PLAN DU COURS

Théorie élémentaire des
I. ~~Rappel sur les~~ groupes
II Systèmes linéaires
III Algèbre matricielle
IV Déterminants
V Valeurs propres et vecteurs propres

Théorie élémentaire
I ~~Rappel sur~~ des groupes
0. Introduction

Bien des concepts math. se présentent comme unification, généralisations et simplification de méthodes et outils utilisés dans de nombreux cas particuliers. Historiquement, on constate des périodes où les mathématiciens font des rapprochements entre des résultats en essayant de dégager des idées communes et en "oubliant" les particularités propres à chaque situation : c'est ce qu'on appelle la démarche axiomatique.
La notion de groupe est issue de cette démarche.
Les groupes sont omniprésents en physique,
Vous les trouverez en particulier :

- en relativité restreinte : groupe des transformations de Lorentz, groupe de Poincaré
- en théorie des champs : groupes de jauge
- en physique des particules :
  groupe $U(1)$ (electromagnétisme)

SU(2) (interaction faible)
SU(3) (interaction forte)

- en cristallographie : groupes cristallographiques
- et d'en n'importe quel système physique : groupe des symétries du système (sous lequel les équations de la physique doivent être invariantes), par exemple si vous voulez savoir résoudre le Rubik's cube à coup sûr...

1. Lois de composition interne

Déf : Une loi de composition interne sur un ensemble E est une application $\star$ de $E \times E$ dans E.
Elle est dite :

- commutative si pour tout $x \in E$, $y \in E$,
  $x \star y = y \star x$
- associative si $\forall x, y, z \in E$,
  $x \star (y \star z) = (x \star y) \star z$

On dit que la loi $\star$ admet un élément neutre s'il existe $e \in E$ tq $\forall x \in E$ $x \star e = e \star x = x$.

Rque : Pour une loi donnée, E possède <u>au plus</u> un élément neutre. En effet, si e et e' désignent deux éléments neutres, on doit avoir $e \star e' = e = e'$.

Déf : Soit un ensemble E muni d'une loi de composition interne $\star$. On dit que $x \in E$ admet un inverse si il existe

$y \in E$ avec $x \star y = y \star x = e$

Rque: Si la loi est associative et si x possède un inverse, cet inverse est unique. En effet si y_1 et y_2 désignent deux inverses de x, on a:

$$x \star y_1 = x \star y_2 = e \quad \text{et}$$
$$\Leftrightarrow (y_1 \star x) \star y_1 = (y_1 \star x) \star y_2$$
$$\Leftrightarrow \quad y_1 = y_2 .$$

Déf: La table de Pythagore d'une loi $\star$ sur un ensemble fini s'obtient en écrivant dans un tableau les différents résultats de $x \star y$

Ex:

$\star$	a	b
a	$a \star a$	$a \star b$
b	$b \star a$	$b \star b$

2. Groupes:

a. Définition d'un groupe:

Déf: Soit G un ensemble muni d'une loi de composition interne $\star : G \times G \longrightarrow G$. On dit que cette loi détermine sur G une structure de groupe si
1. elle est associative
2. elle possède un élément neutre
3. chaque élément de G possède un inverse.

Déf: Soit $(G, \star)$ un groupe. Si $\star$ est commutative on dit que G est un groupe commutatif ou abélien.

Exemples de groupes :

a. $\{-1, 1\}$ avec le produit

$\cdot$	1	-1
1	1	-1
-1	-1	1

élément neutre 1, (-1) est son propre inverse

b. $(\mathbb{Z}, +)$ élément neutre $= 0$ car $n + 0 = 0 + n = n$
inverse de $n = -n$

c. $(\mathbb{R}^*, \times)$ élément neutre $= 1$ car $1 \times x = x \times 1 = x$
inverse de $x = \frac{1}{x} = x^{-1}$

d. ensemble des bijections d'un ensemble E
avec pour loi la composition des applications $\circ$
élément neutre = application identité $E \to E$
inverse de $f : E \to E$ = bijection inverse

e. groupe des rotations : composer deux rotations donne une rotation, l'inverse d'une rotation d'angle θ est la rotation d'angle $-\theta$.

⚠ Il y a deux notations communément utilisées pour un groupe abstrait
- s'il est commutatif, on peut désigner la loi par un $+$, l'élément neutre par un 0_G et l'inverse de x par $-x$.
- dans tous les cas, on peut utiliser la notation multiplicative $\times$ ou $\cdot$, l'élément neutre est alors désigné par 1_G ou e et l'inverse de x par x^{-1}.

DANS LA SUITE, ON UTILISE LA NOTATION MULTIPLICATIVE. AINSI $x \cdot y$ signifie $x \star y$

Premières propriétés :

1. Dans un groupe $ax = b$ a une solution unique $x = a^{-1}b$
2. $ax = bx \Leftrightarrow a = b$. De même $xa = xb \Leftrightarrow a = b$.
3. L'inverse de xy est $y^{-1}x^{-1}$. En effet

$$xy \cdot y^{-1}x^{-1} = x(y \cdot y^{-1})x^{-1} = x e x^{-1} = x x^{-1} = e$$

b. Sous-groupes :

Déf : Soient G un groupe et H une partie de G. On dit que H est un sous-groupe de G si H est non-vide et si $\forall x, y \in H$, $xy^{-1} \in H$.
De façon équivalente, H est un sous-groupe de G si
1. $e \in H$
2. $x, y \in H \Rightarrow xy \in H$
3. $x \in H \Rightarrow x^{-1} \in H$

Ex : a. $\{e\}$ et G sont des sous-groupes de G
b. $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$
c. $\{1, -1\}$ est un sous-groupe de $(\mathbb{R}^*, \times)$
d. $\{$identité, rotations d'angle $\pi/2$, π et $3\pi/2\}$ forme un sous-groupe du groupe des rotations

c. Morphisme de groupes :

Déf : Soit $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. Un morphisme de groupe de G_1 vers G_2 est une application $f : G_1 \longrightarrow G_2$ tq $\forall x, y \in G_1$,

$$f(\underbrace{x \star_1 y}_{\in G_1}) = \underbrace{f(x) \star_2 f(y)}_{\in G_2}$$

<u>Rque</u>: Automatiquement 1. $f(e_1) = e_1$
2. $f(x^{-1}) = f(x)^{-1}$

<u>Déf</u>: Soit f un morphisme de groupes $f : G_1 \longrightarrow G_2$
- Le noyau de f est l'ensemble des antécédents de l'élément neutre de G_2 : $\operatorname{Ker} f = f^{-1}(e_2)$
- L'image de f est l'ensemble des images par f des éléments de G_1 : $\operatorname{Im} f = \{ f(x), x \in G_1 \}$

<u>Prop</u>: Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes.
Alors $\operatorname{Ker} f$ est un sous-groupe de G_1
$\operatorname{Im} f$ —————————— " —— G_2

<u>Dem</u>: - Soient $x, y \in \operatorname{Ker} f$. On a :

$$f(x *_1 y^{-1}) = f(x) *_2 f(y^{-1}) = f(x) *_2 f(y)^{-1}$$
$$= e_2 *_2 e_2^{-1} = e_2$$
$$\Rightarrow x *_1 y^{-1} \in \operatorname{Ker} f$$

- Soient $z, t \in \operatorname{Im} f$, alors il existe $x, y \in G_1$ tels que $z = f(x)$ et $t = f(y)$. Alors

$$z *_2 t^{-1} = f(x) *_2 f(y)^{-1} = f(x *_1 y^{-1})$$
$$\in \operatorname{Im} f.$$

d. <u>Ordre d'un élément dans un groupe</u>:

<u>Déf</u>: Soit G un groupe. L'ordre de G est le nombre d'éléments de G. On le note $|G|$ ou $\operatorname{card} G$

<u>Déf</u>: On dit qu'un groupe est d'ordre fini ou simplement fini s'il possède un nombre fini d'éléments.

Déf: On appelle sous-groupe engendré par x le plus petit sous-groupe qui contient x. C'est l'ensemble des x^n, $n \in \mathbb{Z}$
avec $x^n = \underbrace{x * x * \dots * x}_{n \text{ fois}}$, $n \in \mathbb{N}$ et $x^{-n} = \underbrace{x^{-1} * \dots * x^{-1}}_{n\text{-fois}}$, $x^0 = e$

Ex: Le sous-groupe du groupe des rotations engendré par la rotation d'angle $\pi/2$ est l'ensemble $\{$identité, rotations d'angle $\pi/2$, π et $3\pi/2\}$.

Déf: L'ordre d'un élément $x \in G$ est le nombre d'éléments (donc l'ordre) du sous-groupe engendré par x.

Ex: La rotation d'angle $\pi/2$ est un élément d'ordre 4 du groupe des rotations.

Prop: L'ordre de $x \in G$ est le plus petit entier n non nul tq $x^n = e$.

Thm de Lagrange:
Si H est un sous-groupe d'un groupe fini G alors l'ordre de H divise l'ordre de G.
En particulier, l'ordre d'un élément de G divise l'ordre de G.

Dem: Les ensembles de la forme $xH = \{xh, h \in H\}$ ont exactement card$H$ éléments. Deux tels ensembles sont soit disjoints soit confondus.
En effet soient $x_1 H$ et $x_2 H$ deux tels ensembles. Si $x_1 H \cap x_2 H \neq \emptyset$, il existe $y \in x_1 H \cap x_2 H$. Alors $y = x_1 h_1 = x_2 h_2$.

Mais cela implique $x_2 = x_1 h_1 h_2^{-1}$ donc $x_1 H = x_2 H$.
Finalement G se partitionne en sous-ensembles de la forme xH $\Rightarrow$ card G est un multiple de card H.

PAUSE ...

3. Le groupe symétrique :

a. Permutations :

Déf : On appelle permutation de $\{1, \dots, n\}$ une application bijective de l'ensemble $\{1, \dots, n\}$ sur lui-même.

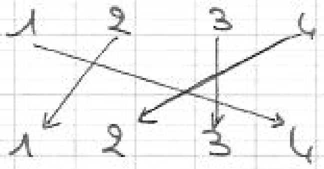
Notation : Une permutation σ de $\{1, \dots, n\}$ s'écrit

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

Ex : $n = 4$

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

Représentation graphique :



Prop : L'ensemble des permutations de $\{1, \dots, n\}$ muni de la loi $(\sigma_1, \sigma_2) \mapsto \sigma_1 \circ \sigma_2$ forme un groupe à $n!$ éléments. On l'appelle le groupe symétrique et on le note S_n.

Dem : - la composition est associative : $\sigma_1 \circ (\sigma_2 \circ \sigma_3) = (\sigma_1 \circ \sigma_2) \circ \sigma_3$
- l'élément neutre est l'application identité

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

- l'inverse d'une permutation est la bijection inverse.

- Pour définir une permutation σ, on choisit sur quel nombre est envoyé 1 : n choix possibles

______________________ 2 : $(n-1)$ possibilités

– – – " – – – – . . $\vdots$ $\vdots$

______________________ n : 1 possibilité

Au total : $n!$ possibilités

$\Rightarrow S_n$ a $n!$ éléments.

<u>Rque</u>: Pour $n \geq 3$, S_n n'est pas un groupe commutatif. Par exemple $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ne commutent pas.

En effet :

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

=  = 

<u>Déf</u> : Le support d'une permutation σ est l'ensemble des éléments de $\{1, \dots, n\}$ bougés par σ

$$\operatorname{Supp} \sigma = \{ i \in \{1, \dots, n\} , \sigma(i) \neq i \}$$

<u>Ex</u> : $\operatorname{Supp} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \{1, 2\}$

<u>Propriété</u> : Deux permutations à supports disjoints commutent.

<u>Ex</u> : $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

$\operatorname{Supp} \sigma_3 = \{1, 2\}$ $\operatorname{Supp} \sigma_4 = \{3, 4\}$

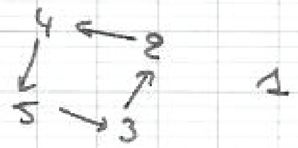
$\Rightarrow \sigma_3 \circ \sigma_4 = \sigma_4 \circ \sigma_3$

⚠ Deux permutations σ_1 et σ_2 dont les supports s'intersectent ne vont en général pas commuter ! Dans l'exemple ci-dessus $\operatorname{Supp} \sigma_1 = \{1, 2, 3\} = \operatorname{Supp} \sigma_2$ et $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$.

b. Cycles :

<u>Déf</u> : Un cycle de longueur m ou m-cycle de support $\{k_1, \dots, k_m\}$ est une permutation σ telle que $k_1 \xrightarrow{\sigma} k_2 \xrightarrow{\sigma} k_3 \mapsto \dots \mapsto k_{m-1} \xrightarrow{\sigma} k_m \xrightarrow{\sigma} k_1$ et tout $k \notin \{k_1, \dots, k_m\}$ est laissé fixe par σ.

<u>Ex</u> : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$



<u>Notation</u> : Un m-cycle tel que $k_1 \xrightarrow{\sigma} k_2 \mapsto \dots \mapsto k_{m-1} \mapsto k_m \mapsto k_1$ est noté $(k_1\ k_2 \dots k_{m-1}\ k_m)$. Ainsi l'image d'un élément de la liste est le suivant dans la liste, et l'image du dernier est le premier. Les éléments qui n'apparaissent pas dans la liste ne sont pas bougés.

<u>Ex</u> : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix} = (2\ 4\ 5\ 3)$

<u>Rque</u> : On a le choix de l'élément de tête dans l'écriture d'un m-cycle : un m-cycle a m écritures.

<u>Ex</u> : $\sigma = (2\ 4\ 5\ 3) = (4\ 5\ 3\ 2) = (5\ 3\ 2\ 4)$
$= (3\ 2\ 4\ 5)$

<u>Notation</u> : la composée $c_1 \circ c_2$ de deux cycle
$c_1 = (k_1 \dots k_m)$ et $c_2 = (k_1' \dots k_{m'}')$
s'écrit
$c_1 \circ c_2 = (k_1 \dots k_m)(k_1' \dots k_{m'}')$. On l'appelle aussi : le produit de c_1 et c_2 par référence à la notation multiplicative du groupe S_n (mais attention à l'ordre !)

Comment effectuer un produit de cycle ?

<u>Ex</u>: $\sigma = \underbrace{(1\ 2)}_{c_1}\underbrace{(1\ 3\ 2)}_{c_2} = c_1 \circ c_2$

$\sigma(1) = c_1(c_2(1)) = c_1(3) = 3$
$\sigma(2) = c_1(c_2(2)) = c_1(1) = 2$
$\sigma(3) = c_1(c_2(3)) = c_1(2) = 1$

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

<u>Thm</u>: Toute permutation se décompose en un produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près des éléments.

fin du cours 1
2005

<u>Ex</u> : $n = 8$ $\quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 5 & 6 & 3 & 2 & 1 & 8 \end{pmatrix}$

On a : $1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1$

La décomposition de σ contient le cycle $c_1 = (1\ 4\ 6\ 2\ 7)$. Ensuite on prend un élément qui n'appartient pas au support de c_1, par exemple 3. On a $3 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 3$. On a obtenu un deuxième cycle $c_2 = (3\ 5)$* Comme on a utilisé tous les chiffres de 1 à 8, on s'arrête là.

* il reste 8 : on a un troisième cycle à 1 élément : (8).

Alors $\sigma = c_1 \circ c_2 \circ c_3$
$= (1\ 4\ 6\ 2\ 7)(3\ 5)(8)$
$= (3\ 5)(1\ 4\ 6\ 2\ 7)$

<u>Proposition</u> : l'ordre d'un cycle est égal à sa longueur : un m-cycle est d'ordre m.

($k \in \mathbb{N}$) Plus généralement, $c^k =$ identité si et seulement si k est multiple de la longueur de c.

Dem: Si $c = (k_1 \dots k_m)$, par définition,

$$c^m(k_1) = \underbrace{c \circ c \dots \circ c}_{m\text{-fois}}(k_1) = \underbrace{c \circ \dots \circ c}_{(m-1)\text{-fois}}(k_2) = \dots$$
$$= c(k_m) = k_1 .$$

De même $c^m(k_j) = k_j \quad \forall j \in \{1, \dots, k\}$

Donc c^m est l'application identité, élément neutre du groupe S_n. De plus, m est le plus petit entier tel que c^m = identité car $\forall j = 1, \dots, m-1$, $c^j(k_1) = k_{j+1} \neq k_1$.

Il reste à montrer que c^k = identité $\Leftrightarrow m \mid k$ (m divise k).

$\Leftarrow$ Si $m \mid k$ alors k s'écrit $k = pm$ et
$$c^k = c^{pm} = (c^m)^p = (\text{identité})^p = \text{identité}$$

$\Rightarrow$ Si c^k = identité, on sait déjà que $k \notin \{1, \dots, m-1\}$ (voir ci-dessus). Effectuons la division euclidienne de k par m:
$$k = pm + \underbrace{r}_{\text{reste de la division euclidienne}} \quad \text{où } r \in \{0, 1, \dots, m-1\}$$

Alors $c^k = c^{pm+r} = c^{pm} \circ c^r = \underbrace{(c^m)^p}_{\text{identité}} \circ c^r = c^r$

Ainsi $c^r = c^k$ = identité

avec $r \in \{0, 1, \dots, m-1\} \Rightarrow r = 0$ et k est multiple de m.

Corollaire: L'ordre d'une permutation est le PPCM (plus petit commun multiple) des ordres des cycles qui composent sa décomposition en produit de cycles à support disjoints.

Dem: Soit $\sigma = c_1 \circ c_2 \circ \dots \circ c_k$ la décomposition de σ en cycles à supports disjoints. Posons

m_i l'ordre de c_i et $m = \text{PPCM}(m_i)$. On a
$\sigma^m = (c_1 \circ c_2 \circ \dots \circ c_k)^m = c_1^m \circ c_2^m \circ \dots \circ c_k^m$ car
les c_i commutent. De plus, comme les supports des
c_i sont disjoints, σ^m = identité si et seulement si
c_i^m = identité pour tout i. D'après la proposition
précédente, m est multiple de tous les m_i, c-à-d
m est multiple du $\text{ppcm}(m_i)$.

__Ex__ : $\sigma = (3\ 5)(1\ 4\ 6\ 2\ 7)$ est d'ordre
$\text{ppcm}(2,5) = 10$.

__Thm:__ (Formule de conjugaison)
Soit un m-cycle $(k_1 \dots k_m)$. Pour toute
permutation σ, on a :

$$\sigma \circ \underbrace{(k_1\ k_2\ \dots\ k_m)}_{\text{cycle de longueur } m} \circ \sigma^{-1} = \underbrace{(\sigma(k_1)\ \sigma(k_2) \dots \sigma(k_m))}_{\text{cycle de longueur } m}$$

__Dem:__ En effet : $\sigma(k_i) \xrightarrow{\sigma^{-1}} k_i \xrightarrow{\text{cycle}} k_{i+1} \xrightarrow{\sigma} \sigma(k_{i+1})$

__Ex__ : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}$

$\sigma \circ (1\ 3\ 4\ 5\ 2) \circ \sigma^{-1} = (4\ 5\ 6\ 3\ 7)$

c. __Transpositions :__

__Déf:__ Une transposition de $\{1, \dots, n\}$ est une permutation
dont le support possède exactement deux éléments :
une transposition échange deux éléments de $\{1, \dots, n\}$

__Ex__ : $(1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ ou $(5\ 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$

Proposition : Les transpositions engendrent S_n : tout élément σ de S_n peut s'écrire comme produit (non-unique) de transposition (pas nécessairement à supports disjoints).

Dem : Par récurrence sur n :

- vrai pour $n=1$ ou $n=2$.
- supposé établi pour $n-1$. Soit $\sigma \in S_n$

  1^e cas : $\sigma(n)=n$, alors σ permute seulement les $(n-1)$ premiers entiers. Par hypothèse de récurrence, σ est produit de transpositions.

  2^e cas : $\sigma(n) = m \neq n$. Alors $(n\ m) \circ \sigma$ laisse fixe n, donc est un produit de transpositions $c_1 \circ \dots \circ c_k$ par le 1^e cas. Ainsi

  $\sigma = (n\ m)^{-1} \circ c_1 \circ \dots \circ c_k = (n\ m) \circ c_1 \circ \dots \circ c_k$

  est aussi un produit de transpositions.

Rque : Un m-cycle peut s'écrire comme un produit de $(m-1)$ transposition. En effet

$$(k_1 \dots k_m) = (k_1 k_2)(k_2 k_3) \dots (k_{m-1}\ k_m).$$

d. Signature d'une permutation :

Déf : Pour toute permutation $\sigma \in S_n$, on appelle signature de σ et on note $\varepsilon(\sigma)$ le nombre

$$\varepsilon(\sigma) = \frac{\prod_{1 \leq i < j \leq n} (\sigma(i) - \sigma(j))}{\prod_{1 \leq i < j \leq n} (i - j)} \qquad (*)$$

Ex: $n=3$: les couples (i,j) tels que $1 \leq i < j \leq 3$ sont $(1,2)$; $(1,3)$ et $(2,3)$.
Ainsi, pour tout $\sigma \in S_3$, le numérateur et le dénominateur de $\mathcal{E}(\sigma)$ contiennent un produit de 3 termes.
Prenons $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$\mathcal{E}(\sigma) = \frac{(\sigma(1)-\sigma(2))(\sigma(1)-\sigma(3))(\sigma(2)-\sigma(3))}{(1-2)(1-3)(2-3)}$$

$$= \frac{(3-1)(3-2)\cancel{(1-2)}}{\cancel{(1-2)}(1-3)(2-3)} = (-1)^2 = 1$$

Chaque parenthèse du numérateur se retrouve au signe près au dénominateur. Le signe est $\ominus$ lorsque $\sigma(i) > \sigma(j)$ alors que $i<j$.

Déf: Soit $\sigma \in S_n$. Si $i,j \in \{1,\dots,n\}$ sont tels que $i<j$ et $\sigma(i) > \sigma(j)$, on dit que i et j présentent une inversion sous σ.

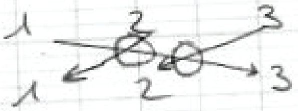
En généralisant l'exemple précédent, on peut montrer :

Prop: $\mathcal{E}(\sigma)$ vaut toujours ± 1. Plus précisément, soit N_σ le nombre d'inversion de $\{1,\dots,n\}$ sous $\sigma \in S_n$: $N_\sigma = \{(i,j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$
Alors $\mathcal{E}(\sigma) = (-1)^{N_\sigma}$.

Ex: Dans l'exemple précedent $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ présente deux inversions :
$1<2$ mais $\sigma(1) = 3 > \sigma(2) = 1$
$1<3$ mais $\sigma(1) = 3 > \sigma(3) = 2$.

Rque: Le nombre d'inversions est égal au nbre d'intersections dans la représentation graphique de σ

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



Thm: La signature ε est un morphisme de groupe de S_n dans $\{1, -1\}$ qui prend la valeur (-1) sur toute transposition.

Dem: - En utilisant la formule $(*)$, on voit que la signature d'une transposition vaut (-1)

- En utilisant $\varepsilon(\sigma) = (-1)^{N_\sigma}$ où N_σ est le nbre d'inversions de $\{1, \dots, n\}$ pour σ, montrons que ε est un morphisme de groupe. Soient σ_1 et σ_2 deux permutations de $\{1, \dots, n\}$. On doit montrer que

$$\varepsilon(\sigma_2 \circ \sigma_1) = \varepsilon(\sigma_2) \times \varepsilon(\sigma_1)$$

$$\Leftrightarrow (-1)^{N_{\sigma_2 \circ \sigma_1}} = (-1)^{N_{\sigma_2}} \times (-1)^{N_{\sigma_1}} = (-1)^{N_{\sigma_2} + N_{\sigma_1}}$$

$$\Leftrightarrow N_{\sigma_2 \circ \sigma_1} = N_{\sigma_2} + N_{\sigma_1} \text{ modulo } 2$$

($N_{\sigma_2 \circ \sigma_1}$ et $N_{\sigma_2} + N_{\sigma_1}$ ont la même parité)

Soit $i, j \in \{1, \dots, n\}$ tels que $i < j$.

On est dans l'un des 4 cas suivants :

1^e cas :

$1 \dots i \dots j \dots n$ — (i, j) présentent inv sous σ_1

$1 \dots \sigma_1(j) \dots \sigma_1(i) \dots n$ — $(\sigma_1(j), \sigma_1(i))$ ne présentent pas d'inv sous σ_2

$1 \dots \sigma_2 \circ \sigma_1(j) \dots \sigma_2 \circ \sigma_1(i) \dots n$

2^e cas :

$1 \dots i \dots j \dots n$ — (i, j) ne présente pas d'inv sous σ_1

$1 \dots \sigma_1(i) \dots \sigma_1(j) \dots n$ — $(\sigma_1(i), \sigma_1(j))$ présente inv sous σ_2

$1 \dots \sigma_2 \circ \sigma_1(j) \dots \sigma_2 \circ \sigma_1(i) \dots n$

3^e cas :

$1 \dots i \dots j \dots n$ — (i, j) ne présente pas d'inv sous σ_1

$1 \dots \sigma_1(i) \dots \sigma_1(j) \dots n$ — $(\sigma_1(i), \sigma_1(j))$ ——— σ_2

$1 \dots \sigma_2 \circ \sigma_1(i) \dots \sigma_2 \circ \sigma_1(j) \dots n$

4^e cas :

$1 \dots i \dots j \dots n$ — (i, j) présente une inv sous σ_1

$1 \dots \sigma_1(j) \dots \sigma_1(i) \dots n$

$1 \dots \sigma_2 \circ \sigma_1(i) \dots \sigma_2 \circ \sigma_1(j) \dots n$ — $(\sigma_1(j), \sigma_1(i))$ ——— σ_2

Contribution à :

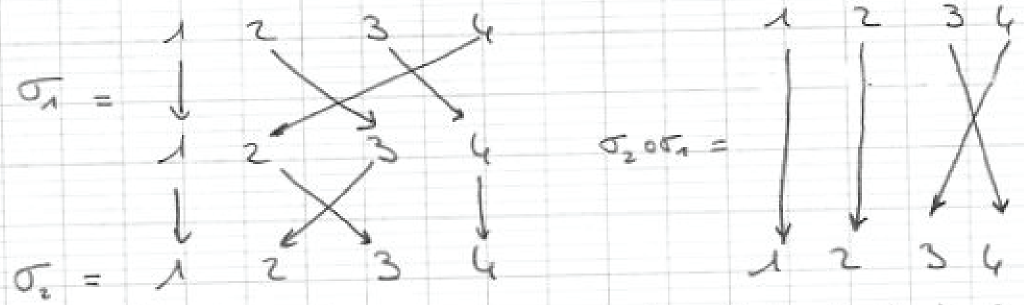
	N_{σ_1}	N_{σ_2}	$N_{\sigma_2 \circ \sigma_1}$
1^e cas	$+1$	0	$+1$
2^e cas	0	$+1$	$+1$
3^e cas	0	0	0
4^e cas	$+1$	$+1$	0

CCL : Lorsque $\{i, j\}$ parcourt tous les ensembles à deux éléments de $\{1, \dots, n\}$, $\{\sigma_1(i), \sigma_1(j)\}$ parcourt aussi tous les ensembles à 2 éléments de $\{1, \dots, n\}$. En comptabilisant le nbre d'inversions, on obtient :

$$N_{\sigma_1} + N_{\sigma_2} = N_{\sigma_1 \circ \sigma_2} \text{ modulo } 2$$

Autre façon de voir : on obtient la représentation graphique de $\sigma_2 \circ \sigma_1$ à partir de celle de σ_1 et celle de σ_2 " en tendant la corde " entre i et $\sigma_2 \circ \sigma_1(i)$.

Ex :



$\Rightarrow$ le nombre d'intersections est un invariant modulo 2 de la tresse.

Rque : Comme les transpositions engendrent S_n, tout morphisme de groupe S_n dans $\{1, -1\}$ qui vaut (-1) sur toute transposition est égal à la signature ε.

Propriété : Comme un m-cycle est le produit de $(m-1)$ transpositions, la signature d'un m-cycle est $(-1)^{m-1}$.

Proposition : Pour toute permutation $\sigma \in S_n$, $\varepsilon(\sigma) = (-1)^p$ où p = nombre de cycles de longueur paire dans la décomposition de σ en cycles à supports disjoints.

Dem : Soit $\sigma = c_1 \circ c_2 \circ \dots \circ c_k$ la décomposition de σ en cycle à supports disjoints. Comme ε est un morphisme de groupes :

$$\varepsilon(\sigma) = \varepsilon(c_1) \times \dots \times \varepsilon(c_k)$$
$$= (-1)^{m_1 - 1} \times \dots \times (-1)^{m_k - 1}$$

où m_i est la longueur du cycle c_i. Si m_i est pair, $m_i - 1$ est impair et $(-1)^{m_i - 1} = -1$. Sinon $(-1)^{m_i - 1} = 1$. D'où $\varepsilon(\sigma) = (-1)^p$.

Récapitulatif du Chapitre I

L'ordre d'un sous-groupe divise l'ordre du groupe (Thm de Lagrange)

Toute permutation se décompose en un produit de cycles à supports disjoints (donc qui commutent).

Un m-cycle est d'ordre m

L'ordre d'une permutation est le ppcm des ordres des cycles qui composent sa décomposition en cycles à supports disjoints

Formule de conjugaison :

$$\sigma \circ (k_1 \dots k_m) \circ \sigma^{-1} = (\sigma(k_1) \dots \sigma(k_m))$$

Les transpositions engendrent S_n.
La signature est un morphisme de groupe de S_n dans $\{1,-1\}$.

pas très facile à utiliser...

$$\varepsilon(\sigma) = \frac{\prod_{1 \leq i < j \leq n} (\sigma(i) - \sigma(j))}{\prod_{1 \leq i < j \leq n} (i - j)}$$

pour $n = 15$, ça fait $C_{15}^2 = \frac{15 \times 14}{1 \times 2} = 105$ couples (i,j) à considérer...

$= (-1)^{N_\sigma}$ où N_σ = nbre d'inversions de $\{1, \dots, n\}$ sous σ

ça commence à aller mieux, ms ne pas se tromper dans l'écriture d'un cycle (le dernier élément revient sur le premier)

$= (-1)^p$ où p = nbre de cycles de longueur paire dans la déc de σ

~~$= (-1)^t (-1)^?$ où t = nbre de cycles dans la déc.~~

~~ne pas oublier les cycles de longueur 1.~~