

Groupe symétrique

Dans ce chapitre, n désigne un entier naturel non nul.

I. Généralités

Définition. On appelle groupe symétrique d'ordre n et on note \mathcal{S}_n le groupe des permutation de l'ensemble $\llbracket 1, n \rrbracket$. Les éléments de \mathcal{S}_n sont appelés permutations.

Proposition. Le groupe \mathcal{S}_n est de cardinal $n!$

Soit σ une permutation de \mathcal{S}_n . On la notera

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Définition. On appelle support d'une permutation $\sigma \in \mathcal{S}_n$ l'ensemble

$$\{k \in \llbracket 1, n \rrbracket, \sigma(k) \neq k\}$$

Remarque : le support de la permutation Id est l'ensemble vide.

Définition. Soit $k \geq 2$. On dit qu'une permutation σ est un k -cycle s'il existe k entiers distincts a_1, \dots, a_k entre 1 et n tels que

$$\begin{cases} \forall p \in \llbracket 1, k-1 \rrbracket, & \sigma(a_p) = a_{p+1} \\ & \sigma(a_k) = a_1 \\ \forall p \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_k\}, & \sigma(p) = p \end{cases}$$

On note $\sigma = (a_1, \dots, a_k)$.

Un 2-cycle est appelé une transposition.

Remarque : les notations $(1, 2)$ et $(2, 1)$ représentent deux écritures possibles de la même transposition qui échange 1 et 2.

Remarque : le groupe \mathcal{S}_n n'est pas commutatif dès que $n \geq 3$.

En effet, $(1, 2, 3)(1, 2) = (1, 2, 3) \neq (2, 3) = (1, 2)(1, 2, 3)$.

Proposition. Deux permutations à support disjoints commutent.

Proposition. Soit (G, \star) un groupe de cardinal fini N et $g \in G$.

Il existe un unique $p \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z} : g^k = e\} = p\mathbb{Z}$. Cet entier p est appelé ordre de g .

On a en particulier que $p = \text{Min}\{k \in \mathbb{N}^* : g^k = e\}$

Corollaire. Soit $\sigma \in \mathcal{S}_n$

Il existe un unique $p \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z} : \sigma^k = Id\} = p\mathbb{Z}$. Cet entier p est appelé ordre de σ .

On a en particulier que $p = \text{Min}\{k \in \mathbb{N}^* : \sigma^k = e\}$

Proposition. Un k -cycle est d'ordre k .

II. Décomposition canonique d'une permutation

Définition. Soit $\sigma \in \mathcal{S}_n$ et $k \in \llbracket 1, n \rrbracket$. On appelle orbite de k sous l'action de σ l'ensemble

$$\mathcal{O}_\sigma(k) = \{\sigma^p(k), p \in \mathbb{N}\}$$

Exemple. L'orbite de 1 par la transposition $(1, 2)$ est l'ensemble $\{1, 2\}$ alors que l'orbite de 3 par la même transposition est le singleton $\{3\}$.

Proposition. Soit $\sigma \in \mathcal{S}_n$. La relation \mathcal{R} définie sur $\llbracket 1, n \rrbracket$ par

$$\forall (k, k') \in \llbracket 1, n \rrbracket^2, \quad k \mathcal{R} k' \Leftrightarrow k' \in \mathcal{O}_\sigma(k)$$

est une relation d'équivalence.

La classe d'un entier k pour cette relation est son orbite sous l'action de σ .

Les orbites sous l'action de σ forment donc une partition de $\llbracket 1, n \rrbracket$.

Proposition. Soit $\sigma \in \mathcal{S}_n$ et $k \in \llbracket 1, n \rrbracket$.

Si l'on note r le cardinal de $\mathcal{O}_\sigma(k)$, alors $\mathcal{O}_\sigma(k) = \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-1}(k)\}$ et $\sigma^r(k) = k$.

Théorème. (admis)

Soit $\sigma \in \mathcal{S}_n$ une permutation, alors σ s'écrit comme un produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près.

Proposition. Soit (a_1, a_2, \dots, a_k) un cycle. On a :

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2).$$

Proposition. Toute permutation peut s'écrire comme un produit de transpositions. On dit que les transpositions engendrent le groupe symétrique \mathcal{S}_n .

Remarque : Attention, la décomposition d'une permutation en produit de transpositions n'est pas unique et les transpositions ne sont pas à support disjoints. C'est une différence importante avec la décomposition en cycles à support disjoints.

Proposition. Soit $\sigma \in \mathcal{S}_n$ et $c = (a_1, a_2, \dots, a_k)$ un cycle. On a :

$$\sigma^{-1} \circ c \circ \sigma = (\sigma^{-1}(a_1), \dots, \sigma^{-1}(a_k)).$$

III. Signature, groupe alterné

Théorème. (admis) Il existe un unique morphisme de groupes non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$. On l'appelle signature et on le note ε .

Proposition. Toute transposition est de signature -1 .

Corollaire. La signature d'un k -cycle est égale à $(-1)^{k-1}$.

Définition. Le noyau de ε est un sous-groupe de \mathcal{S}_n appelé groupe alterné et noté \mathcal{A}_n .

Exemple. $\mathcal{A}_1 = \{Id\}$, $\mathcal{A}_2 = \{Id\}$ et $\mathcal{A}_3 = \{Id, (1, 2, 3), (1, 3, 2)\}$. Le groupe \mathcal{A}_3 est abélien. Pour $n > 3$, le groupe \mathcal{A}_n n'est pas commutatif car $(1, 2, 3)(1, 2, 4) \neq (1, 2, 4)(1, 2, 3)$.

Proposition. Soit τ une transposition de \mathcal{S}_n . L'application $\phi : \mathcal{S}_n \rightarrow \mathcal{S}_n$, $\sigma \mapsto \tau\sigma$ est involutive et donc bijective. Comme $\phi(\mathcal{A}_n) = \mathcal{S}_n \setminus \mathcal{A}_n$, on en déduit que

$$\#\mathcal{A}_n = \frac{\#\mathcal{S}_n}{2} = \frac{n!}{2}.$$