Groupe symétrique

Extrait du programme officiel :

Le groupe symétrique est introduit exclusivement en vue de l'étude des déterminants.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Généralités	
Groupe des permutations de l'ensemble $\{1,\dots,n\}$.	Notation S_n.
Cycle, transposition.	Notation $(a_1\ a_2\ \dots\ a_p)$.
Décomposition d'une permutation en produit de cycles à supports disjoints : existence et unicité.	La démonstration n'est pas exigible, mais les étudiants doivent savoir décomposer une permutation. Commutativité de la décomposition.
b) Signature d'une permutation	
Tout élément de S_n est un produit de transpositions.	
Signature : il existe une et une seule application ε de S_n dans $\{-1,1\}$ telle que $\varepsilon(\tau)=-1$ pour toute transposition τ et $\varepsilon(\sigma\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$ pour toutes permutations σ et σ'.	La démonstration n'est pas exigible.

Table des matières

I PERMUTATIONS

1 Définition

La première utilisation historique du mot groupe (dans le sens actuel) est due à Évariste Galois [1] qui travaillait sur les racines d'un polynôme et s'autorisait en particulier à les permuter.

Définition : Permutation, groupe symétrique

Si E est un ensemble, on appelle ***permutation*** de E toute bijection de E dans E. On note $\mathfrak{S}(E)$ leur ensemble.

Si $E = \mathbb{N}_n = [\![1, n]\!]$ où $n \in \mathbb{N}^*$, on note $\mathfrak{S}_n$ appelé ***groupe symétrique d'ordre n (ou de degré n)*** cet ensemble.

Si $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Remarque

Attention ! $\mathfrak{S}_n$ n'est pas de cardinal n mais ... $n!$ (!)
(n choix pour $\sigma(1)$ puis $n-1$ pour $\sigma(2)$ etc. et un seul pour $\sigma(n)$.)

Propriété

$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre (ie de cardinal) $n!$, non abélien dès que $n \geqslant 3$.

Démonstration

C'est une groupe car $\circ$ est une loi associative sur $\mathbb{N}_n^{\mathbb{N}_n}$, l'élement neutre est $\mathrm{id}_{\mathbb{N}_n} \in \mathfrak{S}_n$ et si $\sigma, \rho \in \mathfrak{S}_n$, $\sigma \circ \rho \in \mathfrak{S}_n$ et σ est bijective d'inverse $\sigma^{-1} \in \mathfrak{S}_n$.

De plus, avec les notations qui seront vu dans le paragraphe suivant,

$$(1\ 2) \circ (1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3) \circ (1\ 2).$$

Si $n = 2$, $\mathfrak{S}_2 = \{\mathrm{id}, (1\ 2)\}$ est commutatif. □

1. 

Évariste Galois (Bourg-la-Reine 1811 - Paris 1832) est un mathématicien français. Sa principale découverte est la non résolubilité par radicaux, en général, des équations polynomiales de degré au moins 5. Sa biographie est un véritable roman : son caractère belliqueux lui vaut un échec au concours d'"entrée à l'École Polytechnique (il aurait lancé le chiffon à craie à la figure de l'examinateur) à la suite de quoi il entre à l'École Préparatoire (future École Normale) de laquelle il sera renvoyé. Il envoie ses travaux sur les polynômes à l'Académie des Sciences, mais son mémoire est emporté par Fourier qui meurt entre temps, et donc perdu. Il réécrit plus tard ce mémoire qui sera jugé incompréhensible par Poisson et Lacroix. Il connaît la prison et meurt à 21 ans dans un duel à l'épée pour les beaux yeux d'une demoiselle. La nuit précédant sa mort, il couche sur le papier toutes ses dernières découvertes. Ses travaux ne seront reconnus qu'une dizaine d'années après sa mort.

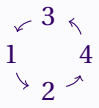
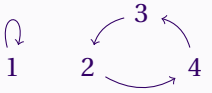
Remarque

Si E est fini de cardinal n, on construit sans mal une bijection entre E et $\mathbb{N}_n$ et on en déduit que $\mathfrak{S}(E) \simeq \mathfrak{S}_n$ (isomorphisme de groupes).

Exemple

Soit, dans $\mathfrak{S}_4$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

Alors $\sigma \circ \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ et $\sigma' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ (regarder les images successives par les deux permutations.) De plus $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ et $\sigma'^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \sigma'$ (échanger la première et la deuxième ligne.) Représentation par orbites :

σ :		$\sigma' = \sigma'^{-1}$:	
$\sigma \circ \sigma'$:		$\sigma' \circ \sigma$:	
σ^{-1} : (On a juste inversé les flèches de σ)			

2 Ordre d'une permutation

Définition

L'ordre d'une permutation σ est le plus petit $k \in \mathbb{N}^*$ tel que $\sigma^k = \mathrm{id}$.

Remarque

Cette définition se généralise aux éléments de n'importe quel groupe $(G, *)$: g est d'ordre fini si et seulement s'il existe $p \in \mathbb{N}^*$ tel que $g^p = e_G$.

Si on considère le noyau du morphisme de groupes $k \in \mathbb{Z} \mapsto g^k$ qui est un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ unique, n est l'ordre de g et $g^p = e_G \iff n | p$.

Propriété

L'ordre d'une permutation de $\mathfrak{S}_n$ est bien défini et vaut au plus l'ordre $n!$ de ce groupe.

Démonstration

Les σ^p pour $p \in [\![1, n!+1]\!]$ sont dans $\mathfrak{S}_n$ qui continent $n!$ éléments : il y en a forcément deux égaux. Donc on a $1 \leqslant p \leqslant p' \leqslant n!+1$ tels que $\sigma^p = \sigma^{p'}$.

Alors, par bijectivité, $\sigma^{p'-p} = \mathrm{id}$. □

Remarque

Le théorème de Lagrange affirme qu'en fait, cet ordre divise $n!$.

3 Orbites et support

Définition : Orbites

Soit $\sigma \in \mathfrak{S}_n$. La relation binaire définie sur $\mathbb{N}_n$ par

$$x \sim y \iff \exists\, k \in \mathbb{Z},\quad y = \sigma^k(x)$$

est une relation d'équivalence dont les classes d'équivalence sont les **orbites** de σ.

Si $x \in [\![1, n]\!]$,

$$\mathcal{O}(x) = \left\{\sigma^k(x) \mid k \in \mathbb{Z}\right\}.$$

Remarque

Une orbite n'est jamais vide, elle est réduite à un point si set seulement si celui-ci est invariant par σ. Les orbites sont finies (car incluses dans $[\![1, n]\!]$) et forment une partition de $[\![1, n]\!]$ (comme pour toute relation d'équivalence). Elles sont en particulier disjointes.

Exemple

Pour σ, $\mathcal{O}(1) = \mathcal{O}(2) = \mathcal{O}(3) = \mathcal{O}(4) = \{1,2,3,4\}$ et pour σ', $\mathcal{O}(1) = \mathcal{O}(3) = \{1,3\}$, $\mathcal{O}(2) = \{2\}$ et $\mathcal{O}(4) = \{4\}$.

Propriété

Soit $\sigma \in \mathfrak{S}_n$, $x \in [\![1, n]\!]$. Alors il existe $\ell \in \mathbb{N}$ tel que $\mathcal{O}(x) = \{x, \sigma(x), \ldots, \sigma^{\ell-1}(x)\}$ (deux à deux distincts).

Démonstration

$\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\}$ est une partie non vide de $\mathbb{N}$ donc admet un minimum ℓ.

Il suffit ensuite, si $k \in \mathbb{Z}$, de poser la division euclidienne de k par ℓ. Les éléments sont bien distincts par minimalité de ℓ. □

Remarque

$\ell \leqslant \mathrm{ordre}(\sigma)$.

Définition : Support

Si $\sigma \in \mathfrak{S}_n$, son ***support*** est l'ensemble des éléments de $\mathbb{N}_n$ qui **ne sont pas** invariants par σ.

Exemple

Avec les permutations de l'exemple précédent, $\text{Supp}(\sigma) = \{1,2,3,4\}$ et $\text{Supp}(\sigma') = \{1,3\}$.

Remarque

C'est la réunion de toutes les orbites non réduites à un élément.

Propriétés

(i) $\text{Supp}(\sigma)$ *est stable par* σ.

(ii) Deux permutations à supports disjoints commutent.

Démonstration

(i) Si $i \in \text{Supp}(\sigma)$, $\sigma(i) \neq i$ donc $\sigma^2(i) \neq \sigma(i)$ par injectivité, donc $\sigma(i) \in \text{Supp}(\sigma)$.

(ii) Soient σ et σ' à support S et S' disjoints.
- Si $i \notin S \cup S'$, $\sigma \circ \sigma'(i) = i = \sigma' \circ \sigma(i)$.
- Si $i \in S$, $i \notin S'$ donc $\sigma'(i) = i$ et $\sigma \circ \sigma'(i) = \sigma(i)$.
  Mais $\sigma(i) \in S$ donc $\sigma(i) \notin S'$ d'où $\sigma' \circ \sigma(i) = \sigma(i) = \sigma \circ \sigma'(i)$.
- Si $i \notin S$, $i \in S'$ et on conclut de la même manière.

On a donc bien $\sigma' \circ \sigma = \sigma \circ \sigma'$.

□

4 Transpositions, cycles

On suppose ici $n \geqslant 2$.

Définition : Transposition

Une ***transposition*** τ est une permutation qui échange deux éléments i et j de $\mathbb{N}_n$, et laisse les autres invariants *ie* dont le support est $\{i, j\}$.

On la note $\tau = (i\ j)$ ou parfois $\tau_{i,j}$.

$\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$ et si $k \notin \{i, j\}$, $\tau_{i,j}(k) = k$.

Exemple

Pour $n = 5$, $\tau_{2,4} = (2\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$.

Remarques

R1 – Il y a $\binom{n}{2} = \dfrac{n(n-1)}{2}$ permutations dans $\mathfrak{S}_n$.

R2 – (i j)=(j i).

R3 – Toute transposition est une involution ($\tau^2 = \mathrm{id}$), donc d'ordre 2.
En particulier, $(i\ j)^{-1} = (i\ j) = (j\ i)$.
La réciproque est fausse pour $n \geqslant 4$ car si $\sigma = (1\ 2)(3\ 4)$, $\sigma^2 = \mathrm{id}$.

Définition : Cycle

Soit $p \in \mathbb{N}$ tel que $2 \leqslant p \leqslant n$.
On appelle ***p*-cycle** une permutation c de $\mathfrak{S}_n$ qui permute circulairement p éléments $i_1, i_2, \ldots, i_n$ de $\mathbb{N}_n$ et laisse les autres invariants *ie* dont le support est $\{i_1, \ldots, i_p\}$ et telle que

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

p est la ***longueur*** du cycle c. On note $c = (i_1\ i_2\ \cdots\ i_p)$.

Exemple

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} = (2\ 5\ 3) = (5\ 3\ 2) = (3\ 2\ 5) \neq (2\ 3\ 5).$$

Remarques

R1 – $(i_1\ i_2\ \cdots\ i_p) = (i_2\ i_3\ \cdots\ i_p\ i_1) = (i_p\ i_1\ i_2\ \cdots\ i_{p-1})$.

R2 – Les 2-cycles sont les transpositions.

R3 – Un cycle de longueur n dans $\mathfrak{S}_n$ est appelé permutation circulaire de $\mathbb{N}_n$. Il y en a exactement $(n-1)!$.

R4 – Le nombre de p-cycles dans $\mathfrak{S}_n$ est $\binom{n}{p}(p-1)! = \dfrac{n(n-1)\cdots(n-p+1)}{p}$ (deux calculs possibles).

R5 – Les cycles sont les permutations possédant exactement une orbite non réduite à un point.

Propriété

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

(ii) Un p-cycle est d'ordre p.

Démonstration

Il suffit de regarder directement les images de chaque entier. □

Exercice

Montrer que si σ est une permutation, alors $\sigma(i_1\ i_2\ \cdots\ i_p)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_p))$.

Théorème

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

Démonstration

- **Analyse** : Si on a une décomposition en produit de cycles à support disjoints, alors pour tout $x \in \mathbb{N}_n$, soit x est invariant, soit x est un élément d'un et un seul des cycles qui s'écrit $\begin{pmatrix} x & \sigma(x) & \dots & \sigma^p(x) \end{pmatrix}$ avec $\sigma^{p+1}(x) = x$ et correspond donc à l'orbite de x.
- **Synthèse** : Soient $x_1, \dots, x_m$ un élément de chaque orbite non réduite à un point. Alors $\mathcal{O}(x_i) = \{x_i, \sigma(x_i), \dots, \sigma^{\ell_i - 1}(x_i)\}$ avec $\sigma^{\ell_i}(x_i) = x_i$ et

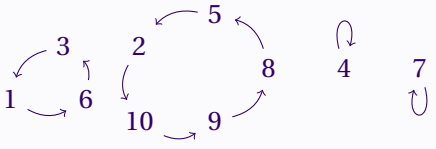
$$\varphi = \prod_{i=1}^{m} \begin{pmatrix} x_i & \sigma(x_i) & \dots & \sigma^{\ell_i}(x_i) \end{pmatrix}$$

est égale à σ car les images sont les mêmes pour tout élément de $\mathbb{N}_n$, chacun apparaissant dans exactement une orbite.

□

Exemple

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$. Représentation :



- Orbite de 1 : $\{1,3,6\}$.
- Orbite de 2 : $\{2,10,9,8,5\}$.
- Orbite de 4 : $\{4\}$.
- Orbite de 7 : $\{7\}$.

Alors $\sigma = (1\ 3\ 6)(2\ 10\ 9\ 8\ 5) = (2\ 10\ 9\ 8\ 5)(1\ 3\ 6)$.
Avec la proposition précédente, on tire d'ailleurs, par exemple,

$$\sigma = (2\ 5)(2\ 8)(2\ 9)(2\ 10)(1\ 3)(3\ 6) = (2\ 10)(10\ 9)(9\ 8)(8\ 5)(1\ 6)(1\ 3).$$

Remarque

Par commutativité des cycles à supports disjoints, on a facilement que si m est le ppcm des ordres des cycles, $\sigma^m = \mathrm{id}$. On peut même montrer que le ppcm est égal à l'ordre de σ.

Corollaire

Toute permutation se décompose en produit de transpositions.

Remarque

On dit qu'un groupe G est engendré par un ensemble A lorsque tout élément du groupe est un produit d'éléments ou d'inverses d'éléments de A. C'est le plus petit groupe contenant tous les éléments de A. C'est l'analogue du Vect des espaces vectoriels.

On a donc ici que les transpositions de $\mathfrak{S}_n$ engendrent $\mathfrak{S}_n$.

II MORPHISME DE SIGNATURE ET SOUS-GROUPE ALTERNÉ

On fixe $n \in \mathbb{N}^*$.

1 Signature d'une permutation

Définition : Inversions, signature

Soit $\sigma \in \mathfrak{S}_n$. On appelle ***inversion*** par σ tout couple (i,j) tel que $i<j$ et $\sigma(i)>\sigma(j)$.

On note $I(\sigma)$ le nombre d'inversions par σ.

On appelle ***signature*** de σ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1,1\}$.

Une permutation σ est dite ***paire*** lorsque $I(\sigma)$ est pair et donc $\varepsilon(\sigma)=1$. Elle est dite ***impaire*** dans le cas contraire.

Détermination pratique du nombre d'inversions :

Pour chaque nombre de la deuxième ligne (image), on compte le nombre de nombres plus petits situés à sa droite. Et on fait la somme.

Exemple

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$.

Ici,

Terme	3	10	6	4	2	1	7	5	8	9
Nombre d'inversions	2	8	4	2	1	0	1	0	0	0

$I(\sigma) = 2+8+4+2+1+1 = 18$. σ est donc paire car $\varepsilon(\sigma)=1$.

Propriété

Toute transposition est impaire.

Démonstration

- Si $\tau = (i\ i{+}1)$ où $i \in [\![1, n-1]\!]$, $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & 3 & \cdots & i+1 & i & \cdots & n \end{pmatrix}$. La seule inversion par τ est donc $(i, i+1)$. Ainsi, $\varepsilon(\tau) = -1$.
- Si, plus généralement, $\tau = (i\ j)$, $i < j$,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & i-1 & i & i+1 & \cdots & j-1 & j & j+1 & \cdots & n \\ 1 & 2 & 3 & \cdots & i-1 & j & i+1 & \cdots & j-1 & i & j+1 & \cdots & n \end{pmatrix}.$$

Les inversions par τ sont donc

$$(i, i+1), (i, i+2), \ldots, (i, j-1)\ ;\ (i, j)\ ;\ (i+1, j), (i+2, j), \ldots, (j-1, j)$$

et $I(\tau) = 2(j-i-1)+1$ et donc $\varepsilon(\tau) = -1$.

□

Théorème

Soit $n \geqslant 2$. L'application $\varepsilon : \left| \begin{array}{ccc} (\mathfrak{S}_n, \circ) & \longrightarrow & (\{-1,1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{array} \right.$ *est un morphisme de groupe, ie si $\sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.*

Démonstration : (Non exigible)

Il s'agit de comparer les nombres d'inversions de $\sigma \circ \sigma'$ aux nombres d'inversions de σ et de σ'.

Les couples $(i, j) \in \mathbb{N}_n$ tels que $i < j$, se classent en quatre cas distincts :

- $\sigma'(i) < \sigma'(j)$ et $\sigma \circ \sigma'(i) < \sigma \circ \sigma'(j)$ (on note N_1 le nombre de tels couples.)
- $\sigma'(i) < \sigma'(j)$ et $\sigma \circ \sigma'(i) > \sigma \circ \sigma'(j)$ (on note N_2 le nombre de tels couples.)
- $\sigma'(i) > \sigma'(j)$ et $\sigma \circ \sigma'(i) < \sigma \circ \sigma'(j)$ (on note N_3 le nombre de tels couples.)
- $\sigma'(i) > \sigma'(j)$ et $\sigma \circ \sigma'(i) > \sigma \circ \sigma'(j)$ (on note N_4 le nombre de tels couples.)

Le nombre d'inversion $I(\sigma')$ de σ' est le nombres de couples $(i, j) \in \mathbb{N}_n$ tels que $i < j$ tels que $\sigma'(i) > \sigma'(j)$:

$$I(\sigma') = N_3 + N_4.$$

Le nombre d'inversion $I(\sigma \circ \sigma')$ de $\sigma \circ \sigma'$ est le nombres de couples $(i, j) \in \mathbb{N}_n$ tels que $i < j$ tels que $\sigma \circ \sigma'(i) > \sigma \circ \sigma'(j)$:

$$I(\sigma \circ \sigma') = N_2 + N_4.$$

Pour le nombre d'inversions de σ, il y a un peu plus de travail : remarquons que $(i, j) \mapsto \{\sigma'(i), \sigma'(j)\}$ est une bijection de l'ensemble des couples (i, j) de $\mathbb{N}_n$ tels que $i < j$ dans l'ensemble des paires de $\mathbb{N}_n$ par bijectivité de σ'.

Or compter les couples (k, l), $k < l$ tels que $\sigma(k) > \sigma(l)$ revient

— à compter les paires $\{k,l\}$ distinctes telles que

$$\begin{cases} k<l \\ \sigma(k)>\sigma(l) \end{cases} \text{ ou } \begin{cases} k>l \\ \sigma(k)<\sigma(l) \end{cases}$$

— ou encore, par la bijection précédente, à compter les couples (i,j) de $\mathbb{N}_n$ tels que $i<j$ et

$$\begin{cases} \sigma'(i)<\sigma'(j) \\ \sigma(\sigma'(i))>\sigma(\sigma'(j)) \end{cases} \text{ ou } \begin{cases} \sigma'(i)>\sigma'(j) \\ \sigma(\sigma'(i))<\sigma(\sigma'(j)) \end{cases}$$

Ainsi,

$$I(\sigma) = N_2 + N_3.$$

Finalement, $\varepsilon(\sigma)\varepsilon(\sigma') = (-1)^{2N_3+N_2+N_4} = (-1)^{N_2+N_4} = \varepsilon(\sigma\sigma')$. □

Propriétés

(i) Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.

(ii) Si $\sigma \in \mathfrak{S}_n$ se décompose en produit de N transpositions, $\varepsilon(\sigma) = (-1)^N$.
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.

(iii) ε est le seul morphisme de groupes de $\mathfrak{S}_n$ dans $\{-1,1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ. (C'est en fait aussi le seul morphisme de groupe surjectif.)

(iv) Si c est un p-cycle, $\varepsilon(c) = (-1)^{p-1}$.

(v) Si $\sigma \in \mathfrak{S}_n$, $\varepsilon\left(\sigma^{-1}\right) = \varepsilon(\sigma)$.

Remarque

L'autre morphisme de groupes est $\sigma \mapsto 1$.
Si pour un transposition τ, $\varphi(\tau) = -1$, alors si τ' est une autre transposition, on a $\sigma \in \mathfrak{S}_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$ et donc $\varphi(\tau') = -1$. Les deux seuls morphismes sont donc ε et $\sigma \mapsto 1$.

Démonstration

(i) car $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.
(ii) Avec des notations évidentes et par récurrence, $\varepsilon(\tau_1 \cdots \tau_N) = \varepsilon(\tau_1)\cdots\varepsilon(\tau_N) = (-1)^N$.
(iii) Facile avec (ii).
(iv) Avec le (ii) et les décompositions précédentes des p-cycles, par exemple

$$(i_1\ i_2\ \cdots\ i_p) = (i_1\ i_p)(i_1\ i_{p-1})\cdots(i_1\ i_2).$$

(v) $\varepsilon\left(\sigma^{-1}\right) = \varepsilon(\sigma)^{-1} = \varepsilon(\sigma)$ car ε est un morphisme de groupe puis car $\varepsilon(\sigma) \in \{-1,1\}$. □

Exercice

Montrer que si $\sigma \in \mathfrak{S}_n$ et si p est le nombre d'orbites de σ, alors $\varepsilon(\sigma) = (-1)^{n-p}$.

2 Groupe alterné

Définition

Le sous-groupe $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon)$ des permutations paires de $\mathfrak{S}_n$ est appelé ***groupe alterné d'ordre n (ou de degré n).***

On a bien $\mathfrak{A}_n = \mathrm{Ker}(\varepsilon) = \varepsilon^{-1}(\{1\}) = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\}$ sous-groupe de $\mathfrak{S}_n$.

Propriété

Pour tout $n \geqslant 2$, $|\mathfrak{A}_n| = \dfrac{n!}{2}$.

Démonstration

Soit τ une transposition (ou n'importe quelle autre permutation impaire), $\varphi : \left|\begin{array}{ccc} \mathfrak{A}_n & \longrightarrow & \mathfrak{S}_n \setminus \mathfrak{A}_n \\ \sigma & \longmapsto & \tau \circ \sigma \end{array}\right.$ est bijective, d'inverse $\psi : \left|\begin{array}{ccc} \mathfrak{S}_n \setminus \mathfrak{A}_n & \longrightarrow & \mathfrak{A}_n \\ \rho & \longmapsto & \tau^{-1} \circ \rho \end{array}\right.$.

Ainsi, ces sous-ensembles de $\mathfrak{S}_n$ (donc finis) vérifient $|\mathfrak{A}_n| = |\mathfrak{S}_n \setminus \mathfrak{A}_n|$ et $|\mathfrak{A}_n| + |\mathfrak{S}_n \setminus \mathfrak{A}_n| = |\mathfrak{S}_n| = n!$ donc $|\mathfrak{A}_n| = \dfrac{n!}{2}$. □

Remarque

Il y a donc autant de permutations paires que de permutations impaires dans $\mathfrak{S}_n$.

Exemple

Décrivons $\mathfrak{S}_4$: il contient $4! = 24$ permutations.

$$\begin{aligned}\mathfrak{S}_4 = \{&\mathrm{id}, (1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)\circ(3\,4), (1\,3)\circ(2\,4), (1\,4)\circ(2\,3)\\ &(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3),\\ &(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}\end{aligned}$$

et

$$\begin{aligned}\mathfrak{A}_4 = \{&\mathrm{id}, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3),\\ &(1\,2)\circ(3\,4), (1\,3)\circ(2\,4), (1\,4)\circ(2\,3)\}\end{aligned}$$

(Il y a bien $\dfrac{4!}{2} = 12$ permutations paires.)

Soit $G = \{\mathrm{id}, \sigma_1 = (1\,2)\circ(3\,4), \sigma_2 = (1\,3)\circ(2\,4), \sigma_3 = (1\,4)\circ(2\,3)\}$.

Il s'agit d'un sous-groupe commutatif de $\mathfrak{A}_4$ comme l'atteste sa table ci-contre, appelé groupe de Klein[1].

On peut montrer qu'il est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ et que tout groupe d'ordre 4 est soit isomorphe au groupe de Klein, soit isomorphe à $(\mathbb{Z}/4\mathbb{Z}, \times)$ (ou de manière équivalente $(\mathbb{U}_4, \times)$. Cf cours sur les groupes.)

$\circ$	id	σ_1	σ_2	σ_3
id	id	σ_1	σ_2	σ_3
σ_1	σ_1	id	σ_3	σ_2
σ_2	σ_2	σ_3	id	σ_1
σ_3	σ_3	σ_2	σ_2	id

Remarque

On peut facilement trouver des sous-groupes de $\mathfrak{A}_4$ d'ordre 1, 2, 3, 4, et 12 mais il n'y a pas de sous-groupe d'ordre 6. On peut démontrer que ceux-ci sont soit cycliques (mais $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6), soit isomorphes au groupe diédral D_6 des isométries du triangle équilatéral (contenant 3 rotations et 3 symétries). On en trouve dans $\mathfrak{S}_4$ engendrés par un 3-cycle et une transposition facilement isomorphe à D_6 (qui est aussi isomorphe à $\mathfrak{S}_3$, par ailleurs !).

1. 

Felix Klein (Düsseldorf 1849 - Göttingen 1925) Mathématicien allemand ayant contribué en théorie des groupes, géométrie non euclidienne et en analyse.