Le Groupe Symétrique

MPSI-1 Prytanée National Militaire

Pascal Delahaye - D'après le cours d'Alain Soyeur

13 janvier 2011

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 $\sigma : E \mapsto E$.
On note $\mathfrak{S}_E$ l'ensemble des permutations de l'ensemble E.
$(\mathfrak{S}_E, \circ)$ est un groupe, appelé *groupe des permutations* de l'ensemble E.

Dans la suite, on considèrera un ensemble fini E de cardinal n.
Comme il est possible de numéroter les éléments de E, on pourra considérer que $E = [\![1,n]\!]$.

Remarque 1. Permuter n éléments consiste à les ranger dans un ordre différent.
Ainsi, choisir une permutation de $[\![1,n]\!]$ revient à permuter l'ordre des éléments de cet ensemble.

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

$$\sigma = \begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix} \quad \text{ou, plus simplement :} \quad \sigma = \begin{pmatrix} \sigma(1) & \dots & \sigma(n) \end{pmatrix}$$

`Exemple 1.` Décrire la permutation $\sigma = (3\ 5\ 1\ 2\ 4)$.

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

2 Cycles, transpositions

DÉFINITION 3 : **Orbite d'un élément**
Soit une permutation $\sigma \in \mathfrak{S}_n$ et un élément $x \in [\![1,n]\!]$.
On appelle *orbite* de l'élément x selon la permutation σ, l'ensemble : $\mathcal{O}_\sigma(x) = \{\sigma^k(x)\ ;\ k \in \mathbb{Z}\}$

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

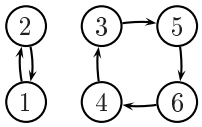

FIG. 1 – *Orbites d'une permutation*

PROPOSITION 1 : **Propriétés des orbites**
Soit $\sigma \in \mathfrak{S}_n$ avec $n \in \mathbb{N}^*$.

1. Pour tout $x \in [\![1,n]\!]$, il existe $p \in [\![1,n]\!]$ tel que $x = \sigma^p(x)$
   Dans ce cas, nous avons $\mathcal{O}_\sigma(x) = \{\sigma^k(x)\ ;\ k \in [\![0,p-1]\!]\}$.
2. Soit x, $y \in [\![1,n]\!]$.
$$y \in \mathcal{O}_\sigma(x) \iff x \in \mathcal{O}_\sigma(y) \iff \mathcal{O}_\sigma(x) = \mathcal{O}_\sigma(y)$$

Preuve 1 :

1. Il suffit de remarquer que $\text{Card}\{\sigma^k(x),\ k \in [\![1,n+1]\!]\} \leq n$.
2. (a) On commence par prouver la première équivalence en utilisant le résultat précédent.
   (b) La deuxième équivalence est alors quasi-immédiate.

Remarque 2. L'ensemble des orbites d'une permutation $\sigma \in \mathfrak{S}_n$ forme une partition de $[\![1,n]\!]$

PROPOSITION 2 : **Définition plus simple de l'orbite d'un élément**
Si $\sigma \in \mathfrak{S}_n$ et $x \in [\![1,n]\!]$, alors : $\mathcal{O}_\sigma(x) = \{\sigma^k(x)\ ;\ k \in [\![0,n-1]\!]\}$.

Preuve 2 : C'est un corollaire de la proposition précédente.

Exercice : 1
Soit $s \in \mathfrak{S}_{10}$ la permutation : $s = (6\ 5\ 4\ 1\ 7\ 10\ 2\ 3\ 9\ 8)$.

1. Déterminer les orbites de s
2. Déterminer le plus petit entier n tel que $s^n = s$. (au sens de la composition des applications !)
3. En déduire s^{100}

Exercice : 2
Une démonstration originale du petit théorème de Fermat.
Soit $a \in \mathbb{N}^*$ et p un nombre premier.

1. On considère $\Delta = \{\text{mots à } p \text{ caractères composés à l'aide d'un alphabet composé de } a \text{ lettres}\}$.

   On considère l'application $\varphi : \begin{array}{ccc} \Delta & \longrightarrow & \Delta \\ (a_1, \ldots, a_p) & \mapsto & (a_{\sigma(1)}, \ldots, a_{\sigma(p)}) \end{array}$ où $\sigma = \begin{pmatrix} 2 & 3 & \ldots & p & 1 \end{pmatrix}$.
   En remarquant que l'ensemble des orbites de φ forme une partition de Δ, montrer que $a^p \equiv a[p]$.
2. En déduire dans le cas où p ne divise pas a que $a^{p-1} \equiv 1\ [p]$.

DÉFINITION 4 : **Permutation circulaire**
Soit une permutation $\sigma \in \mathfrak{S}_n$.
On dit que c'est une *permutation circulaire* s'il existe un élément $x \in [\![1,n]\!]$ tel que $\mathcal{O}_\sigma(x) = [\![1,n]\!]$.

`Exemple 4.` $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{smallmatrix}\right)$ est une permutation circulaire de $[\![1,4]\!]$ (ou de $\mathfrak{S}_4$) :

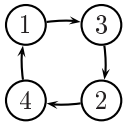

FIG. 2 – *Permutation circulaire*

Remarque 3.

1. Dans ce cas, tout x élément de $[\![1,n]\!]$ est tel que $\mathcal{O}_\sigma(x) = [\![1,n]\!]$.
2. Il y a $(n-1)!$ permutations circulaires dans le groupe symétrique $\mathfrak{S}_n$.

DÉFINITION 5 : **Cycle**
Soit une permutation $\sigma \in \mathfrak{S}_n$.
On dit que σ est un *cycle* s'il y a au plus une orbite 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.

`Exemple 5.` $\sigma = \left(\begin{smallmatrix}1&2&3&4&5&6\\2&3&1&4&5&6\end{smallmatrix}\right)$, est un cycle de support {1,2,3} et de longueur 3 de $\mathfrak{S}_6$.
On note plus simplement $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ ce cycle de $\mathfrak{S}_6$.

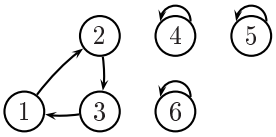

FIG. 3 – *Un cycle de longueur* 3

Remarque 4. 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 $\mathfrak{S}_n$.

DÉFINITION 6 : **Transpositions**
Une *transposition* de $\mathfrak{S}_n$ est un cycle de longueur 2.

Remarque 5.

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 6.`

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

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

Décomposition d'une permutation en "produit" de transpositions

THÉORÈME FONDAMENTAL 3 : **Décomposition d'une permutation en produit de transpositions**
Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose en un produit fini de transpositions :

$$\sigma = \tau_1 \circ \cdots \circ \tau_k$$

Preuve 3 : Procédons par récurrence sur n.

1. Pas de difficulté pour $n = 1$ (et $n = 2$).
2. Soit $n \in \mathbb{N}^*$. On suppose le théorème vrai pour cette valeur de n.
   Soit $\sigma \in \mathfrak{S}_{n+1}$. On traite alors les deux cas suivants :
   (a) Si $\sigma(n+1) = n+1$ alors on peut appliquer l'hypothèse de récurrence à $\sigma_{|[\![1,n]\!]}$.
   (b) Si $\sigma(n+1) \neq n+1$. On se ramène au cas précédent en considérant $\sigma' = \tau_{n+1,\sigma(n+1)} \circ \sigma$.

Remarque 6.

1. En d'autres termes, l'ensemble des transpositions engendre le groupe symétrique.
2. Il n'y a pas unicité de la décomposition et les transpositions ne commutent pas.

Exercice : 5

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 $\mathfrak{S}_n$.

3 Signature d'une permutation

DÉFINITION 7 : **Signature d'une permutation**
Soit une permutation $\sigma \in \mathfrak{S}_n$.
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

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

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 7.` Déterminer le nombre d'inversions et la signature de la permutation $\sigma = \begin{pmatrix} 3 & 5 & 7 & 2 & 1 & 4 & 6 \end{pmatrix}$.

PROPOSITION 4 : Les transpositions sont de signature -1.

Preuve 4 : Il suffit de vérifier que le nombre d'inversions correspondant à une transposition est impair.

THÉORÈME FONDAMENTAL 5 : **Signature d'une composée**
Pour tout couple $(\sigma_1, \sigma_2) \in \mathfrak{S}_n$ on a :

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

Preuve 5 : Démonstration non exigible.

Remarque 8.

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

COROLLAIRE 6 : **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 6 : 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

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

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

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

FIG. 4 – *Position initiale et finale du puzzle* 15

Le défi consiste à obtenir la même configuration que la configuration initiale où les cases 14 et 15 sont inversées. Qu'en pensez-vous?