

Groupes symétriques

Définition

Soit E un ensemble non vide.

On appelle permutation de E toute bijection de E et on note $S(E)$ l'ensemble des permutations de E .

En particulier, S_n est l'ensemble des permutations de $\mathbb{N}_n^* = \{1, 2, \dots, n\}$ où $n \geq 1$.

Rappel

$\text{Card}(S_n) = n!$.

Propriété

Pour tout ensemble non vide E , $(S(E), \circ)$ est un groupe.

Démonstration

En effet,

- La composée de deux bijections est une bijection.
- La loi \circ est associative.
- Id_E est bijective.
- Toute application bijective ρ admet une réciproque ρ^{-1} qui vérifie $\rho \circ \rho^{-1} = \rho^{-1} \circ \rho = \text{Id}_E$.

Remarques

- Le groupe $(S(E), \circ)$ est appelé groupe symétrique (ou groupe des permutations). En particulier, (S_n, \circ) est appelé groupe symétrique d'ordre n ou de degré n .
- De plus, si deux ensembles E et E' sont équipotents et si φ est une bijection de E dans E' , alors, l'application qui, à toute bijection σ de E , associe l'application $\varphi \circ \sigma \circ \varphi^{-1}$ est un isomorphisme de groupes de $S(E)$ dans $S(E')$. Cette dernière remarque permet de ramener l'étude du groupe des permutations d'un ensemble fini E à celle de S_n où n est le cardinal de E .

Notation

Soit l'application $\varphi : \{1, 2, 3, 4, 5, 6\} \rightarrow \{1, 2, 3, 4, 5, 6\}$

définie par : $\varphi(1) = 5$, $\varphi(2) = 2$, $\varphi(3) = 1$, $\varphi(4) = 6$, $\varphi(5) = 3$ et $\varphi(6) = 4$.

On peut représenter φ des façons suivantes :

- $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$.
- $\varphi = (1\ 5\ 3)(2)(4\ 6)$: on dit que l'on a décomposé la permutation en cycles.

Remarques

- L'objet $(1\ 5\ 3)$ est le même que $(5\ 3\ 1)$.
- Soit $\varphi = (1\ 5\ 3)(2)(4\ 6)$ et $\tau = (1\ 6\ 3\ 4)(2\ 5)$.
On a $\varphi \circ \tau = (1\ 4\ 5\ 2\ 3\ 6)$.
- On note aussi $\varphi \tau$ pour $\varphi \circ \tau$ et l'on parle de produit à la place de composition.
Mais attention, ce produit n'est pas en général commutatif.

Définition

Soient $n \in \mathbb{N}^*$, $\rho \in S_n$ et $k \in \mathbb{N}_n^*$.

On appelle orbite de k pour ρ et on note $\text{Orb}_\rho(k)$, $\text{Orb}(k)$ ou simplement $O_\rho(k)$ l'ensemble $\{\rho^p(k) / p \in \mathbb{N}\}$ avec la convention $\rho^0 = \text{Id}$.

Exemple

Soit $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \in S_6$.

On a : $\text{Orb}(1) = \{1, 3, 5\} = \text{Orb}(3) = \text{Orb}(5)$, $\text{Orb}(2) = \{2\}$ et $\text{Orb}(4) = \{4, 6\} = \text{Orb}(6)$.

Propriété

Soient $n \in \mathbb{N}^*$, $\rho \in S_n$ et $k \in \mathbb{N}_n^*$.

On a $\text{Orb}(k) = \{\rho^p(k) / p \in \mathbb{N}_{n-1}\}$.

Remarque

Cela signifie qu'il suffit de calculer un nombre fini de $\rho^p(k)$ pour avoir $\text{Orb}(k)$.

Ce nombre est au maximum n (de 0 à $n - 1$), mais ce n'est pas forcément n (voir exemple précédent).

Démonstration

Soit l'ensemble $P = \{\rho^s(k) / s \in \mathbb{N}_{n-1}\} = \{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$. P est un sous-ensemble de \mathbb{N}_n^* .

- Si P contient n éléments différents, alors $P = \mathbb{N}_n^*$ et $\forall r > n - 1, \rho^r(k) \in P$.

- Si P contient au plus $n - 1$ éléments différents.

Donc au moins deux éléments parmi $\{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$ sont égaux.

Soit i le plus petit indice tel que $\rho^i(k)$ apparaisse deux fois dans $\{k, \rho(k), \rho^2(k), \dots, \rho^{n-1}(k)\}$.

Soit j le plus petit indice différent de i tel que $\rho^i(k) = \rho^j(k)$.

On a obligatoirement $i = 0$ car sinon $\rho^{i-1}(k) = (\rho^{-1} \circ \rho^i)(k) = (\rho^{-1} \circ \rho^j)(k) = \rho^{j-1}(k)$: ce qui est contraire aux hypothèses. D'où $\rho^i(k) = k$.

Pour tout entier r , on a $r = pj + q$ avec $0 \leq q < j$ et donc $\rho^r(k) = \rho^{pj+q}(k) = \rho^q(k) \circ \rho^{pj}(k) = \rho^q(k)$.

Remarque

Avec les notations de la démonstration, on a donc $\text{Orb}_\rho(k) = \{\rho^s(k) / 0 \leq s < j\}$.

Propriété

Soient $n \in \mathbb{N}^*$ et $\rho \in S_n$.

La relation \mathcal{R}_ρ définie sur \mathbb{N}_n^* par $x \mathcal{R}_\rho y \Leftrightarrow y \in \text{Orb}_\rho(x)$ est une relation d'équivalence.

Démonstration

$\forall x \in \mathbb{N}_n^*, x = \rho^0(x)$ donc $x \mathcal{R}_\rho x$.

$\forall x, y \in \mathbb{N}_n^*$, soit i le plus petit entier non nul tel que $x = \rho^i(x)$.

$x \mathcal{R}_\rho y \Rightarrow y \in \text{Orb}_\rho(x)$

\Rightarrow il existe un entier $r \leq i$ tel que $y = \rho^r(x)$.

\Rightarrow il existe un entier $r \leq i$ tel que $\rho^{i-r}(y) = \rho^{i-r}(\rho^r(x))$.

\Rightarrow il existe un entier $r \leq i$ tel que $\rho^{i-r}(y) = \rho^i(x) = x$.

$\Rightarrow x \in \text{Orb}_\rho(y) \Rightarrow y \mathcal{R}_\rho x$.

Soit $x, y, z \in \mathbb{N}_n^*$.

$x \mathcal{R}_\rho y \Rightarrow y \in \text{Orb}_\rho(x) \Rightarrow$ il existe un entier r tel que $y = \rho^r(x)$.

$y \mathcal{R}_\rho z \Rightarrow z \in \text{Orb}_\rho(y) \Rightarrow$ il existe un entier s tel que $z = \rho^s(y)$.

On a $z = \rho^s(y) = \rho^s(\rho^r(x)) = \rho^{s+r}(x)$.

Remarques

- Soit A une orbite d'une permutation σ de S_n ($n \in \mathbb{N}^*$).
On a $\sigma(A) = A$ et la restriction de σ à A est une permutation de A .
Pour tout x de A , on a $A = \text{Orb}_\sigma(x)$.
- Soit A une orbite non réduite à un élément d'une permutation σ de S_n ($n \in \mathbb{N}^*$).
Alors $\sigma(x) \neq x$ pour tout x de A .
En effet, si $\sigma(x) = x$, alors $\text{Orb}_\sigma(x) = \{\sigma^p(x) / p \in \mathbb{N}\} = \{x\} = A$ ce qui contredit aux hypothèses.
Plus précisément, on a $A = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{p-1}(x)\}$ où p est le cardinal de A .

Définition

Soit $n \in \mathbb{N}^*$.

Une permutation de S_n est appelée un cycle si et seulement si elle ne possède qu'une seule orbite non réduite à un élément.

Exemple

Soit $\varphi = (1) (5 \ 3 \ 2 \ 6) (4) (7) (8) \in S_8$. φ est un cycle que l'on peut noter simplement $\varphi = (5 \ 3 \ 2 \ 6)$.

Remarques

- On peut aussi considérer un cycle comme la restriction d'une permutation donnée à une orbite.
- Le nombre p d'éléments du cycle $\gamma = (a_1 \ a_2 \ \dots \ a_p)$ est appelé la longueur de γ et $\{a_1 \ a_2 \ \dots \ a_p\}$ est appelé l'orbite de γ . On dit aussi que γ est un p -cycle.

Propriété

Un cycle de longueur p est d'ordre p c'est-à-dire $\gamma^p = \text{Id}$.

Propriété

Soient φ et σ deux cycles de S_n ($n \in \mathbb{N}^*$) de même longueur p .

Alors il existe une permutation u de S_n telle que $\varphi = u \circ \sigma \circ u^{-1}$.

On dit que φ et σ sont conjugués.

Démonstration

On suppose que $\varphi = (a_1 a_2 \dots a_p)$ et $\sigma = (b_1 b_2 \dots b_p)$.

Puisque $\text{card} \{b_1 b_2 \dots b_p\} = \text{card} \{a_1 a_2 \dots a_p\}$, il existe une bijection de $\{b_1 b_2 \dots b_p\}$ dans $\{a_1 a_2 \dots a_p\}$

Considérons une extension de cette bijection :

Soit $u : \mathbb{N}_n^* \rightarrow \mathbb{N}_n^*$

$$b_i \mapsto a_i$$

$$x \mapsto x \text{ si } x \notin \{b_1, b_2, \dots, b_p\}$$

Si $i \neq p$, $(u \circ \sigma \circ u^{-1})(a_i) = u(\sigma[u^{-1}(a_i)]) = u(\sigma(b_i)) = u[b_{i+1}] = a_{i+1} = \varphi(a_i)$.

Si $i = p$, $(u \circ \sigma \circ u^{-1})(a_p) = u(\sigma[u^{-1}(a_p)]) = u(\sigma(b_p)) = u[b_1] = a_1 = \varphi(a_p)$.

Et $(u \circ \sigma \circ u^{-1})(x) = x$ si $x \notin \{b_1, b_2, \dots, b_p\}$.

Définition

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

On appelle transposition de i et de j et on note $\tau_{i,j}$ la permutation de S_n définie par : $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et $\tau_{i,j}(k) = k$ pour tout $k \in \mathbb{N}_n^*$ tel que $k \neq i$ et $k \neq j$.

Remarques

- Une transposition est un cycle de longueur 2. On peut noter $\tau_{i,j} = (i j)$.
- Une transposition est une involution i.e. $\tau_{i,j} \circ \tau_{i,j} = \text{Id}$.

Propriété

Soient $n, p \in \mathbb{N}^*$ avec $p \leq n$. Soient $a_1, a_2, \dots, a_p \in \mathbb{N}_n^*$ deux à deux différents.

On a $(a_1 a_2 a_3 a_4 \dots a_p) = (a_1 a_2) (a_2 a_3) (a_3 a_4) \dots (a_{p-1} a_p)$.

Exemple

Cela donne, par exemple, $(1 2) (2 3) = (1 2 3)$

Démonstration

Soit $\varphi = (a_1 a_2) (a_2 a_3) (a_3 a_4) \dots (a_{p-1} a_p)$.

On a $\varphi(a_p) = a_1$ et $\varphi(a_i) = a_{i+1}$ pour tout $1 \leq i \leq p-1$.

Définition

Soit $n \in \mathbb{N}^*$.

On appelle permutation circulaire de S_n toute permutation (de S_n) qui ne possède qu'une seule orbite.

Exemple

Dans S_4 , $\varphi = (1 3 4 2)$ est une permutation circulaire.

Remarque

Si $n \geq 2$, une permutation circulaire de S_n est un cycle de longueur n .

Propriété

La composition (le produit) de cycles disjoints (c'est-à-dire dont l'intersection des orbites est vide) est commutative.

Remarques

- Un cycle n'intervenant que sur une seule orbite, deux cycles disjoints n'agissent que sur des entiers différents.
Par exemple, $(1\ 3\ 4)(2\ 5) = (2\ 5)(1\ 3\ 4)$.
- Mais un produit de cycles non disjoints n'est pas commutatif.
En effet, si par exemple $\rho_1 = (1\ 2)$ et $\rho_2 = (2\ 3)$, on a $\rho_1 \circ \rho_2 = (1\ 2\ 3)$ et $\rho_2 \circ \rho_1 = (1\ 3\ 2)$.

Propriété

Toute permutation se décompose en une composition (un produit) de cycles disjoints et cette décomposition est unique à l'ordre près des cycles.

Remarque

On obtient simplement cette décomposition en considérant les cycles sur les différentes orbites en ne conservant que celles non réduites à un élément.

Exemple

Soit l'application $\varphi : \{1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{1, 2, 3, 4, 5, 6, 7, 8\}$ définie par :
 $\varphi(1) = 5, \varphi(2) = 7, \varphi(3) = 6, \varphi(4) = 4, \varphi(5) = 8, \varphi(6) = 3, \varphi(7) = 2$ et $\varphi(8) = 1$.
On a $\varphi = (1\ 5\ 8)(2\ 7)(3\ 6)$.

Propriété

Pour tout entier $n \geq 2$, S_n est engendré par ses transpositions.

Remarques

- Cela signifie que toute permutation peut s'exprimer comme une composition (un produit) de transpositions.
- Cette décomposition n'est pas unique.

Exemples

- Soit $\rho = (1\ 3\ 4)(2\ 3)$.
On a $\rho = (1\ 3)(3\ 4)(2\ 3)$.
- Soit $\rho = (1\ 2\ 3)$.
On a $\rho = (1\ 2)(2\ 3)$ mais aussi $\rho = (1\ 3)(1\ 2)$.

Démonstration 1

On raisonne par récurrence sur le nombre n de S_n .

- Si $n = 2$, $S_2 = \{\text{Id}, \tau_{1,2}\}$ avec $\text{Id} = \tau_{1,2} \circ \tau_{1,2}$.

- On suppose la propriété vraie au rang $n - 1$ et soit $\rho \in S_n$.
 Si $\rho(n) = n$ alors la restriction de ρ à $\{1, 2, \dots, n - 1\}$ appartient à S_{n-1} et ρ en a la même décomposition en transpositions.
 Si $\rho(n) = m \neq n$, alors $\tau_{n,m} \circ \rho$ est une permutation de S_n qui vérifie $(\tau_{n,m} \circ \rho)(n) = n$.
 Nous sommes donc dans le cas précédent et $\rho = \tau_{n,m} \circ (\tau_{n,m} \circ \rho)$ avec $\tau_{n,m} \circ \rho$ qui peut se décomposer en produit de transpositions.

Démonstration 2

Cela découle directement du fait que tout cycle peut se décomposer en un produit de transpositions.

Propriété

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

Si $j > i$, alors $\tau_{i,j} = \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \dots \circ \tau_{j-2,j-1} \circ \tau_{j-1,j} \circ \tau_{j-2,j-1} \circ \dots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1}$.

Démonstration

Si $\rho = (i \ i+1) (i+1 \ i+2) \dots (j-2 \ j-1) (j-1 \ j) (j-2 \ j-1) \dots (i+1 \ i+2) (i \ i+1)$, on a :
 $\rho(j) = i$, $\rho(i) = j$ et $\rho(k) = k$ pour tout $i < k < j$ (car k apparaît dans 2 transpositions).

Corollaire

Pour tout entier $n \geq 2$, S_n est engendré par les transpositions du type $\tau_{i, i+1}$ où $1 \leq i \leq n - 1$.

Remarque

Le nombre de transpositions d'une décomposition d'une permutation peut varier. Mais nous allons voir que la parité de ce nombre reste la même.

Définition

Soit $n \in \mathbb{N}^*$ et soient $i, j \in \mathbb{N}_n^*$.

On dit que le couple (i, j) présente une inversion pour une permutation ρ de S_n si $i < j$ et $\rho(i) > \rho(j)$.

Exemple

Soit $\rho = (1 \ 4 \ 2)$ dans S_4 . On doit étudier le signe de $\rho(j) - \rho(i)$:

i	j	$\rho(j) - \rho(i)$
1	2	-3
1	3	-1
1	4	-2
2	3	2
2	4	1
3	4	-1

Il y a en tout C_4^2 couples (i, j) possibles. Quatre couples présentent une inversion.

Remarque

Soit $n \in \mathbb{N}^*$. Il y a C_n^2 couples (i, j) tels que $i, j \in \mathbb{N}_n^*$ et $i < j$.

Le produit $p = \prod_{i < j} (j - i)$ est un entier positif.

Soit $\varphi \in S_n$, on s'intéresse à $p' = \prod_{i < j} (\varphi(j) - \varphi(i))$.

Si l'on reprend l'exemple précédent, $\rho = (1\ 4\ 2)$ dans S_4 , on a :

$p = (2 - 1)(3 - 1)(4 - 1)(3 - 2)(4 - 2)(4 - 3) = (1)(2)(3)(1)(2)(1)$ et $p' = (-3)(-1)(-2)(2)(1)(-1)$.

On remarque que p' et p ne peuvent différer que par le signe. Le nombre de soustractions qui changent de signe est égale au nombre d'inversions.

Définition

Soit $n \in \mathbb{N}^*$ et soit $\varphi \in S_n$.

On appelle signature de φ et on note $\sigma(\varphi)$ le nombre $\sigma(\varphi) = \frac{\prod_{i < j} \varphi(j) - \varphi(i)}{\prod_{i < j} (j - i)}$.

Si $\sigma(\varphi) > 0$, on dit que φ est paire.

Si $\sigma(\varphi) < 0$, on dit que φ est impaire.

Exemple

Toujours avec le même exemple, $\rho = (1\ 4\ 2)$ dans S_4 , on a $\sigma(\rho) = 1$.

Propriété

Soit l le nombre d'inversions d'une permutation φ de S_n où $n \geq 2$.

On a $\sigma(\varphi) = (-1)^l$ et donc $\prod_{i < j} (\varphi(j) - \varphi(i)) = (-1)^l \prod_{i < j} (j - i)$.

Remarque

$$\prod_{i \neq j} (\varphi(j) - \varphi(i)) = (-1)^l \prod_{i \neq j} (j - i).$$

Démonstration

Soit $\varphi \in S_n$. On a $\varphi(\mathbb{N}_n^*) = \mathbb{N}_n^*$.

D'où $\prod_{i, j \in \{1, \dots, n\}} (\varphi(j) - \varphi(i)) = \prod_{a, b \in \{1, \dots, n\}} (b - a)$ et donc $\prod_{i < j} (|\varphi(j) - \varphi(i)|) = \prod_{i < j} (|j - i|)$.

Etant donné que $j - i$ est positif et que seuls les couples présentant une inversion sont tels que $\varphi(j) - \varphi(i) < 0$, le signe de $\prod_{i < j} (\varphi(j) - \varphi(i))$ dépend du nombre d'inversions de φ .

Remarques

- La parité d'une permutation est donc égale à la parité du nombre total d'inversions qu'elle produit.
- La signature d'une transposition est -1 .

Exemple

Avec $\rho = (1\ 4\ 2)$ dans S_4 , on a $\sigma(\rho) = (-1)^4$ et ρ paire.

Propriété

La signature est un morphisme de groupe de (S_n, \circ) dans $(\{-1, 1\}, \times)$ c'est-à-dire :

$\forall f, g \in S_n$, on a $\sigma(f \circ g) = \sigma(f) \times \sigma(g)$.

Démonstration

On a $\prod_{i < j} ((f \circ g)(j) - (f \circ g)(i)) = \sigma(f \circ g) \prod_{i < j} (j - i)$.

Or $\prod_{i < j} (f[g(j)] - f[g(i)]) = \sigma(f) \prod_{i < j} (g(j) - g(i)) = \sigma(f) \sigma(g) \prod_{i < j} (j - i)$.

Remarque

Le noyau de ce morphisme (c'est-à-dire l'ensemble des permutations de S_n de signature 1) est appelé groupe alterné d'ordre n et on le note A_n .

Les éléments de A_n sont appelés les permutations paires et ceux de $S_n \setminus A_n$ les permutations impaires.

Corollaire

Soit m le nombre de transpositions dans une décomposition quelconque d'une permutation φ de S_n où $n \geq 2$. On a $\sigma(\varphi) = (-1)^m$.

Remarque

Ce dernier corollaire donne une méthode plus rapide que les précédentes pour déterminer la signature d'une permutation.

Par exemple, si $\varphi = (1\ 2\ 6)(4\ 5)$ dans S_6 , on a $\varphi = (1\ 2)(2\ 6)(4\ 5)$ et $\sigma(\varphi) = -1$.

Propriété

Soit φ une permutation de S_n et m son nombre d'orbites.

On a $\sigma(\varphi) = (-1)^{n-m}$.