Cours de mathématiques M.P.S.I.

D'après les cours de M. De Granrut

Henriet Quentin
Ausseil Lucas
Perard Arsène
Philipp Maxime

Groupe symétrique

1. Permutation d'un ensemble fini

1.1. Notation

Définition :
Soit E un ensemble fini. On appelle permutation de E toute application $\sigma : E \to E$ bijective.

Remarque :
Tout ensemble de cardinal n est en bijection avec $[\![1,n]\!]$: On peut se contenter d'étudier les permutations de $[\![1,n]\!]$.

Définition :
On note S_n l'ensemble des permutations de $[\![1,n]\!]$.

Propriétés :
- $\mathrm{Card}(S_n) = n!$
- $(S_n, \circ)$ est un groupe de neutre $e = \mathrm{id}_{[\![1,n]\!]}$

1.2. Composition

Exemple :
Soient $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 1 & 7 & 6 & 4 & 2 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 6 & 3 & 1 & 4 \end{pmatrix}$

Alors : $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 2 & 4 & 1 & 5 & 7 \end{pmatrix}$ et $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$.

Propriété :
S_n n'est pas commutatif si $n \geqslant 3$.

Remarque :
On note souvent $\sigma\tau$ pour $\sigma \circ \tau$ et on parle du produit de deux permutations.

2. Décomposition d'une permutation en produit de transpositions

2.1. Transposition

Définition :
On appelle transposition de S_n toute permutation de S_n qui échange deux éléments en laissant les autres invariants.
On la note $(i,j)_n \quad (i<j)$.

Exemple :
$(3,7)_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 4 & 5 & 6 & 3 & 8 \end{pmatrix}$

Remarque :
Il y a $\binom{n}{2} = \dfrac{n(n-1)}{2}$ transpositions dans S_n.

Propriétés :
- $(i,j)_n^{-1} = (i,j)_n$
- $(i,j)_n \circ (i,j)_n = e$

2.2. Les transpositions engendrent S_n

Théorème :

Toute permutation de S_n, $n \geqslant 2$, peut s'écrire comme le produit de transpositions.

Preuve et algorithme :

Récurrence sur n :

- Pour $n=2$, $S_2=\{e,(1,2)_2\}$
- Supposons $n\geqslant 2$ et la propriété vraie au rang n :

  Soit $\sigma\in S_{n+1}$

  1er cas : $\sigma(n+1)=n+1$: σ se restreint en une permutation σ' de S_n

  H.R. $\Rightarrow$ $\sigma'=\tau_1'\ldots\tau_k'$ où τ_i' est une transposition de S_n

  qui se prolonge en τ_i une transposition de S_{n+1}, en posant $\tau_i(n+1)=n+1$

  $\sigma=\tau_1\ldots\tau_k$

  2ème cas : $\sigma(n+1)=p<n+1$

  $\sigma'=[(p,n+1)\circ\sigma]\in S_{n+1}$ $\quad\sigma'(n+1)=n+1$

  D'après le premier cas : $\sigma'=\tau_1\ldots\tau_k$, τ_i transposition de S_{n+1}

  $\sigma=(p,n+1)\circ\tau_1\circ\ldots\circ\tau_k$

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

Par récurrence, la propriété est vraie pour tout $n\geqslant 2$.

Remarques :

Toute permutation peut s'écrire comme le produit d'au plus n transpositions.

Il n'y a pas unicité de la décomposition.

3. Signature

3.1. Inversion

Définition :

Soit $\sigma\in S_n$. On appelle inversion de σ toute paire $\{i,j\}\,i\neq j$ tel que $\dfrac{\sigma(i)-\sigma(j)}{i-j}<0$ c'est-à-dire les images de i et j par σ ne sont pas dans le même ordre que i et j.

Exemple :

Soit $\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&4&1&2\end{pmatrix}$ Inversions : $\{1,2\}\ \{1,3\}\ \{1,4\}\ \{1,5\}\ \{2,4\}\ \{2,5\}\ \{3,4\}\ \{3,5\}$

3.2. Signature

Définition :

On dit qu'une permutation est paire (resp. impaire) si son nombre d'inversion est pair (resp. impair).

Définition :

On appelle signature de σ et on note $\varepsilon(\sigma)=(-1)^N$ où N est le nombre d'inversion de σ.

Théorème :

$$\forall\sigma,\tau\in S_n,\varepsilon(\sigma\tau)=\varepsilon(\sigma)\varepsilon(\tau)$$

Remarque :

ε est un morphisme de $(S_n,\circ)\to(\{-1,1\},\times)$

Preuve du théorème :

Soient :

$A_1=\{\{i,j\}$ avec $i<j$, $\tau(i)<\tau(j)$ et $\sigma\tau(i)<\sigma\tau(j)\}$

$A_2=\{\{i,j\}$ avec $i<j$, $\tau(i)<\tau(j)$ et $\sigma\tau(i)>\sigma\tau(j)\}$

$A_3=\{\{i,j\}$ avec $i<j$, $\tau(i)>\tau(j)$ et $\sigma\tau(i)<\sigma\tau(j)\}$

$A_4=\{\{i,j\}$ avec $i<j$, $\tau(i)>\tau(j)$ et $\sigma\tau(i)>\sigma\tau(j)\}$

On pose $n_k=\mathrm{Card}(A_k)$

Nombre d'inversions de σ : n_2+n_3 de τ : n_3+n_4 de $\sigma\tau$: n_2+n_4

$\varepsilon(\sigma)=(-1)^{n_2+n_3}$ $\quad\varepsilon(\tau)=(-1)^{n_3+n_4}$ $\quad\varepsilon(\sigma\tau)=(-1)^{n_2+n_4}$

$\varepsilon(\sigma).\varepsilon(\tau)=(-1)^{n_2+n_3+n_3+n_4}=(-1)^{n_2+n_4}\times(-1)^{2n_3}=\varepsilon(\sigma\tau)$

Définition :

Le noyau de ε est un sous-groupe de S_n (c'est le sous-groupe des permutations paires), appelé groupe alterné, noté A_n.

Proposition :

Une transposition est une permutation impaire.

Corollaire :

Une permutation qui se décompose en produit d'un nombre pair (resp. impair) de transpositions est pair (resp. impair).

Corollaire :

Toute permutation paire (resp. impaire) se décompose en un nombre pair (resp. impair) de transpositions.

Preuve de la proposition :

Pour $i<j$:

$$\tau=\begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

Inversions : $\{i,i+1\},\{i,i+2\},\dots,\{i,j-1\},\{i,j\}$
$\{i+1,j\},\{i+2,j\},\dots,\{j-1,j\}$

Nombre d'inversions : $2k+1$

Donc $\varepsilon(\tau)=-1$.

4. Cycles

Définition :

Soit $n\geqslant 2$. On appelle cycle de S_n toute permutation pour laquelle il existe :

- un entier $k\in[\![2,n]\!]$, appelé longueur du cycle.
- k nombres $\{a_1,a_2,\dots,a_k\}$ deux à deux distincts dans $[\![1,n]\!]$ (support du cycle), tels que :
  - $c(a_i)=a_{i+1}$ pour $1\leqslant i\leqslant k-1$
  - $c(a_k)=a_1$
  - $c(j)=j$ pour $j\notin\{a_1,a_2,\dots,a_k\}$

On la note $c=(a_1,\dots,a_k)_n$.

Proposition :

La signature d'un cycle de longueur k est $(-1)^{k-1}$.

Preuve :

Soit c un cycle de S_n de longueur k, de support $\{a_1,a_2,\dots,a_k\}$ $\quad c=(a_1,\dots,a_k)_n$

Soit a la permutation définie par $a=\begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots & n \\ a_1 & a_2 & \dots & a_k & \underbrace{*\quad\dots\quad *}_{\text{en dehors du support}} \end{pmatrix}$

Soit γ le cycle $(1,2,\dots,k)_n$: $\gamma=\begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & \dots & n \\ 2 & 3 & \dots & k & 1 & k+1 & \dots & n \end{pmatrix}$

Montrer que : $c=a\gamma a^{-1}$

Si $j\in\{a_1,\dots,a_k\}$ $\quad j=a_i \qquad c(j)=c(a_i)=\begin{cases} a_{i+1} & \text{si } i\neq k \\ a_1 & \text{si } i=k \end{cases}$

$$a\gamma a^{-1}(j)=a\gamma a^{-1}(a_i)=a\gamma(i)=\begin{cases} a(i+1)=a_{i+1} \\ a(1)=a_1 \end{cases}$$

Si $j\notin\{a_1,\dots,a_k\}$ $\quad c(j)=j$

$$a\gamma a^{-1}(j)=a\gamma(l) \quad l>k$$
$$=a(l)=j$$

Donc $c=a\gamma a^{-1}$

$\varepsilon(c)=\varepsilon(a)\varepsilon(\gamma)\varepsilon(a^{-1})=\varepsilon(aa^{-1})\varepsilon(\gamma)=\varepsilon(\gamma)$

Inversions de γ : $\{1,k\},\{2,k\},\dots,\{k-1,k\}$ $\quad k-1$ inversions

Donc $\varepsilon(c)=\varepsilon(\gamma)=(-1)^{k-1}$

* * * * *

Mis à jour le 25.05.10