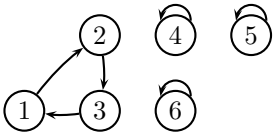
Le Groupe Symétrique

MPSI Prytanée National Militaire

Pascal Delahaye

9 avril 2018



Les notions vues dans ce chapitre seront surtout utiles lorsque nous aborderons le chapitre sur les déterminants.

1 Le groupe symétrique

DÉFINITION 1 : **Groupe des permutations**
Soit un ensemble E.
On appelle *permutation* de E, une bijection $\sigma : E \mapsto E$.
$\big(\mathcal{B}(E),\ \circ\big)$ est un groupe, appelé *groupe des permutations* de l'ensemble E.

DÉFINITION 2 : **Groupe symétrique : S_n**
Lorsque l'ensemble $E = [\![1, n]\!]$, on note S_n le groupe des permutations de E.
S_n est un groupe fini de cardinal $n!$ que l'on appellera le *groupe symétrique* d'ordre n.
Une permutation $\sigma \in S_n$ se note :

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

`Exemple 1.` $(*)$ Décrire la permutation $\sigma = \begin{pmatrix} 1&2&3&4&5 \\ 3&5&1&2&4 \end{pmatrix}$.

`Exemple 2.` $(*)$ Déterminer les permutations de l'ensemble $\{1,\ 2\}$ puis les permutations de $\{1,\ 2,\ 3\}$.

`Exemple 3.` Composition de deux permutations :
$(*)$ Déterminer les composées $\sigma \circ \sigma'$ et $\sigma' \circ \sigma$ des deux permutations suivantes : $\sigma = \begin{pmatrix} 1&2&3&4&5 \\ 3&5&1&2&4 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1&2&3&4&5 \\ 2&5&3&1&4 \end{pmatrix}$.

Exercice : 1
$(**)$ **Petit théorème de Fermat (1601-1665)**
Soit p un nombre premier. Soit $n \in \mathbb{Z}$, premier avec p.
On pose $x_k = k.n$ pour $1 \leq k \leq p-1$ et $\sigma(k)$ est le reste de la division de x_k par p. Soit $X = x_1.x_2 \ldots .x_{p-1}$.

1. Démontrer que $\sigma \in S_{p-1}$. En déduire que $X \equiv (p-1)!\ [p]$.
2. Démontrer que $n^{p-1} = 1\ [p]$.

DÉFINITION 3 : **Support d'une permutation**
On appelle *support* d'une permutation $\sigma \in S_n$ l'ensemble des éléments de $[\![1, n]\!]$ non invariants.

Ainsi, le support de $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{smallmatrix}\right)$ est : $\{1,\ 2,\ 4,\ 5\}$

DÉFINITION 4 : **Ordre d'une permutation**
On appelle *ordre* d'une permutation $\sigma \in S_n$ le plus petit entier $p \in \mathbb{N}^*$ tel que $\sigma^p = \mathrm{id}$.
On rappelle la convention d'écriture : $\sigma^p = \overbrace{\sigma \circ \cdots \circ \sigma}^{p \text{ fois}}$.

Preuve : Il suffit de remarquer que $\{\sigma^p \mid p \in \mathbb{N}\} \subset S_n$ qui est de cardinal fini.

`Exemple 4.` $(*)$ Donner l'ordre de la permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{smallmatrix}\right)$.

DÉFINITION 5 : **Sous-Groupe engendré par une permutation**

Soit $\sigma \in S_n$. Notons p l'ordre de σ.

$(\{\sigma^k \mid k \in \mathbb{N}\},\ \circ)$ est un sous-groupe de S_n d'ordre p appelé *le sous-groupe engendré par* σ

`Exemple 5.` Déterminer les éléments du sous-groupe de S_4 engendré par $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{smallmatrix}\right)$.

2 Cycles, transpositions

DÉFINITION 6 : **Orbite d'un élément**
Soit une permutation $\sigma \in S_n$ et un élément $x \in [\![1, n]\!]$.
On appelle *orbite* de l'élément x selon la permutation σ, l'ensemble : $\mathcal{O}_\sigma(x) = \{\sigma^k(x)\ ;\ k \in \mathbb{Z}\}$
Il s'agit des images itérées de l'élément x par σ.

`Exemple 6.` Si $E = [\![1, 6]\!]$, et $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{smallmatrix}\right)$, alors : $\begin{cases} \mathcal{O}_\sigma(1) = \mathcal{O}_\sigma(2) = \{1,\ 2\} \\ \mathcal{O}_\sigma(3) = \mathcal{O}_\sigma(5) = \mathcal{O}_\sigma(6) = \mathcal{O}_\sigma(4) = \{3,\ 4,\ 5,\ 6\} \end{cases}$.

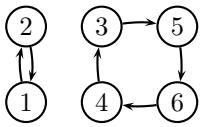


FIGURE 1 – Orbites d'une permutation

Remarque 1.

1. On pourra aussi représenter les orbites en attribuant une couleur différente à chacune d'entre elles.
2. L'ensemble des orbites d'une permutation $\sigma \in S_n$ forme une partition de $[\![1, n]\!]$

`Exemple 7.` $(*)$ Déterminer les orbites de la permutation : $s = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 4 & 1 & 7 & 10 & 2 & 3 & 9 & 8 \end{smallmatrix}\right)$.

DÉFINITION 7 : **Permutation circulaire**
Soit une permutation $\sigma \in S_n$.
On dit que c'est une *permutation circulaire* si σ n'admet qu'une seule orbite.

`Exemple 8.` $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{smallmatrix}\right)$ est une permutation circulaire de $[\![1, 4]\!]$ (ou de S_4) :

Remarque 2. Dans ce cas, tout x élément de $[\![1, n]\!]$ est tel que $\mathcal{O}_\sigma(x) = [\![1, n]\!]$.

Exercice : 2
$(*)$ Déterminer le nombre de permutations circulaires dans le groupe symétrique S_n.

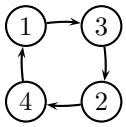


FIGURE 2 – Permutation circulaire

DÉFINITION 8 : **Cycle**
Soit une permutation $\sigma \in S_n$.
On dit que σ est un *cycle* s'il y a au plus une orbite $\{x_1,\ x_2,\ \ldots,\ x_k\}$ qui n'est pas réduite à un élément.
Cette orbite s'appelle le *support* du cycle, et le cardinal de cette orbite s'appelle la *longueur* du cycle.
Dans le cas des cycles, on utilise une notation plus simple que la notation usuelle. On note :

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}$$

Cette notation signifie que : "l'image de x_1 est x_2, l'image de x_2 est x_3 ... etc..."

`Exemple 9.` $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{smallmatrix}\right)$, est un cycle de support $\{1, 2, 3\}$ et de longueur 3 de S_6.
On note plus simplement $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ ce cycle de S_6.

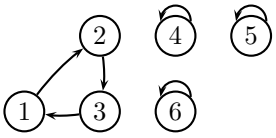


FIGURE 3 – Un cycle de longueur 3

Remarque 3. Une permutation circulaire est un cycle particulier. (aucune orbite ne contient un unique élément)

Exercice : 3
(∗) Déterminer le nombre de cycles de longueur p dans S_n.

NOTATION 9 : La composée de deux cycles $\sigma = \begin{pmatrix} x_1 & x_2 & \ldots & x_p \end{pmatrix}$ et $\sigma' = \begin{pmatrix} y_1 & y_2 & \ldots & y_q \end{pmatrix}$ est notée :

$$\sigma \circ \sigma' = \begin{pmatrix} x_1 & x_2 & \ldots & x_p \end{pmatrix} \begin{pmatrix} y_1 & y_2 & \ldots & y_q \end{pmatrix}$$

Lorsque les supports sont disjoints, cette composée est commutative.

`Exemple 10.` (∗) Déterminer la permutation suivante : $\sigma = \begin{pmatrix} 1 & 4 & 3 & 5 \end{pmatrix} \begin{pmatrix} 2 & 3 & 5 \end{pmatrix}$.

1. Cette composée est-elle commutative ?
2. La composée de deux cycles est elle un cycle ?

PROPOSITION 1 : **Ordre d'un cycle**
L'ordre d'un cycle est égal à sa longueur.

THÉORÈME 2 : **Décomposition d'une permutation en produit de cycles**
Soit une permutation $\sigma \in S_n$.
Elle se décompose de façon unique en un produit fini de cycles de supports disjoints.
Les cycles de la décomposition correspondent aux différentes orbites de σ et commutent deux à deux.

Preuve 2 : Non exigible.

`Exemple 11.` Décomposition de $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{smallmatrix}\right)$ en produit de cycles :

`Exemple 12.` (∗) Décomposer $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 1 & 2 & 4 & 6 & 7 & 5 & 8 & 3 \end{smallmatrix}\right)$ en produit de cycles.

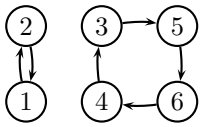


FIGURE 4 – Décomposition en produit de cycles : $\sigma = (1\ 2)(3\ 5\ 6\ 4) = (3\ 5\ 6\ 4)(1\ 2)$

PROPOSITION 3 : **Ordre d'une permutation**
L'ordre d'une permutation est le PPCM des ordres des différents cycles qui composent la permutation.

`Exemple 13.` $(*)$ Soit $s \in S_{10}$ la permutation : $s = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 4 & 1 & 7 & 10 & 2 & 3 & 9 & 8 \end{smallmatrix}\right)$.

1. Décomposer s en produit de cycles.
2. Déterminer l'ordre de s.
3. En déduire :
   (a) l'expression de s^{100}.
   (b) le cardinal du sous-groupe de S_{10} engendré par s

DÉFINITION 10 : **Transpositions**
Une *transposition* de S_n est un cycle de longueur 2.

Remarque 4.

1. Une transposition échange deux éléments a, b et laisse tous les autres invariants. On note τ_{ab} cette transposition.
2. Une transposition est involutive : $\tau \circ \tau = \mathrm{id}$

`Exemple 14.` $(*)$

1. Quel est le nombre de transpositions dans le groupe S_n ?
2. Calculer $\tau_{12} \circ \tau_{23}$ et $\tau_{23} \circ \tau_{12}$ dans S_n, $(n \geq 3)$.

PROPOSITION 4 : **Décomposition d'un cycle en produit de transpositions**
Un cycle se décompose facilement en produit (au sens de la compositions) de transpositions.
Soit le cycle $\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_p \end{pmatrix} \in S_n$. On a alors :

$$\sigma = \tau_{x_1,x_2} \circ \tau_{x_2,x_3} \circ \tau_{x_3,x_4} \circ \cdots \circ \tau_{x_{p-1},x_p}$$

On constate que si le cycle est de longueur p alors la décomposition comprend $p-1$ transpositions.

Preuve 4 : On vérifie de façon immédiate que pour tout $k \in [\![1, n]\!]$, on a bien $\sigma(x_k) = x_{k+1}$

Remarque 5. Ainsi, toute permutation se décompose en produit de N transpositions où $N = \sum_{O \in \{\text{orbites}\}} (l(O) - 1)$.

`Exemple 15.` $(*)$ Décomposer $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{smallmatrix}\right)$ en produit de transpositions.

THÉORÈME 5 : **Décomposition d'une permutation en "produit" de transpositions**
L'ensemble des transpositions engendre le groupe symétrique.

$$S_n = \{\tau_1 \circ \dots \tau_p \mid p \in \mathbb{N}^*,\ \tau_1,\ \dots \tau_p \text{ des transpositions de } S_n\}$$

Preuve 5 : Immédiat puisque les cycles engendrent S_n.

Remarque 6. Il n'y a pas unicité de la décomposition et les transpositions ne commutent pas entre elles.

Exercice : 4
$(*)$

1. Pour $(i,\ j) \in [\![1, n]\!]^2$, calculer $\tau_{1i} \circ \tau_{1j} \circ \tau_{1i}$.
2. En déduire que les transpositions de la forme τ_{1i} engendrent le groupe symétrique S_n.

Exercice : 5
$(*)$ Soit τ_1 et τ_2, deux transpositions de S_n. Montrer que l'on a $\tau_1 \circ \tau_2 = \mathrm{id}$ ou $(\tau_1 \circ \tau_2)^2 = \mathrm{id}$ ou $(\tau_1 \circ \tau_2)^3 = \mathrm{id}$

3 Signature d'une permutation

Définition 11 : **Signature d'une permutation**
Soit une permutation $\sigma \in S_n$.
On dit qu'un couple $(i,\ j) \in [\![1, n]\!]^2$ est une *inversion* de σ lorsque : $\begin{cases} i < j \\ \sigma(i) > \sigma(j) \end{cases}$.
On note $I(\sigma)$ le nombre d'inversions de la permutation σ, et on définit la *signature* de la permutation σ par

$$\boxed{\varepsilon(\sigma) = (-1)^{I(\sigma)}}$$

La signature d'une permutation $\sigma \in \mathcal{S}_n$ est également donnée par la formule :

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

Remarque 7. On dit qu'une permutation σ est $\begin{cases} \textit{paire} & \text{si } \varepsilon(\sigma) = +1 \\ \textit{impaire} & \text{si } \varepsilon(\sigma) = -1 \end{cases}$.

`Exemple 16.` $(*)$ Déterminer le nombre d'inversions et la signature de la permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 1 & 4 & 6 \end{smallmatrix}\right)$.

Proposition 6 : Les transpositions sont de signature -1.

Preuve 6 : Il suffit de vérifier que le nombre d'inversions correspondant à une transposition est impair.

Théorème Fondamental 7 : **Signature d'une composée**
Pour tout couple $(\sigma_1,\ \sigma_2) \in S_n$ on a :

$$\boxed{\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \times \varepsilon(\sigma_2)}$$

Preuve 7 : Démonstration non exigible.

Remarque 8.

1. Cela signifie en particulier que l'application $\varepsilon : \begin{array}{ccc} (S_n, \circ) & \longrightarrow & (\{-1, 1\}, \times) \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array}$ est un morphisme de groupes.
2. Le noyau de ce morphisme $\mathcal{A}_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = +1\}$ (l'ensemble des permutations de signature 1) est un sous-groupe de S_n appelé le *groupe alterné* d'ordre n.

Corollaire 8 : **Autre caractérisation de la signature**
Si une permutation σ s'écrit comme produit de p transpositions, $\sigma = \tau_1 \circ \cdots \circ \tau_p$. Alors :

$$\boxed{\varepsilon(\sigma) = (-1)^p}$$

Preuve 8 : Pas de difficulté.

Remarque 9. La décomposition d'une permutation en produit de transpositions n'est pas unique, mais le corollaire précédent prouve que la *parité* du nombre de transpositions est la même pour toute décomposition.

Exercice : 6
$(*)$ Montrer que la signature d'une permutation $\sigma \in S_n$ vaut $\varepsilon(\sigma) = (-1)^{n-k}$ où k est le nombre d'orbites de σ (on compte les orbites réduites à un singleton).

Exercice : 7
$(***)$ Dans les années 1870, Sam Loyd a offert une prime de 1000 dollars à la personne qui trouverait la solution du jeu de taquin suivant :

1. La case 16 est vide, et les pièces numérotées peuvent glisser sur cette case vide.

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	

4	3	2	1
5	6	7	8
12	11	10	9
13	15	14	

FIGURE 5 – Position initiale et finale du puzzle 15

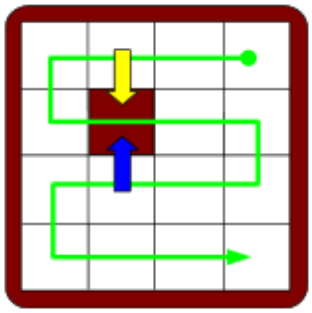
2. Lors du premier coup, on peut faire glisser la case 15 ou la case 12 sur la case vide, et ainsi de suite.

Le défi consiste à obtenir la même configuration que la configuration initiale où les cases 14 et 15 sont inversées.

Modélisation :

On décide de modéliser la grille du jeu de Taquin comme le résultat d'une permutation de S_{15}.
La position initiale correspond alors à l'application id.

1. Expliquer pourquoi :
   (a) Le déplacement d'une case horizontalement correspond à composer par l'identité
   (b) Le déplacement d'une case verticalement correspond à composer par un cycle de longueur impaire



2. En déduire que la configuration finale est alors impossible à obtenir en suivant les règles du jeu.

Exercice : 8

(**) Prouver que toute permutation du groupe alterné se décompose en produit de cycles de longueur 3.

4 Connaissez-vous votre cours ?

Vous devez impérativement savoir répondre aux différentes questions suivantes :

	Questions	Réponses attendues
1.	Qu'appelle-t-on le *groupe symétrique* S_n ? Décrire la permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\4&1&2&3&5\end{smallmatrix}\right)$ Pourquoi $\sigma_1 = \left(\begin{smallmatrix}1&2&3&4\\4&1&2&1\end{smallmatrix}\right)$ et $\sigma_2 = \left(\begin{smallmatrix}1&2&3&4\\4&5&2&3\end{smallmatrix}\right)$ ne sont pas dans S_n	cf cours Non bijectives sur $[\![1, n]\!]$
2.	Sans utiliser les orbites, donner l'ordre de la permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\4&1&2&3&5\end{smallmatrix}\right)$	4

3.	Quel est le support de la permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\4&2&1&3&5\end{smallmatrix}\right)$?	$\{1,\ 3,\ 4\}$
4.	Quel sont les orbites de la permutation $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\4&6&7&3&5&2&1\end{smallmatrix}\right)$? Pourquoi σ n'est pas une permutation circulaire ? En déduire son ordre.	$\{1,\ 4,\ 3,\ 7\}$, $\{2,\ 6\}$ et $\{5\}$ plus d'une orbite $\text{ppcm}(4,\ 2,\ 1) = 4$
5.	Reconnaître le cycle suivant : $\sigma = (3,\ 5,\ 1,\ 2,\ 4)$	$\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&4&5&3&1\end{smallmatrix}\right)$
6.	Donner le résultat de la composée suivante : $(3,\ 1,\ 5)(2,\ 3,\ 5,\ 1)$	$\left(\begin{smallmatrix}1&2&3&4&5\\2&1&3&4&5\end{smallmatrix}\right)$
7.	Décomposer $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\4&6&7&3&5&2&1\end{smallmatrix}\right)$ en produit de cycles.	$\sigma = (1,\ 4,\ 3,\ 7)(2,\ 6)$
8.	Calculer σ^{2012} lorsque $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\2&7&5&3&4&1&6\end{smallmatrix}\right)$	$\sigma^{2012} = \sigma^8 = \left(\begin{smallmatrix}1&2&3&4&5&6&7\\1&2&4&5&3&6&7\end{smallmatrix}\right)$
9.	Décomposer la cycle $\sigma = (6,\ 2,\ 1,\ 4,\ 7)$ en produit de transpositions.	$\sigma = \tau_{6,\ 2} \circ \tau_{2,\ 1} \circ \tau_{1,\ 4} \circ \tau_{4,\ 7}$
10.	Sauriez-vous prouver que l'ensemble des transpositions de la forme $\tau_{1,\ p}$ engendre S_n	cf exo cours
11.	Quelles sont les méthodes permettant de calculer la signature d'une permutation ?	avec les inversions avec les transpositions avec les orbites