

Groupe Symétrique

GS[1]

déf: X un ensemble, une permutation de X est
une bijection de X vers X .

Pour ce cours, on va considérer le cas où
 X est un ensemble fini de n éléments.

exemple: $X = \{1, 2, 3, 4\}$, $f: X \rightarrow X$
 $1 \mapsto 2$
 $2 \mapsto 3$
 $3 \mapsto 1$
 $4 \mapsto 4$

on notera les permutations comme

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

On notera par $\tilde{S}_n$ l'ensemble des permutations
de X , un ensemble fini de n éléments.

Comme composition de deux bijections est une
bijection, la composition définit une opération
sur $\tilde{S}_n$. c.a.d.

$$\begin{aligned} o: \tilde{S}_n \times \tilde{S}_n &\longrightarrow \tilde{S}_n \\ (f, g) &\longmapsto f \circ g \end{aligned}$$

THM 2.1 $(\tilde{S}_n, o)$ forment "un groupe"
c.a.d. la composition satisfait les
propriétés suivantes

(1) associativité: $\forall f, g, h \in \tilde{S}_n \quad (f \circ g) \circ h = f \circ (g \circ h)$

(2) $\exists$ un élément neutre, id , tq $\forall f \in \tilde{O}_n$
 $f \circ id = id \circ f = f$

(3) chaque élément possède un symétrique :
 $\forall f \in \tilde{O}_n, \exists \tilde{f} \in \tilde{O}_n$ tq $f \circ \tilde{f} = \tilde{f} \circ f = id$

Remarque: théoriquement parlant

- la composée est associative car la composée des applications est associative

- l'application identité étant une bijection est dans $\tilde{O}_n$ ainsi $\exists$ une identité

- Puisque $\tilde{O}_n$ contient que des bijections chaque élément possède une inverse

démonstration: (1) associativité :

Soit $f, g, h \in \tilde{O}_n$

d'un côté $\forall x \in X, (f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x)))$

de l'autre $\forall x \in X, f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x)))$

ainsi $\forall x \in X, (f \circ g) \circ h(x) = f \circ (g \circ h)(x)$

$$\Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$$

(2) élément neutre: Soit $X = \{1, 2, 3, \dots, n\}$

considérons $id = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$

$\forall f \in \tilde{O}_n$ $f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$

(3) l'inverse: Soit $f \in \mathcal{O}_n$ $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$

on consider $\tilde{f} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix} \leftarrow \begin{array}{l} \text{just change} \\ \text{les lignes sur} \\ f \end{array}$

$$f \circ f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} = \text{id}, \quad f \circ \tilde{f} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} = \text{id}$$

□

exemple: $X = \{1, 2, 3, 4\}$ $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

$$f^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} \xrightarrow[\text{en reordonnant}]{\quad} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Remarque: la composition n'est pas toujours commutative.

eg. $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

THM 2.2: l'ensemble $\mathcal{O}_n$ est fini et de cardinalité $n!$

dém: On va calculer tous les possible bijections sur $\{1, 2, \dots, n\}$ en regardant l'image possible

$1 \longrightarrow n$ possibilité pour choisir image
 $2 \longrightarrow n-1$ par injectivité il nous reste
 $\vdots$ $n-1$ choix
 $n-1 \longrightarrow 2$
 $n \longrightarrow 1$

Donc, $n(n-1)(n-2)\dots 3.2.1 = n!$ possibilités des bijections sur X .

□.

exemples: $X = \{1\}$ $\tilde{\mathcal{O}}_1 = \{\text{id}\}$ $\text{card } \tilde{\mathcal{O}}_1 = 1$
 $X = \{1, 2\}$ $\tilde{\mathcal{O}}_2 = \{\text{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$, $\text{card } \tilde{\mathcal{O}}_2 = 2! = 2$
 $X = \{1, 2, 3\}$ $\tilde{\mathcal{O}}_3 = \left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$
 $\text{card } \tilde{\mathcal{O}}_3 = 3! = 6$

Notons que spécialement, puisqu'il contient que deux éléments $(\tilde{\mathcal{O}}_2, \circ)$ forme un groupe commutative tandis que à partir de $n \geq 2$ ce ne serait pas le cas.

Quelques éléments spéciale de $\tilde{\mathcal{O}}_n$

(1) Transposition: Soit $i, j \in \{1, \dots, n\}$ on considère $\sigma \in \tilde{\mathcal{O}}_n$ tq.

supposons $i < j$ pour écriture $\rightarrow \sigma = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$

σ échange i et j garde fix tout les autres.

σ s'appelle une transposition, on notera par $\sigma = (ij)$.

(2) un k -cycle : soit $2 \leq k \leq n$ et

$$\{a_1, \dots, a_k\} \subseteq X$$

soit $\sigma: X \rightarrow X$

$$a_1 \rightarrow a_2$$

$$a_2 \rightarrow a_3$$

$$\vdots$$

$$a_{k-1} \rightarrow a_k$$

$$x \mapsto x \quad \forall x \in X \setminus \{a_1, \dots, a_k\}$$

$$\left. \begin{array}{l} a_1 \rightarrow a_2 \\ a_2 \rightarrow a_3 \\ \vdots \\ a_{k-1} \rightarrow a_k \end{array} \right\} \sigma(a_s) = a_{s+1} \quad \forall s \in \{1, \dots, k-1\} \\ \text{et } \sigma(a_k) = a_1.$$

on notera les k -cycle par $\sigma = (a_1 a_2 \dots a_k)$

Remarque: (1) une transposition est un 2-cycle

(2) l'inverse de k -cycle est un k -cycle.

THM 2.3 Tous élément de $\tilde{S}_n$, $n \geq 2$ s'écrit comme composition des transpositions.

Remarque: A partir de là on va prendre un langage plus abstrait donc au lieu de composition des bijections on va dire produit des permutations

ainsi Thm 2.3 devient

THM 2.3: tous élément de $\tilde{S}_n$, $n \geq 2$ s'écrit comme un produit des transpositions

démonstration: Récurrence sur n .

I $n=2$ $\tilde{S}_2 = \{id, (1 \underset{2}{2})\}$

τ est une transposition donc un produit de proposition.

$\text{id} = \tau \cdot \tau^{-1} = \tau \cdot \tau$ donc id est un produit des transpositions.
 $\uparrow$
car l'inverse de transposition est soit même.

[H] Supposons que l'assertion est vrai pour le rang n . c.a.d.

tous élément de $\mathcal{O}_n$ s'écrit comme un produit des transpositions.

$\forall \sigma \in \mathcal{O}_{n+1}$, soit $\sigma(n+1) = n+1$
soit $\sigma(n+1) \neq n+1$

Si $\sigma(n+1) = n+1$ on considère $\sigma' = \sigma|_{\{1, \dots, n\}}$

c.a.d. $\sigma' = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ puisque $\sigma(n+1) = n+1$ on peut l'oublier.

ainsi $\sigma' \in \mathcal{O}_n$ et donc par l'hypothèse

σ' s'écrit comme un produit des transposition

Puisque $\sigma(n+1) = n+1$ ainsi σ s'écrit comme un produit des transpositions.

Si $\sigma(n+1) \neq n+1$ la semaine prochaine!

si $\sigma(n+1) \neq n+1$ considérons la transposition

$\tau = (\sigma(n+1), n+1)$ qui échange $n+1$ et $\sigma(n+1)$

Soit $\eta = \tau \circ \sigma$ (à lire comme $\tau \sigma$)

$$= (\sigma(n+1), n+1) \sigma$$

Ainsi $\eta(n+1) = n+1$ donc par les discussions précédentes η s'écrit comme produit des transpositions or $\sigma = \tau^{-1} \circ \eta = \tau \circ \eta$ donc σ est un produit des transpositions.

□

Soit $\sigma \in \mathcal{S}_n$, considérons

$I_\sigma = \{(i, j) : i < j \text{ et } \sigma(i) > \sigma(j)\}$, les éléments de cet ensemble I_σ s'appellent les "inversions".

Soit $\ell(\sigma) = \text{card}(I_\sigma)$, le nombre des inversions de σ .

déf. $\forall \sigma \in \mathcal{S}_n$ on définit la signature de σ noté, $\varepsilon(\sigma)$, comme le nombre $(-1)^{\ell(\sigma)}$.

eg. $\varepsilon(\text{id}) = (-1)^0 = 1$ car il n'y a aucun inversions.

Remarque Une formule pour $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \text{sign}[\sigma(j) - \sigma(i)]$

(2) c'est aussi bien voir ε comme une application

$$\varepsilon: \mathfrak{S}_n \longrightarrow \{\pm 1\}$$

$$\sigma \longmapsto \begin{cases} 1 & \text{si } \exists \text{ un nombre pair d'inversions} \\ -1 & \text{si } \exists \text{ un nombre impair d'inversions} \end{cases}$$

THM 24: $\forall \sigma, \eta \in \mathfrak{S}_n$

$$\varepsilon(\sigma \circ \eta) = \varepsilon(\sigma) \cdot \varepsilon(\eta)$$

↑
produit des nombres

De plus, si τ est une transposition alors

$$\varepsilon(\tau) = -1$$

dém: d'abord on démontre $\varepsilon(\tau) = -1$:

$$\text{Soit } \tau = (i \ j) = \begin{pmatrix} 1 & 2 & \dots & i-1 & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

Comptons les inversions pour τ :

- $\forall \{k, l\} \notin \{i, j\}$ pas d'inversions

- (i, j) inversion

- si $k=i$ et $l \neq j$ $\forall l \in \{i+1, \dots, j-1\}$ on a des inversions.

- si $l=j$ et $k \neq i$ $\forall k \in \{i+1, \dots, j-1\}$ on a des inversions

total nombre des inversions donc

$$2(j-1-(i+1)+1) + 1 = \underbrace{2(j-i-1)+1}_{\text{un nombre impair}}$$

Donc, $\varepsilon(\tau) = (-1)^{2(j-i-1)+1} = -1$

Pour montrer $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \varepsilon(\tau)$, on va utiliser

$$\forall \sigma \in \mathcal{S}_n \quad \varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(j) - \sigma(i))$$

Notons que

$$\varepsilon(\sigma \circ \tau) = \prod_{1 \leq i < j \leq n} \text{sign}(\sigma \circ \tau(j) - \sigma \circ \tau(i))$$

et

$$\begin{aligned} \varepsilon(\sigma) \cdot \varepsilon(\tau) &= \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(j) - \sigma(i)) \cdot \prod_{1 \leq i < j \leq n} \text{sign}(\tau(j) - \tau(i)) \\ &= \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(j) - \sigma(i)) \cdot \text{sign}(\tau(j) - \tau(i)) \end{aligned}$$

Soit $a = \min\{\tau(i), \tau(j)\}$ et $b = \max\{\tau(i), \tau(j)\}$

on a donc $a < b$.

Si $\tau(j) > \tau(i)$ alors $(\Rightarrow \tau(j) \text{ max}, \tau(i) \text{ min})$

$$\sigma(\tau(j)) - \sigma(\tau(i)) = \sigma(b) - \sigma(a)$$

Si $\tau(j) < \tau(i)$ alors $(\Rightarrow \tau(j) \text{ min}, \tau(i) \text{ max})$

$$\sigma(\tau(j)) - \sigma(\tau(i)) = \sigma(a) - \sigma(b) = -(\sigma(b) - \sigma(a))$$

$$\text{OR si } \eta(j) > \eta(i) \quad \text{sign}(\eta(j) - \eta(i)) = +$$

$$\text{si } \eta(j) < \eta(i) \quad \text{sign}(\eta(j) - \eta(i)) = -$$

Ainsi on peut écrire

$$\text{sign}(\sigma(\eta(j)) - \sigma(\eta(i))) = \text{sign}(\sigma(b) - \sigma(a)) \text{sign}(\eta(j) - \eta(i))$$

Alors

$$\varepsilon(\sigma \circ \eta) = \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(\eta(j)) - \sigma(\eta(i)))$$

$$= \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(b) - \sigma(a)) \text{sign}(\eta(j) - \eta(i))$$

$$= \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(b) - \sigma(a)) \underbrace{\prod_{1 \leq i < j \leq n} \text{sign}(\eta(j) - \eta(i))}_{\varepsilon(\eta)}$$

Puisque η est une bijection quand

i, j varient de 1 à n $\max\{z(i), z(j)\}$

$\min\{z(i), z(j)\}$ varient de 1 à n de plus

$$\min\{z(i), z(j)\} < \max\{z(i), z(j)\}$$

$$\text{ainsi } \prod_{1 \leq i < j \leq n} \text{sign}(\sigma(b) - \sigma(a)) = \prod_{\substack{1 \leq a < b \leq n \\ \text{par defn } \varepsilon(\sigma)}} \text{sign}(\sigma(b) - \sigma(a))$$

□.

Proposition 2.5: $\forall \sigma \in \tilde{S}_n$ on a $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ AS [6]

dém: On a $\sigma \circ \sigma^{-1} = \text{id} \Rightarrow \varepsilon(\sigma \circ \sigma^{-1}) = \varepsilon(\text{id}) = 1$

$$\Rightarrow \varepsilon(\sigma) \cdot \varepsilon(\sigma^{-1}) = 1$$

THM 2.4

$$\Rightarrow \varepsilon(\sigma^{-1}) = \frac{1}{\varepsilon(\sigma)} = \varepsilon(\sigma)^{-1}$$

$\varepsilon(\sigma) \neq 0$

OR $\varepsilon(\sigma) \in \{\pm 1\}$ si $\varepsilon(\sigma) = 1 \Rightarrow \varepsilon(\sigma^{-1}) = \frac{1}{1} = 1$

si $\varepsilon(\sigma) = -1 \Rightarrow \varepsilon(\sigma^{-1}) = \frac{1}{-1} = -1$

Donc, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma) \quad \forall \sigma \in \tilde{S}_n$

□.

Corollaire 2.6: $\forall \sigma \in \tilde{S}_n$, La PARITÉ du nombre des transpositions dans une décomposition de σ en produit de transposition ne dépend que de σ

dém: Soit $\sigma = \tau_1 \dots \tau_r = \tau'_1 \dots \tau'_s$

$$\varepsilon(\sigma) = \varepsilon(\tau_1 \dots \tau_r) = \varepsilon(\tau_1) \dots \varepsilon(\tau_r) = (-1)^r$$

|| THM 2.4

$$\varepsilon(\tau'_1 \dots \tau'_s) = \varepsilon(\tau'_1) \dots \varepsilon(\tau'_s) = (-1)^s$$

THM 2.4

Ainsi $(-1)^r = \varepsilon(\sigma) = (-1)^s \Rightarrow r \equiv s \pmod{2}$

Remarque: Par le corollaire précédent on peut calculer $\varepsilon(\sigma) = (-1)^k$ où k le nombre des transpositions sur une décomposition. □.

