Groupe des permutations

I Définitions :

Permutation

Notons :

$$\mathbb{N}_n = \{1, 2, \dots, n\}$$

On appelle permutation de $\mathbb{N}_n$ une bijection de $\mathbb{N}_n$ dans lui-même.

On note S_n l'ensemble des permutations de $\mathbb{N}_n$.

On appelle support d'une permutation σ de S_n le sous ensemble de $\mathbb{N}_n$ suivant :

$$S(\sigma) = \{i \in \mathbb{N}_n : \sigma(i) \neq i\}$$

Exemple : Une permutation σ peut être représentée par son tableau de valeurs comme cette permutation de S_4 :

i	1	2	3	4
$\sigma(i)$	4	2	1	3

Transposition

On appelle transposition de $\mathbb{N}_n$ une permutation τ de $\mathbb{N}_n$ qui ne fait qu'échanger deux termes, c'est-à-dire, si i et j sont les rangs de ces termes, alors :

$$\tau(i) = j$$

$$\tau(j) = i$$

$$\forall k \in \mathbb{N}_n : k \notin \{i, j\} \Rightarrow \tau(k) = k$$

On notera une telle transposition sous la forme :

$$\tau = (i, j)$$

ou bien :

$$\tau = \tau_{ij}$$

Le support de τ_{ij} est donc le sous ensemble $\{i, j\}$

Exemple de transposition de S_4 :

i	1	2	3	4
$\sigma(i)$	1	3	2	4

Cette transposition échange les termes de rang 2 et 3, on la notera :

$$\sigma = (2,3)$$

Cycle

On appelle cycle de $\mathbb{N}_n$ de longueur $1 \leq p \leq n$ une permutation σ de S_n telle qu'il existe un sous ensemble $\{i_1, i_2, \dots, i_p\}$ de p entiers de $\mathbb{N}_n$ tel que :

$$\forall\, k \in [\![1, p-1]\!]\ \sigma(i_k) = i_{k+1},\ \ \sigma(i_p) = i_1$$

$$\forall\, j \in \mathbb{N}_n \backslash \{i_1, i_2, \dots, i_p\} :\ \sigma(j) = j$$

Un tel cycle se notera :

$$\sigma = (i_1, i_2, \dots, i_p)$$

Et on pourra changer de notation par permutation circulaire :

$$\sigma = (i_2, \dots, i_p, i_1) = (i_3, \dots, i_p, i_1, i_2) = \dots = (i_p, i_1, \dots, i_{p-1})$$

Une transposition est un cycle de longueur 2.

Exemples : $\sigma = (1,3,4)$ dans S_4 :

i	1	2	3	4
$\sigma(i)$	3	2	4	1

II Propriétés des permutations vis-à-vis de la composition

1) Composition

La composée de deux permutations de S_n est une permutation de S_n.

Exemple **:** Composée de deux transpositions de S_4 : $\sigma = \tau_{23} \circ \tau_{13}$

i	1	2	3	4
$\tau_{13}(i)$	3	2	1	4
$\tau_{23}(\tau_{13}(i))$	3	1	2	4

2) Structure de groupe de S_n pour la composition

On note Id l'application identité de $\mathbb{N}_n$ dans lui même

Pour tout triplet $(\sigma, \sigma', \sigma'')$ de permutations de S_n on a :

$$(\sigma \circ \sigma') \circ \sigma'' = \sigma \circ (\sigma' \circ \sigma'')$$

La composition est donc associative

Pour toute permutation σ de S_n on a :

$$\sigma \circ Id = Id \circ \sigma = \sigma$$

et Il existe une permutation (unique) σ' (notée σ^{-1}) telle que :

$$\sigma \circ \sigma' = \sigma' \circ \sigma = Id$$

La composition possède donc un <u>élément neutre</u> et toute permutation de S_n possède un <u>inverse</u> dans S_n.

S_n est donc un groupe pour la composition mais ce groupe n'est pas commutatif (voir l'exemple qui suit)

<u>Exemple 1</u> : On se replace dans S_4 et on reprend les transpositions de l'exemple précédent mais en les composant dans un ordre différent :

i	1	2	3	4
$\tau_{23}(i)$	1	3	2	4
$\tau_{13}(\tau_{23}(i))$	2	3	1	4

On constate bien que :

$$\tau_{23} \circ \tau_{13} \neq \tau_{13} \circ \tau_{23}$$

<u>Exemple 2 :</u> Donner le tableau de valeurs de l'inverse σ^{-1} de la permutation σ dont le tableau est :

i	1	2	3	4
$\sigma(i)$	4	2	1	3

Réponse :

i	1	2	3	4
$\sigma^{-1}(i)$	3	2	4	1

<u>3) Inverse d'une transposition :</u>

Une transposition τ est involutive, ce qui signifie qu'elle est égale à son inverse, soit :

$$\boldsymbol{\tau \circ \tau = Id}$$

<u>4) Composée de deux transpositions</u>

Soit τ_1, τ_2 deux transpositions de S_n pour $n \geq 2$ Alors on a :

Si les transpositions ont même support soit $S(\tau_1) = S(\tau_2)$ alors $\tau_1 = \tau_2$ et :

$$\boldsymbol{\tau_1 \circ \tau_2 = Id}$$

Si $S(\tau_1) \cap S(\tau_2)$ se réduit à un point alors la composée $\tau_1 \circ \tau_2$ est un cycle de longueur 3

Si les transpositions ont des supports disjoints soit $S(\tau_1) \cap S(\tau_2) = \emptyset$ alors elles commutent soit :

$$\boldsymbol{\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1}$$

Preuve :

posons $\tau_1 = (i,j), \tau_2 = (k,l)$

1er cas : $S(\tau_1) \cap S(\tau_2) = \{i,j\} \cap \{k,l\}$ réduit à un point par exemple $k = i$. Alors :

$$\tau_1 \circ \tau_2 = (i,j) \circ (i,l) = (i,l,j)$$

2 ème cas : $S(\tau_1) \cap S(\tau_2) = \emptyset$. On vérifie aisément la relation :

$$\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$$

5) Décomposition d'une permutation en composée de transpositions

Toute permutation de S_n , pour $n \geq 2$ peut se mettre sous la forme (non unique) d'une composée de transpositions.

Preuve :

Par récurrence sur n.

Initialisation : $n = 2$

Soit $\sigma \in S_2$ alors si $\sigma = Id, \sigma = \tau_{12} \circ \tau_{12}$ sinon $\sigma = \tau_{1\sigma(1)}$

Hérédité : Supposons la proposition vraie pour $n \geq 2$. Soit alors $\sigma \in S_{n+1}$. Distinguons deux cas :

1er cas : $\sigma(n+1) = n+1$

Considérons alors la permutation σ' de S_n , restriction de σ à $\mathbb{N}_n$ et donc définie par :

$$\forall\, i \in \mathbb{N}_n :\ \sigma'(i) = \sigma(i)$$

Alors cette permutation peut se mettre sous forme d'une composée de transpositions τ'_k de S_n:

$$\sigma' = \tau'_1 \circ \tau'_2 \circ \ldots \circ \tau'_p$$

Etendons ces transpositions pour en faire des transpositions τ_k de S_{n+1} laissant $n+1$ invariant en posant :

$$\forall\, i \in \mathbb{N}_n :\ \tau_k(i) = \tau'_k(i), \qquad \tau_k(n+1) = n+1$$

Alors :

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_p$$

2ème cas : $\sigma(n+1) = q \neq n+1$

Considérons alors la permutation σ_1 de S_{n+1} définie par :

$$\sigma_1 = \tau_{q,n+1} \circ \sigma$$

Cette permutation laisse $n+1$ invariant et donc sa restriction σ'_1 à $\mathbb{N}_n$ est donc une permutation de S_n que l'on peut décomposer comme précédemment en composée de transpositions de S_n :

$$\sigma'_1 = \tau'_1 \circ \tau'_2 \circ \ldots \circ \tau'_p$$

En définissant alors comme précédemment des transpositions τ_k de S_{n+1} laissant $n+1$ invariant on obtient :

$$\tau_{q,n+1} \circ \sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_p$$

Donc :

$$\sigma = \tau_{q,n+1} \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_p$$

Etant donné qu'on peut insérer dans toute composition la composée d'une transposition quelconque avec elle-même car $\tau \circ \tau = Id$, la décomposition n'est pas unique.

III Signature d'une permutation

Lemme 1 :

Soit τ_1, τ_2 deux transpositions de S_n pour $n \geq 2$ et $q \in \mathbb{N}_n$ Alors on a :

soit $\tau_1 = \tau_2$ et :

$$\tau_1 \circ \tau_2 = Id$$

soit $\tau_1 \neq \tau_2$ et il existe deux transpositions τ'_1, τ'_2 de S_n telles que :

$$\tau_1 \circ \tau_2 = \tau'_1 \circ \tau'_2,$$

$$\tau'_1(q) = q \text{ (Autrement dit, } \tau'_1 \text{ laisse } q \text{ invariant)}$$

Preuve :

Si $\tau_1 \neq \tau_2$, posons $\tau_1 = (i,j), \tau_2 = (k,l)$ donc :

$$S(\tau_1) \cup S(\tau_2) = \{i,j,k,l\}$$

Distinguons plusieurs cas :

1er cas : $q \notin \{i,j\}$ on a :

$$\tau_1 \circ \tau_2 = \tau_1 \circ \tau_2$$

On prend : $\tau'_1 = \tau_1, \tau'_2 = \tau_2$

2ème cas : $q \in \{i,j\}$, par exemple $q = i$ soit $\tau_1 = (q,j), \tau_2 = (k,l)$

1er sous cas : $q \in \{k,l\}$, par exemple $q = k$ soit $\tau_1 = (q,j), \tau_2 = (q,l)$

Comme $\tau_1 \neq \tau_2$, $j \neq l$ et :

$$\tau_1 \circ \tau_2 = (q,j) \circ (q,l) = (l,j,q) = (q,l,j) = (j,l) \circ (j,q)$$

On prend donc : $\tau'_1 = (j,l), \tau'_2 = (j,q)$

$$S(\tau'_1) \cup S(\tau'_2) = \{i,j,l\} \subset S(\tau_1) \cup S(\tau_2)$$

2ème sous cas : $q \notin \{k,l\}$

1er sous sous cas : $j \in \{k,l\}$, par exemple $j = k$ soit $\tau_1 = (q,k), \tau_2 = (k,l)$

$$\tau_1 \circ \tau_2 = (q,k) \circ (k,l) = (l,q,k) = (q,k,l) = (k,l) \circ (l,q)$$

On prend donc : $\tau'_1 = (k,l), \tau'_2 = (l,q)$

$$S(\tau'_1) \cup S(\tau'_2) = \{i,k,l\} \subset S(\tau_1) \cup S(\tau_2)$$

2ème sous sous cas : $j \notin \{k,l\}$

$$\tau_1 \circ \tau_2 = (q,j) \circ (k,l) = (k,l) \circ (q,j) = \tau_2 \circ \tau_1$$

On prend donc : $\tau'_1 = \tau_2,\ \tau'_2 = \tau_1$

$$S(\tau'_1) \cup S(\tau'_2) = \{i,j,k,l\} \subset S(\tau_1) \cup S(\tau_2)$$

Lemme 2 : Soit $n \geq 2$ alors :

Pour tout $p \in \mathbb{N}$, on ne peut pas trouver $2\,p+1$ transpositions τ_k de S_n telles que :

$$\boldsymbol{\tau_1 \circ \tau_2 \circ \ldots \circ \tau_{2\,p+1} = Id}$$

Preuve : Une triple récurrence, en appelant $P(n)$ cette propriété.

Initialisation : $n = 2$

Etant donné qu'il n'y a qu'une seule transposition à savoir $\tau = (1,2)$, un nombre impair de composée de cette transposition donnera τ qui n'est pas l'identité.

Donc $P(2)$ est vraie

Hérédité : supposons la propriété $P(n)$ vraie pour $n \in \mathbb{N}$. Montrons qu'elle est vraie pour $n+1$ par récurrence sur p en notant $Q_{n+1}(p)$ la proposition :

on ne peut pas trouver $2\,p+1$ transpositions τ_k de S_{n+1} telles que :

$$\tau_1 \circ \tau_2 \circ \ldots \circ \tau_{2\,p+1} = Id$$

Initialisation : $p = 0$ c'est trivial donc $Q_{n+1}(0)$ est vraie

Hérédité : on suppose la propriété $Q_{n+1}(p)$ vraie pour $p \in \mathbb{N}$. Montrons que $Q_{n+1}(p+1)$ est vraie par l'absurde en supposant qu'on puisse trouver $2\,p+3$ transpositions τ_k de S_{n+1} telles que :

$$\tau_1 \circ \tau_2 \circ \ldots \circ \tau_{2\,p+3} = Id$$

Nous allons montrer d'abord qu'on peut trouver $2\,p+3$ transpositions τ'_k de S_{n+1} laissant invariant $n+1$ et telles que :

$$\tau'_1 \circ \tau'_2 \circ \ldots \circ \tau'_{2\,p+3} = Id$$

Et pour cela nous allons montrer par récurrence sur $2 \leq k \leq 2\,p+3$ la propriété $R_{n+1,p}(k)$ suivante :

on peut trouver k transpositions τ'_r de S_{n+1} telles que :

$$\tau'_1 \circ \tau'_2 \circ \ldots \circ \tau'_k \circ \tau_{k+1} \circ \ldots \circ \tau_{2\,p+3} = Id$$

et où $\tau'_1, \tau'_2, \ldots, \tau'_{k-1}$ laissent invariant $n+1$

Initialisation : $k = 2$

On utilise le résultat du Lemme 1 avec τ_1, τ_2 sachant qu' on ne peut avoir $\tau_1 \circ \tau_2 = Id$, d'après l'hypothèse de récurrence $Q_{n+1}(p)$. Il existe donc deux transpositions τ'_1, τ'_2 de S_n telles que τ'_1 laisse invariant $n+1$ et :

$$\tau_1 \circ \tau_2 = \tau'_1 \circ \tau'_2$$

Donc :

$$\tau'_1 \circ \tau'_2 \circ \tau_3 \circ \dots \circ \tau_p = Id$$

La propriété $R_{n+1,p}(2)$ est donc vraie.

Hérédité : On suppose la propriété $R_{n+1,p}(k)$ vraie pour $2 \leq k \leq 2\,p + 2$.

On note que $\tau'_k \circ \tau_{k+1} \neq Id$ d'après l'hypothèse de récurrence $Q_{n+1}(p)$. Le Lemme 1 montre alors qu' il existe deux transpositions τ''_k, τ'_{k+1} de S_n telles que τ''_k laisse invariant $n+1$ et :

$$\tau'_k \circ \tau_{k+1} = \tau''_k \circ \tau'_{k+1}$$

Donc :

$$\tau'_1 \circ \tau'_2 \circ \dots \circ \tau''_k \circ \tau'_{k+1} \circ \dots \circ \tau_{2\,p+3} = Id,$$

où $\tau'_1, \tau'_2, \dots, \tau'_{k-1}, \tau''_k$ laissent $n+1$ invariant, ce qui prouve l'hérédité et donc que $R_{n+1,p}(k+1)$ est vraie

En appliquant le fait que $R_{n+1,p}(2\,p+3)$ est vraie, on obtient qu'il existe $2\,p+3$ transpositions τ'_k de S_n telles que :

$$\tau'_1 \circ \tau'_2 \circ \dots \tau'_{2\,p+2} \circ \tau'_{2\,p+3} = Id$$

et où $\tau'_1, \tau'_2, \dots, \tau'_{2\,p+2}$, laissent $n+1$ invariant.

Or, en composant par $\tau'_{2\,p+3}$ à droite , on a :

$$\tau'_1 \circ \tau'_2 \circ \dots \tau'_{2\,p+2} = \tau'_{2\,p+3}$$

Donc

$$\tau'_{2\,p+3}(n+1) = n+1$$

Ainsi, les $2\,p+3$ transpositions $\tau'_1, \tau'_2, \dots, \tau'_{2\,p+3}$ laissent $n+1$ invariant.

Considérons alors les $2\,p+3$ transpositions τ''_k de S_n qui sont les restrictions des τ'_k à $\mathbb{N}_n$. Elles vérifient :

$$\tau''_1 \circ \tau''_2 \circ \dots \circ \tau''_{2\,p+3} = Id$$

Donc, d'après l'hypothèse de récurrence $P(n)$ vraie, c'est absurde.

La propriété $P(n+1)$ est donc vraie. Et donc $P(n)$ est vraie pour tout $n \geq 2$.

Théorème de la signature d'une permutation

Soit $n \geq 2, \sigma$ une permutation de S_n. Soit $q \geq 2, p \geq 2$ et $p+q$ transpositions τ_k et τ'_k de S_n telles que :

$$\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_p = \tau'_1 \circ \tau'_2 \circ \ldots \circ \tau'_q$$

alors p et q sont de même parité et donc :

$$(-1)^p = (-1)^q$$

Cette dernière quantité notée $\varepsilon(\sigma)$ est appelée signature de σ.

Preuve : on a :

$$\tau_1 \circ \tau_2 \circ \ldots \circ \tau_p \circ \tau'_q \circ \ldots \tau'_2 \circ \tau'_1 = Id$$

Et d'après le lemme, $p+q$ ne peut pas être impair, donc p et q sont de même parité.