circ\tau_k$ alors (3°) $s(\sigma)=s(\tau_1)s(\tau_2)\ldots s(\tau_k)$

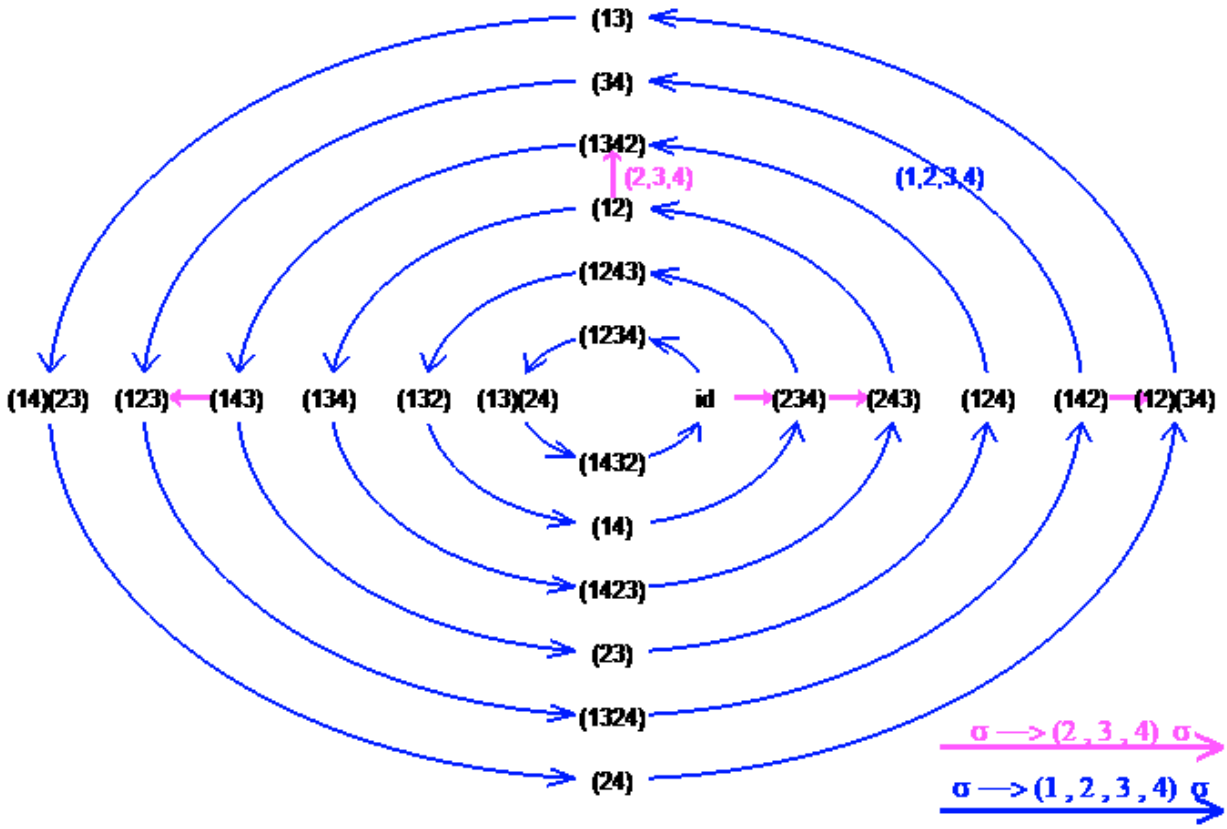
et comme (2°) $\forall i\ s(\tau_i)=-1$ on a bien $s(\sigma)=(-1)^k$ = la signature de σ

Permutation paire :

Une permutation est paire si et seulement si sa signature est +1. Sinon c'est une permutation impaire. L'ensemble des permutations paires est un sous groupe de S_n. On le nomme groupe alterné A_n.

Il est d'ordre $\dfrac{n!}{2}$

o	paire	impaire
paire	paire	impaire
impaire	impaire	paire



S_4 **engendré par les cycles (1,2,3,4) et (2,3,4)**

On définit 6 orbites sous l'action du 4-cycle (1,2,3,4)

5. Applications

Ordre d'une permutation

Mélange « américain » d'un jeu de 32 cartes https://youtu.be/hFFx8ImnP2Y?t=143
Ce mélange réalise la permutation σ de $\{1,2,...,32\}$ telle que

$\sigma(1)=1$, $\sigma(32)=32$, $\forall n \in \{2,3,...,31\} \sigma(n)=2n-1 \bmod 31$

σ se décompose en produit de 6 cycles de supports disjoints, tous d'ordre 5.
Comme ils commutent, $\sigma^5 = id$.

Le jeu du taquin (jeu des quinze)

Voici le récit de Sam Loyd (extrait de Oh ! les Maths de Yakov Perelman Dunod) :
"Les anciens parmi les habitants du royaume de la débrouillardise se rappellent qu'au début des années 70, j'ai amené le monde entier à se casser la tête sur un jeu de carrés mobiles connu sous le nom de "jeu des quinze". Les quinze carrés étaient disposés dans l'ordre à l'intérieur d'un cadre, à l'exception, des pièces 14 et 15, interverties...Le problème consistait à rétablir la disposition initiale, les pièces 14 et 15 étant, cette fois, dans l'ordre.

La prime de 1000 dollars offerte comme récompense au premier qui y parviendrait ne fut décernée à personne, bien que tous se soient acharnés sur le problème...
Nul ne voulait renoncer à ses recherches, chacun étant certain qu'il parviendrait au but."

- Déplacer un carré revient à le permuter avec la case vide (notons-la 0) et donc d'effectuer une transposition sur $\{0,1,2,...,15\}$. On cherche à effectuer un certain nombre de transpositions (k,0) dont le produit donne la transposition (14,15), qui est de signature -1.
- Comme la case vide revient à sa place, le nombre de transpositions qui s'appliquent à 0 est pair. Donc la signature du produit est +1.
- Contradiction

Et en partant de la disposition suivante ?

https://fr.wikipedia.org/wiki/Taquin
http://images.math.cnrs.fr/Le-jeu-de-taquin-du-cote-de-chez-Galois