Groupe symétrique

Définition

Soit X un ensemble non vide. Une permutation de X est une bijection de X sur lui-même. L'ensemble de toutes les permutations de X se note $\mathcal{S}(X)$.

$\mathcal{S}(X)$ muni de la composition des applications est un groupe. En effet,

- la composition $\sigma_1 \circ \sigma_2$ de deux permutations $\sigma_1, \sigma_2 \in \mathcal{S}(X)$ est une permutation de X. On notera $\sigma_1 \circ \sigma_2$ simplement $\sigma_1\sigma_2$ que l'on appellera le produit de σ_1, σ_2.
- L'identité id_X est une permutation de X et c'est l'élément neutre de ce produit.
- La composition des applications est associative : $\sigma_1(\sigma_2\sigma_3) = (\sigma_1\sigma_2)\sigma_3$.
- si σ est une permutation de X alors σ^{-1} est une permutation de X (tout élément admet un inverse pour ce produit).

Définition

Soit n un entier naturel non nul. Le groupe des permutations de $X_n = \{1, \cdots, n\}$ s'appelle le groupe symétrique $\mathcal{S}_n$.

Une permutation $\sigma \in \mathcal{S}_n$ est représentée par deux lignes, la première contient les éléments de X_n et la seconde contient les images $\sigma(i), i = 1, \cdots, n$ comme suit :

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

Pour écrire σ^{-1} on inverse les lignes puis on réordonne suivant l'ordre croissant de la première ligne.

Exemples

1. $\mathcal{S}_1$ contient un seul élément l'identité. **Nous supposons dans toute la suite que** $n \geq 2$.
2. $\mathcal{S}_2$ contient deux éléments :
$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{et} \quad \tau_{12} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$
3. La permutation
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$
est un élément de $\mathcal{S}_5$. Pour écrire σ^{-1} on inverse les lignes puis on réordonne suivant l'ordre croissant de la première ligne. Ainsi
$$\sigma^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

Exemples

Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Le calcul de $\sigma\sigma'$ se fait en trois lignes comme suit :

$$\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

De même, on a

$$\sigma'\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

On remarque que $\sigma'\sigma \neq \sigma\sigma'$ et donc le produit des permutations n'est pas commutatif sur $\mathcal{S}_3$. Ainsi ce produit est non commutatif sur $\mathcal{S}_n$ pour tout $n \geq 3$.

Exemple

Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

Le calcul de $\sigma\sigma'$ se fait en trois lignes comme suit :

$$\sigma\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

De même, on a

$$\sigma'\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

Ici aussi $\sigma'\sigma \neq \sigma\sigma'$.

Théorème

Muni de la composition des applications, $\mathcal{S}_n$ est un groupe de cardinal $n!$ qui est non commutatif pour $n \geq 3$.

Démonstration : Il reste à montrer que $\mathcal{S}_n$ est de cardinal $n!$. Pour cela, il suffit de remarquer que pour définir une permutation de X_n revient à choisir une image pour 1, ce qui nous donne n possibilités, ensuite pour l'image de 2 on a $n-1$ choix, ainsi de suite pour l'image n on a un seul choix. Finalement, nous avons $n(n-1)\cdots 2 \cdot 1$ choix pour définir une permutation.

Définition

Soit $n \geq 2$ et soit $1 \leq i < j \leq n$. La permutation $\tau_{i,j}$ qui échange i et j et laisse invariants les autres éléments est appelée **transposition** et se note aussi par $(i\ j)$.

- L'inverse de la transposition $\tau_{i,j}$ est elle même.
- Les deux éléments de $\mathcal{S}_2$ sont l'identité et la transposition $(1\ 2)$.

Définition

Soit $n \geq 2$ et $2 \leq p \leq n$. Un **cycle de longueur** p, ou p-cycle, est une permutation σ pour la quelle il existe un sous-ensemble $\{i_1, \cdots, i_p\}$ de X vérifiant

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

les autres éléments restant fixes. Dans ce cas, on écrit $\sigma = (i_1\ i_2 \cdots\ i_p)$.

Notons que la représentation d'un cycle n'est pas unique. Par exemple,

$$\sigma = (1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 3\ 2).$$

On note aussi que pour obtenir l'inverse du p-cycle $\sigma = (i_1\ i_2 \cdots\ i_p)$ il suffit d'inverser l'ordre de sorte que $\sigma^{-1} = (i_p\ i_{p-1} \cdots\ i_2\ i_1)$. Notons aussi qu'une transposition est un 2-cycle.

Exemples

Voici les six éléments de $\mathcal{S}_3$:

- l'identié : $\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$;
- trois transpositions : $\tau_{12} = \begin{pmatrix} 1 & 2 \end{pmatrix}$, $\tau_{13} = \begin{pmatrix} 1 & 3 \end{pmatrix}$ et $\tau_{23} = \begin{pmatrix} 2 & 3 \end{pmatrix}$;
- deux cycles de longueur 3 :

$$c_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \quad \text{et} \quad c_2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}.$$

On remarque que, dans $\mathcal{S}_3$ on a :

$$\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

En particulier, les transpositions $(1\ 2)$ et $(1\ 3)$ ne commutent pas et donc $(\mathcal{S}_n, \cdot)$, n'est pas commutatif pour tout $n \geq 3$. En revanche, $\mathcal{S}_1$ et $\mathcal{S}_2$ sont commutatifs.

Remarque

Toute transposition est une involution : $\tau \circ \tau = \mathrm{id}$; une transposition est un cycle de longueur 2. $\mathcal{S}_n$ contient exactement $\binom{n}{2} = n(n-1)/2$ transpositions.

Définition

1. Soit σ une permutation de $\mathcal{S}_n$. Un point fixe de σ est un point $i \in X_n$ tel que $\sigma(i) = i$. L'ensemble des éléments de X_n qui ne sont pas fixes par σ est appelé *support de* σ et se note $\text{supp}(\sigma)$.
2. Deux permutations dont les supports sont disjoints sont dites disjointes.

Exemples

1. Le support de la transposition $(i\ j)$ est la paire $\{i, j\}$. Plus généralement, le support du p-cycle $\sigma = (i_1\ i_2 \cdots\ i_p)$ est $\{i_1, i_2, \cdots, i_p\}$.
2. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 4 & 2 & 1 & 7 & 6 \end{pmatrix} \in S_8$. Le support de σ est $\{1, 2, 3, 5, 6, 8\}$ et l'ensemble de ses points fixes est $\{4, 7\}$.
3. Les permutations (1 2) et (3 4 7) sont disjointes, par contre (1 2) et (1 3 4) ne sont pas disjointes.

Remarque

Notons aussi que pour toute permutation σ on a :

$$i \in \text{supp}(\sigma) \iff \sigma(i) \in \text{supp}(\sigma).$$

En effet, $i \notin \text{supp}(\sigma)$, si et seulement si $\sigma(i) = i$. Comme σ est une bijection, $\sigma(i) = i$ équivaut à $\sigma(\sigma(i)) = \sigma(i)$, ce qui signifie que $\sigma(i) \notin \text{supp}(\sigma)$.
En particulier, le support d'une permutation σ et son complémentaire sont stables par σ.

Proposition

Si deux permutations σ_1 et σ_2 sont disjointes alors elles commutent, c'est-à-dire

$$\sigma_1\sigma_2 = \sigma_2\sigma_1.$$

Démonstration Soit σ_1 et σ_2 deux permutations disjointes de $\mathcal{S}_n$. Si $i \notin \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2)$ alors $\sigma_1\sigma_2(i) = \sigma_2\sigma_1(i) = i$.

Si $i \in \text{supp}(\sigma_1)$ alors $i \notin \text{supp}(\sigma_2)$. Ainsi $\sigma_1(i) \in \text{supp}(\sigma_1)$ et $\sigma_1(i) \notin \text{supp}(\sigma_2)$. Finalement,

$$\sigma_1\sigma_2(i) = \sigma_1(i) = \sigma_2\sigma_1(i).$$

En faisant jouer le rôle de σ_1 à σ_2 et vice versa on obtient le résultat souhaité.

Exemple

Les permutations (1 2) et (3 4 7) sont disjointes et on a

$$(1\ 2)(3\ 4\ 7) = (3\ 4\ 7)(1\ 2).$$

Par contre (1 2) et (1 3 4) ne sont pas disjointes et on voit que

$$(1\ 2)(1\ 3\ 4) = (1\ 3\ 4\ 2) \text{ alors que } (1\ 3\ 4)(1\ 2) = (1\ 2\ 3\ 4).$$

Théorème

Pout toute permutation σ de $\mathcal{S}_n$ il existe un entier m tel que $\sigma^m = id$. Le plus petit de ces entiers s'appelle l'ordre de la permutation σ.

Démonstration Suit d'un résultat général sur les groupes.

Démonstration directe : D'abord on remarque que si on considère les puissances successives de σ données par

$$\sigma^0 = \mathrm{id},\ \sigma,\ \sigma^2,\ \cdots$$

on obtient un sous ensemble (sous groupe) de $\mathcal{S}_n$. Donc il y a au moins deux entiers $k < l$ tels que

$$\sigma^k = \sigma^l.$$

Ainsi, pour tout $i \in X_n$,

$$\sigma^k(i) = \sigma^l(i) = \sigma^k(\sigma^{l-k}(i)).$$

Comme σ est une permutation on déduit que, pour tout $i \in X_n$,

$$\sigma^{l-k}(i) = i.$$

Autrement dit, $\sigma^{l-k} = \mathrm{id}$. Il suffit de prendre $m = l - k$.

Exemple

Par exemple l'ordre de toute transposition est 2. L'ordre de tout cycle de longueur p est p.

Connaissant l'ordre p d'une permutation σ, on peut calculer facilement ses puissances successives en termes des premières puissances σ^r avec $r = 0, 1, \cdots, p-1$. En effet, pour chaque entier n on effectue la division euclidienne de n par p ce qui donne $n = pq + r$ avec $0 \leq r < p$. Alors

$$\sigma^n = \sigma^{pq+r} = \sigma^r.$$

Exemple

Par exemple, supposons que l'ordre de σ est 6. Alors

$$\sigma^{2020} = \sigma^4\ ,\ \sigma^{2019} = \sigma^3\ ,\ \sigma^{2018} = \sigma^2\ ,\ \sigma^{2017} = \sigma\ ,\ \sigma^{2016} = \mathrm{id}.$$

De plus, on remarque que si m est l'ordre de σ alors

$$\sigma^{-1} = \sigma^{m-1}.$$

Structure d'une permutation

Définition

Soit $\sigma \in \mathcal{S}_n$ et $i \in X_n$. On appelle **orbite** de i sous l'action σ l'ensemble $\{\sigma^k(i)\ ,\ k \in \mathbb{Z}\}$.

Théorème

Soit $\sigma \in \mathcal{S}_n$ et $i \in X_n$. Il existe un unique $p \in \mathbb{N}^*$ tel que $\{\sigma^k(i)\ ,\ k \in \mathbb{Z}\} = \{\sigma^k(i)\ ,\ 0 \leq k \leq p-1\}$. De plus, $\sigma^k(i) \neq \sigma^l(i)$ pour tout $0 \leq k \leq p-1$ et $l \neq k$.

Démonstration : Si m est l'ordre de σ alors $\sigma^m = \mathrm{id}$. En particulier, $\sigma^m(i) = i$. Il suffit ensuite de prendre p comme le plus petit des entiers k vérifiant $\sigma^k(i) = i$.

On remarque que p est plus petit que l'ordre de σ. En fait, si m est l'ordre de σ alors p divise m. En effet, grâce à la division euclidienne, il existe deux entiers q et r tels que $m = pq + r$ avec $0 \leq r < p$. Alors, comme $\sigma^m = \mathrm{id}$,

$$i = \sigma^m(i) = \sigma^{pq+r}(i) = \sigma^r(i)$$

et donc $r = 0$, car p est le plus petit entier strictement positif vérifiant $\sigma^p(i) = i$.

Remarque

1. Voici une autre façon de démontrer le théorème précédent sans utiliser la notion d'ordre. Comme l'orbite $\{i, \sigma(i), \sigma^2(i), \cdots\}$ de i est fini car inclus dans X_n, il existe deux entiers $k < l$ tels que $\sigma^k(i) = \sigma^l(i)$. Autrement dit, $\sigma^k(\sigma^{l-k}(i)) = \sigma^k(i)$, de sorte que $\sigma^{l-k}(i) = i$. Il suffit de prendre p comme le plus petit des entiers q vérifiant $\sigma^q(i) = i$.
2. Les orbites d'une permutation σ sont disjointes et forment une partition de X_n. La restriction de σ à toute orbite est un p-cycle où p est le nombre d'éléments de l'orbite en question.

Théorème

Toute permutation $\sigma \in \mathcal{S}_n$ se décompose en un produit de cycles disjoints, c'est-à-dire il existe r cycles disjoints $c_1, c_2, \cdots, c_r$ tels que

$$\sigma = c_1 c_2 \cdots c_r.$$

Cette décomposition est unique dans le sens suivant : s'il existe r' cycles disjoints $c'_1, c'_2, \cdots, c'_{r'}$ tels que $\sigma = c'_1 c'_2 \cdots c'_{r'}$ alors

$$r = r' \quad et \quad \{c_1, c_2, \cdots, c_r\} = \{c'_1, c'_2, \cdots c'_{r'}\}.$$

Démonstration On sait déjà que la propriété est vraie pour $\mathcal{S}_2$ et $\mathcal{S}_3$. Plus généralement, on procède de la façon suivante. D'abord on choisit $i_1 = 1$ et on calcule son orbite. Notons p_1 le plus petit entier p vérifiant $\sigma^p(1) = 1$. On obtient un premier cycle

$$c_1 = (i_1\ \sigma(i_1) \cdots\ \sigma^{p_1-1}(i_1)).$$

Ensuite, on considère un entier $i_2 \in X_n \setminus \{i_1, \sigma(i_1), \cdots, \sigma^{p_1-1}(i_1)\}$. On effectue la même opération et on obtient un nouveau cycle

$$c_2 = (i_2\ \sigma(i_2) \cdots\ \sigma^{p_2-1}(i_2)).$$

Il est clair que ce procédé se termine après un nombre fini d'étapes car n est fini. On obtient ainsi r cycles disjoints $c_1, c_2, \cdots, c_r$ tels que

$$\sigma = c_1 c_2 \cdots c_r.$$

La dernière identité suit du fait que les supports des c_i forment une partition de X_n et que la restriction de σ au support de c_i vaut c_i.

Supposons que σ se décompose en un produit de r cycles disjoints $c_1, c_2, \cdots, c_r$:

$$\sigma = c_1 c_2 \cdots c_r.$$

on montre facilement que les supports de $c_1, c_2, \cdots, c_r$ sont les orbites de σ. De plus, si i est un élément du support de c_k et l est la longueur de c_k alors

$$c_k = (i \ \sigma(i) \ \cdots \ \sigma^{l-1}(i))$$

Ainsi s'il existe r' cycles disjoints $c'_1, c'_2, \cdots, c'_{r'}$ tels que $\sigma = c'_1 c'_2 \cdots c'_{r'}$ alors r' est aussi le nombre des orbites de σ et donc $r = r'$. Quitte à réordonner les cycles en question on peut supposer que pour tout $k = 1, \cdots, r$, les cycles c_k et c'_k ont le même support et donc $c_k = c'_k = (i \ \sigma(i) \ \cdots \ \sigma^{l-1}(i))$ où i est un élément du support de c_k.

Exemples

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 6 & 7 & 1 & 2 & 4 \end{pmatrix} \in S_7$. On cherche l'orbite de 1 sous l'action e σ :

$$\sigma(1) = 3, \ \sigma(3) = 6, \ \sigma(6) = 2, \ \sigma(2) = 5 \ \text{ et } \ \sigma(5) = 1.$$

Le premier cycle est donné par $c_1 = (1\ 3\ 6\ 2\ 5)$. Ensuite on prend un élément de X_7 en dehors du support de ce premier cycle, par exemple 4 et on cherche son orbite :

$$\sigma(4) = 7 \ \text{ et } \ \sigma(7) = 4.$$

Le deuxième cycle est la transposition $(4\ 7)$. Finalement,

$$\sigma = (1\ 3\ 6\ 2\ 5)(4\ 7) = (4\ 7)(1\ 3\ 6\ 2\ 5).$$

Corollaire

L'ordre de toute permutation σ est le plus petit commun multiple des longueurs des cycles qui la compose.

Démonstration : Supposons que la permutation σ se décompose en produit de p_i-cycles disjoints $c_1, \cdots, c_m$. Notons $p = PPCM(p_1, \cdots, p_m)$. Il est clair que

$$\sigma^p = c_1^p c_2^p \cdots c_m^p = \text{id}.$$

Soit maintenant un entier p' tel que $\sigma^{p'} = \text{id}$. Montrons que p divise p'. Il suffit de montrer que tous les p_i divisent p'. Pour cela effectuons la division euclidienne de p' par chacun des p_i, il vient que pour tout $i = 1, \cdots, m$

$$p' = p_i q_i + r_i \ \text{ avec } q_i \in \mathbb{N} \ \text{ et } \ 0 \leq r_i < p_i.$$

Ainsi

$$\sigma^{p'} = c_1^{r_1} c_2^{r_2} \cdots c_m^{r_m} = \text{id}.$$

Soit $i \in \{1, \cdots, r\}$ et j dans le support de c_i. Donc j est un point fixe des autres $c_k, k \neq i$. Ainsi

$$\sigma^{p'}(j) = c_i^{r_i}(j) = j.$$

Ainsi $c_i^{r_i} = \text{id}$ et donc $r_i = 0$ car sinon ça contredirait le fait que $r_i < p_i$ et la définition de p_i .