Chapitre 32

Un groupe fini : le groupe symétrique

Résumé -

Dans ce petit chapitre, nous étudions un groupe (fini) très particulier : le groupe des permutations d'un ensemble à n éléments. Il y aurait beaucoup de choses à écrire ici, mais on se contentera d'une sorte d'introduction. Cela est comme une base culturelle. Deux résultats parallèles : toute permutation est le produit de cycles ou bien le produit de transpositions.
A partir de l'un ou l'autre de ces points de vue, nous définissons la signature d'une permutation.
L'application de ces résultats sera immédiate dans le chapitre suivant lorsque nous définirons le déterminant des matrices (et endomorphismes)

Sommaire

1. Problèmes

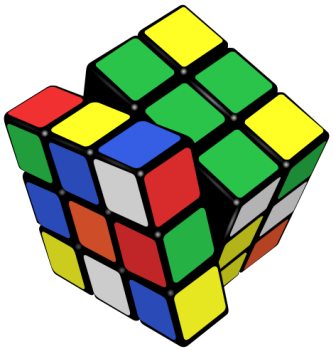
? Problème 137 - Un groupe fini non commutatif

Le cours sur les groupes est un peu frustrant. On sent comme un univers derrière une porte, mais celle-ci n'a été qu'entrouverte. Dans le cours, nous avons vu deux types de groupes : les groupes linéaires (puis orthogonaux...) qui sont des groupes infinis voire « continus » (On parle de goupe de LIE). L'autre type de groupe correspond aux groupes finis ; nos exemples $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$, $\mathbb{U}_n$ ou $(F_p^*,\times)$ sont tous commutatifs.
Existe-t-il des groupes finis non abéliens ? Ils pourraient nous servir d'exemples sur les propriétés fortes de l'univers des groupes, si riche !

? Problème 138 - Recherche d'invariant

En science, et particulièrement en mathématique, pour bien comprendre des objets, on s'intéresse aux invariants des transformations sur les objets.
Les objets qui sont liés par l'invariance forme en règle générale un groupe. Etudier ce groupe permet de mieux comprendre les objets ou les problèmes associés.
L'exemple historique est le groupe des racines d'un polynôme. S'il existe une formule qui donne les racines d'un polynôme en fonction des coefficients de ce polynôme, cette formule doit être *invariante* sous les permutations des racines !
Ainsi, pour le polynôme ax^2+bx+c, la formule des racines $\Delta=(x_1-x_2)^2$ est invariante par permutation.
Comment exploiter ces idées pour démontrer comme GALOIS et ABEL qu'il n'existe aucune formule générale d'expression des racines d'un polynôme de degré 5 ?

Représentation - Rubik's cup



Rubik's cube

? Problème 139 - Rubik's cube

Lorsque l'on manipule le Rubik's cube, chaque manipulation est une bijection sur le cube.
Le cube est représentable par la donnée des positions des 26 petits cubes et leur orientation.
On a donc un (sous-) groupe de permutation d'un ensemble fini. La connaissance du groupe des permutations peut-il nous aider à résoudre tous les Rubik'cube ? Optimiser le nombre minimal de mouvement...

? Problème 140 - Groupe engendré. Base ? Codage...

Une famille d'espaces vectoriels interessante à étudier est celle des espaces vectoriels de dimension finie.
Il existe une famille (finie) qui x tout l'espace vectoriel (infini).
Existe-t-il la même chose pour les groupes (et les groupes finis) ?
Par exemple,

$$\mathbb{U}_n = <e^{\frac{2i\pi}{n}}> := \{\omega^k; k\in\mathbb{Z}\} \qquad (\omega = e^{\frac{2i\pi}{n}})$$

Précisément pour ce chapitre, peut-on engendrer les groupes de permutation à partir d'un ensemble fini de permutation ?
Lorsque cet ensemble fini possède plusieurs éléments $a_1,\dots a_k$, et que

ceux-ci ne commutent pas :

$$< a_1, a_2, \dots a_k >= \left\{ \prod_{i=1}^{d} \alpha_i^{n_i} ; d \in \mathbb{N}, \forall\ i \in \mathbb{N}_d, n_i \in \mathbb{Z}, \alpha_i \in \{a_1, a_2, \dots a_k\} \right\}$$

? Problème 141 - Signature d'ordre 3 ?

On verra plus loin que si σ est une permutation de E, σ se décompose en produit de transpositions. La parité du nombre de transpositions est constante (la décomposition n'est pas unique, mais toute ont la même parité du nombre de transposition génératrice). On appelle signature de σ, la valeur de (-1) à la puissance le nombre de transpositions.
Peut-on décomposer toute permutation de E en produit de permutation particulière (par exemple composée d'un seule cycle de taille 3). Existe-t-il alors un invariant de ces décompositions (non uniques, très certainement) ?

2. Définitions

2.1. Rappels sur le groupe symétrique

Soit $n \geqslant 2$.

Définition - Groupe symétrique
On note S_n (ou $\mathfrak{S}_n$) l'ensemble des permutations de $[\![1, n]\!]$, c'est-à-dire l'ensemble des bijections de $[\![1, n]\!]$ dans $[\![1, n]\!]$.
$(S_n, \circ)$ est un groupe, non commutatif dès que $n > 2$, appelé groupe symétrique (d'ordre n).

Pour aller plus loin - Un meilleur point de vue
« Le bon point » de vue est celui, plus large, de la permutation sur X, un ensemble fini de n éléments ordonnées

On omet parfois $\circ$ dans les écritures et on écrit $\sigma \circ \sigma' = \sigma\sigma'$, on parle alors de **« produit »** plutôt que de composée.

Proposition - Cardinal
Card $S_n = n!$

Démonstration

2.2. Codages des permutations

Le codage classique

Savoir faire - Notation classique
Pour $\sigma \in S_n$, on note

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \dots & \sigma(n) \end{pmatrix}$$

On notera aussi plus efficacement (et classiquement) :

$$\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \dots & \sigma(n) \end{pmatrix}$$

Inspiré par les commandes Python, on pourrait écrire, $\sigma[4] = \sigma(4)$ (le quatrième élément de la liste σ) et plutôt encore : $\sigma[2:5]$, pour désigner $[\sigma(3)\,\sigma(4)\,\sigma(5)]$.

Histoire - Notation de Cauchy
Cette notation (en double ligne) est due à Cauchy (1812). Cauchy employait le mot de substitution au lieu de permutation. Il réalisait ainsi les premiers produits d'autre objets que des nombres. Il a sûrement eu ainsi une idée claire de ce qu'est un groupe…

Le codage matriciel

Proposition - Codage des permutations avec des matrices de $\mathcal{M}_n(\mathbb{K})$
On note Σ_n, l'ensemble des matrices carrées d'ordre n avec un et un seule 1 par ligne et par colonne.
L'application

$$\begin{array}{rccc} \Phi : & S_n & \longrightarrow & \Sigma_n \\ & \sigma & \longmapsto & S \end{array} \quad \text{telle que } \mathrm{Coef}_{i,j}(S) =^{i} [S]_j = \delta_{i,\sigma(j)}$$

est un morphisme bijective de groupes

Exemple - Matrice de $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$

Pour aller plus loin - Action de groupe S_n
On dit qu'un groupe G agit (à gauche) sur un ensemble E, si on dispose d'une application $(g,x) \mapsto g \cdot x$ de $G \times E$ dans E tel que $1 \cdot x = x$ et pour tout $g, g' \in G$, et tout $x \in E$: $g \cdot (g' \cdot x) = (g \times g') \cdot x$.
On remarquera que si $g \in G$, alors $x \mapsto \sigma_g(x) = g \cdot x$ est une bijection σ_g de E sur E.
Les représentations des permutations que l'on a choisit ici sont en fait des actions de groupes :
- *action de S_n sur l'ensemble $[\![1,n]\!]$.*
- *action de S_n sur l'ensemble des matrices.*
- *action des graphes uniflèches…*

Démonstration

Remarque - Structure de groupe
Il faudrait montrer que $(\Sigma_n, \times)$ est un groupe. Mais cela découle directement de l'application Φ.
Exercice
Montrer que pour $S \in \Sigma_n$, S^{-1} s'obtient facilement à partir de S.
Que représente $\mathrm{Tr}(S)$?

Le codage par graphes

Savoir faire - Permutation et graphe
On écrit en ligne les éléments du départ (souvent en haut) et en bas, les (mêmes) éléments de l'arrivée en bas.
Puis on relie les éléments par des flèches.
Un graphe est celui d'une permutation ssi de chaque point du départ

part une unique flèche et à chaque point de l'arrivée arrive une et une seule flèche.
Il s'agit du graphe de la matrice de permutation vue plus haut.

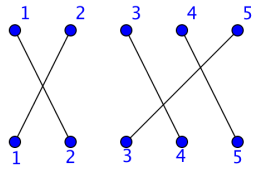
L'avantage très nette de cette représentation : le produit (composition) de permutation consiste simplement à glisser les représentations l'une sous l'autre.
Nous verrons un autre avantage plus loin.

Exercice

Faire la représentation graphique de $\sigma_1 \circ \sigma_2$ si $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$. En déduire la valeur de $\sigma_1 \circ \sigma_2$.

Représentation - Représentation graphique d'une permutation

Soit $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$.
Sa représentation graphique est



2.3. Des permutations particulières

Deux permutations particulières : la transposition et le cycle.

Transpositions

Définition - Transposition
Soit $(a,b) \in [\![1,n]\!]^2$, $a \neq b$. La permutation $\tau_{a,b}$ définie par

$$\tau_{a,b}(a) = b, \tau_{a,b}(b) = a, \forall x \in [\![1,n]\!] \setminus \{a,b\}\ \tau_{a,b}(x) = x$$

s'appelle la transposition de a et b.

Remarque - Involution
On a $\tau_{a,b} \circ \tau_{a,b} = Id$.

Remarque - Transposition
Quelles sont les matrices associées aux transpositions ?
Il s'agit des matrices de permutation vu en cours sur les opérations élémentaires (les noms devraient être unifiées...)

Exercice

Combien de transpositions de S_n existe-t-il ?

Cycles

Définition - Cycle
Soient $a_1, \ldots, a_p$ $(p \leqslant n)$ des éléments distincts de $[\![1,n]\!]$.
La permutation σ telle que

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{p-1}) = a_p, \sigma(a_p) = a_1$$

$$\text{et } \forall x \notin \{a_1, a_2, \ldots, a_p\}, \sigma(x) = x$$

s'appelle un cycle de longueur p ou p-cycle, on le note $(a_1\ a_2\ \ldots\ a_p)$.
L'ensemble $\{a_1, a_2, \ldots, a_p\}$ s'appelle le support du cycle.
Deux cycles sont dits disjoints si leurs supports sont disjoints.

Remarque - 2-cycle
Une transposition est un 2-cycle.

Remarque - Permutation circulaire de S_n
Un n-cycle élément de S_n, s'appelle aussi une permutation circulaire de $[\![1,n]\!]$.

Remarque - Quelle différence entre $(1,2,3)$ et $(2,3,1)$ de S_5 ?

Aucune. La première envoie 1 en 2, 2 en 3, puis 3 en 1.
Alors que la seconde envoie 2 en 3, 3 en 1 puis 1 en 2…

Analyse - Image réciproque d'une permutation réciproque

L'utilisation des orbites, dans la prochaine partie, permettra de répondre à la question : comment décomposer en produit de cycles ?

Exemple - Quelques cycles

Exercice
Déterminer les bijections réciproques des bijections précédentes.

Exercice
Combien de cycle de longueur k de S_n existe-t-il ?

Les exemples permettent d'affirmer :

Proposition - Commutation
Deux cycles (à supports) disjoints commutent.

Démonstration

Exercice
Ecrire les ensembles S_2 et S_3. Donner une permutation de S_4 qui ne soit pas un cycle.

Proposition - Classe de conjugaison
Soit σ une permutation de $\mathbb{N}_n$ et $c = (a_1 \dots a_k)$ un cyle.
Alors $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\big(\sigma(a_1) \dots \sigma(a_k)\big)$

Démonstration

Remarque - Nom arbitraire
Autrement écrit, si les noms sont choisis arbitrairement, les cycles sont équivalents, modulo la relation d'équivalence

$$a\mathscr{R}b \iff \exists\,\sigma \mid a = \sigma b\sigma^{-1} \iff a\sigma = \sigma b$$

Ordre

Définition - Ordre d'un élément
Soit G un groupe fini d'élément neutre e et $x \in G$.
On appelle ordre de x, le nombre $m = \min\{k \in \mathbb{N} \mid \sigma^k(x) = e$.
On appelle ordre de G, le nombre $m = \min\{k \in \mathbb{N} \mid \sigma^k = \mathrm{id}\}$.

Analyse - Existence de l'ordre d'un élément

Proposition - Ordre d'un cycle
Si c est un cycle de longueur p,
alors $c^p = \mathrm{id}$.
Mieux : p est l'ordre du cycle.

Démonstration

3. Décomposition d'une permutation

3.1. Partie génératrice d'un groupe

Dans cette partie, nous rappelons un peu de vocabulaire. Il est valable pour toute la théorie des groupes (et non uniquement pour les groupes de permutation).

Définition - Sous-groupe engendré par une partie
Soit $(G,\star)$ un groupe et S, une partie de G.
On appelle sous-groupe de G, engendré par S, le plus petit sous-groupe de G (au sens de l'inclusion) qui contient S.
On le note $< S >$.
On a donc la caractérisation suivante :

$$< S >< G \text{ et } \left(S \subset H, H < G\right) \Rightarrow < S > \subset H$$

Comme pour les espaces vectoriels, on dispose d'une description explicite de $< S >$:

Proposition - Description explicite
Soit $(G,\star)$ un groupe et S, une partie de G non vide.

$$< S >= \left\{x_1^{\epsilon_1} \star x_2^{\epsilon_2} \cdot \star x_n^{\epsilon_n}; n \in \mathbb{N}, \forall\ i \in \mathbb{N}_n, x_i \in S, \epsilon_i \in \{-1,1\}\right\}$$

Démonstration

Exercice
Dans $(G,+) = \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+\right)$, on considère $r \in [[0,n-1]]$.
Montrer que $< r >= G$ si et seulement si $r \wedge n = 1$

3.2. Décomposition en produit de cycles

Analyse - Quelques exemples

Si les cycles ne sont pas à supports disjoints :

Proposition - Chasles
Soit a_i, a_j, a_k distincts.
Alors $(a_j\ a_i) \circ (a_i\ a_k) = (a_j\ a_i\ a_k)$

Démonstration

Cette formule peut d'étendre à des cycles plus large.

Exercice

Montrer que $(a_1\ a_2\ a_3)\circ(a_3\ a_4\ a_1)=(a_2\ a_3\ a_4)$

Définition - Orbite de x
Soit σ une permutation de $[\![1,n]\!]$.
La relation définie sur $[\![1,n]\!]$ par

$$x\mathscr{R}_\sigma y \iff \exists k\in\mathbb{Z}, y=\sigma^k(x)$$

est une relation d'équivalence.
Pour $x\in[\![1,n]\!]$, il existe un unique $p\in\mathbb{N}^*$ tel que $x,\sigma(x),\dots,\sigma^{p-1}(x)$ soient deux à deux distincts et $\sigma^p(x)=x$.
La classe d'équivalence de x pour la relation $\mathscr{R}_\sigma$ est alors l'ensemble $\{x,\sigma(x),\dots,\sigma^{p-1}(x)\}$, appelé **orbite** de x.

Démonstration

Exercice

Montrer qu'il s'agit bien d'une relation d'équivalence

Théorème - Décomposition en produit de cycles à supports disjoints
Toute permutation autre que l'identité se décompose, de manière unique à l'ordre près des facteurs, en un produit de cycles (de longueur $\geqslant 2$) à supports deux à deux disjoints.
Plus précisément, ces cycles sont entièrement déterminés par σ : leur nombre est égal au nombre d'orbites non réduites à un élément de σ et ils sont égaux aux restrictions de σ à chacune des orbites.

Démonstration

Savoir faire - Comment décrire une permutation en produit de cycles

On suppose que la permutations est écrite classiquement sous la forme d'une liste double.

On peut imaginer que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ s_1 & s_2 & s_3 & s_4 & \dots \end{pmatrix}$ On procède, en plusieurs temps, en suivant le chemin...

— On est choisit librement premier élément du cycle : il ne doit pas être un point fixe.
On le note k $\quad \Longrightarrow (k, \quad)$
— On se dirige alors en s_k. $\quad \Longrightarrow (k, s_k \quad)$
— On se dirige ensuite en $s(s_k)$. $\quad \Longrightarrow (k, s_k, s(s_k) \quad)$
— ...
— On continue ainsi jusqu'à trouver à nouveau k.

Si la permutation considérée est « juste » un cycle, l'écriture est terminée. Mais on ne sait jamais...
Sinon, on cherche alors parmi les nombres qui n'était pas dans le premier cycle, si certains ne sont pas des points fixes. Si c'est le cas, on commence ainsi un nouveau cycle, à support disjoint.

Exercice

Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice qui possède exactement un 1 par ligne et par colonne et que des zéros sinon.
Montrer qu'il existe k tel que $A^k = I_n$.

3.3. Décompositions en produit de transpositions

Transpositions quelconques

On commence par une proposition :

Proposition - Décomposition

Un p-cycle est un produit (i.e. une composée) de $p-1$ transpositions :

$$(a_1\, a_2 \dots a_p) = (a_1\, a_2)(a_2\, a_3)\dots(a_{p-1}\, a_p)$$

Démonstration

On en déduit, associé avec la partie précédente

Théorème - Engendrement des transpositions
Toute permutation se décompose en produit de transpositions.
Autrement écrit : si on note T_n l'ensemble des transpositions de S_n.
Alors $< T_n >= S_n$

Exemple - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 4 & 5 & 7 \end{pmatrix}$

Exercice
Déterminer la permutation $(a_1\ a_p) \circ (a_1\ a_{p-1}) \circ \cdots \circ (a_1\ a_2)$ où les a_i sont des entiers tous distincts compris entre 1 et n, ainsi que la permutation $(a_1\ a_2 \dots a_q) \circ (a_q\ a_{q+1} \dots a_p)$ où $1 < q < p$.

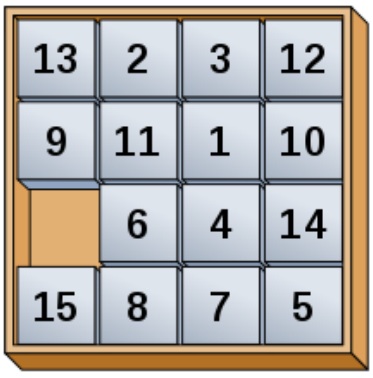
Exercice
Soit $\tau = (a\,b) \in S_n$ et $\sigma = (a\,a_1\,a_2 \dots a_p) \in S_n$ un cycle de longueur $p+1$. Donner la décomposition en produit de cycles à supports disjoints de $\tau\sigma$. Comparer le nombre d'orbites de σ et celui de $\tau\sigma$.

Exercice
Pour $(i,j) \in [\![2,n]\!]^2$, calculer $\tau_{1i} \circ \tau_{1j} \circ \tau_{1i}$ et montrer que les transpositions de la forme τ_{1i} engendrent le groupe symétrique S_n (c'est-à-dire que toute permutation se décompose comme produit de transpositions de la forme τ_{1i}).

Transpositions $\tau_{i,i+1}$

Analyse - Un deuxième algorithme ?

Pour aller plus loin - Jeu du Taquin (1)
Dans le jeu du taquin, on permute deux à deux une case d'une grilles de 15 cases et la case vide.



Si on note chacune des cases par son numéro et la cas vide comme numéro 16. Les transformations autorisées sont des transpositions (mais pas toute). Est-il possible à partir de ces transpositions d'obtenir toutes les permutations possibles ? On peut croire que oui, puisque le principe du jeu est de transformer toute permutation aléatoire en une distribution parfaite (l'opération réciproque correspond bien à une permutation aléatoire)…

Exercice

Appliquer la méthode présentée pour exprimer à nouveau $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 6 & 4 & 5 & 7 \end{pmatrix}$ en produit de transpositions.

Proposition - Décomposition par transposition simple
Toute permutation est le produit de transpositions de la forme $\tau_{i,i+1}$.
Autrement écrit :
Pour tout $\sigma \in \mathscr{S}_n$, il existe $i_1, \dots i_r \in \mathbb{N}_{n-1}$ tel que $\sigma = \tau_{i_1,i_1+1} \circ \cdots \circ \tau_{i_r,i_r+1}$.
Ou encore : si on note T_n^i l'ensemble des transpositions de la forme de $\tau_{i,i+1}$ de S_n.
Alors $< T_n^i >= S_n$

Exercice
A démontrer

4. Signature d'une permutation

4.1. Motivation : nombre d'inversions

Pour aller plus loin - Groupe alterné
L'ensemble des permutation de S_n dont la signature vaut 1 forme un sous-groupe de $(S_n, \circ)$. C'est le groupe alterné A_n. Il joue un rôle important en particulier dans l'étude des groupes…

Heuristique - Parité de changements
Il arrive, très souvent, qu'on s'intéresse au nombre de changement d'ordre dans une permutation.
On avait un ensemble bien ordonné $(1\,2\,\dots\,n)$ et en bout de course, il se trouve tout mélangé.
Combien de changement a-t-il fallut faire ? Ce nombre ne peut pas être fixe, car deux transpositions identiques conduisent à la situation initiale. Donc le seul nombre auquel on peut avoir accès est la parité de ce nombre de changements.

Définition - Une première définition
Soit σ, une permutation de $\mathbb{N}_n$.
On appelle signature de σ, le nombre

$$\epsilon(\sigma) = \prod_{i<j} \text{signe}\big(\sigma(j) - \sigma(i)\big)$$

Pour aller plus loin - Avec les graphes
A chaque croisement de n brins correspond $\binom{n}{2}$ transpositions.
Il suffit donc de faire le graphe de la permutation, de compter le « nombre » K de tels croisements. La signature est alors $(-1)^K$

Exemple - Signature de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$

Vers une formule générale.
Analyse - Calcul pour savoir si $i < j$

Proposition - Formule (sans la fonction signe)
Soit σ, une permutation de $\mathbb{N}_n$.
Alors $\epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,j\}\in\binom{\mathbb{N}_n}{2}} \frac{\sigma(j)-\sigma(i)}{j-i}$

Démonstration

Pour aller plus loin - Jeu du Taquin (2)
En fait les seuls permutations possibles au taquin conservent la signature ($\epsilon(\sigma) = 1$).
En effet, il s'agit d'un produit de transposition de la forme $(i,16)$ et comme 16 doit reprendre sa place initiale en bout de course, il faut un nombre pair de telles transpositions. Toutes les configurations ne sont pas obtenables.
C'est la raison pour laquelle Sam Loyd (créateur du jeu) avait promis à la fin du XIX-ième siècle, mille dollars a qui réussissait à inverser les cases 14 et 15 (seulement). Ce qui est impossible car il s'agit d'une unique transposition, donc de signature égale à -1.

4.2. Propriété caractéristique

Théorème - Caractérisation de ϵ
ϵ est une application de S_n dans $\{-1,1\}$ telle que
- $\epsilon(\tau) = -1$ pour toute transposition τ ;
- $\epsilon(\sigma\sigma') = \epsilon(\sigma)\epsilon(\sigma')$ pour toutes permutations σ et σ'.

Elle est la seule application à vérifier ces propriétés.

Corollaire - Morphisme de groupes
ϵ est donc un morphisme de groupes, du groupe $(S_n,\circ)$ dans le groupe $(\{-1,1\},\times)$.

Démonstration

4.3. Autres façons d'obtenir la signature de σ

Avec les transpositions

On exploite le morphisme de groupe :

Corollaire - Calcul de $\epsilon(\sigma)$
Soit $\sigma \in S_n$, $\sigma = \tau_1 \dots \tau_k$ une décomposition en transpositions.
Alors $\epsilon(\sigma) = (-1)^k$ (en particulier la parité de k est déterminée par σ).

Exemple - $\epsilon\left(\begin{pmatrix}1&2&3&4&5&6&7\\3&5&7&2&1&4&6\end{pmatrix}\right)$

Avec les orbites

On décompose les orbites en produit de transpositions

Corollaire - Signature et décomposition de cycles
Soient $c_1, \dots, c_p$ des cycles à supports disjoints de longueurs respectives $\ell_1, \dots, \ell_p$. Alors la permutation $\sigma = c_1 c_2 \dots c_p$ a pour signature

$$\epsilon(\sigma) = (-1)^{\sum_{i=1}^{p}(\ell_i - 1)} = (-1)^{n-p}.$$

Démonstration

Attention - Le nombre de cycle p
On insiste : dans la formule $\epsilon(\sigma) = (-1)^{n-p}$, p est le nombre de cycles qui décompose σ.
Il faut compter les cycles point fixe parmi ceux-ci !

Exemple - $\epsilon\left(\begin{pmatrix}1&2&3&4&5&6&7\\3&5&7&2&1&4&6\end{pmatrix}\right)$**, avec les orbites**

5. Bilan

Synthèse

⇝ On appelle permutation d'un ensemble E, toute application bijective de E dans E; le mot est reservé au situation où E est fini. Quitte à

appeler $x_1, x_2 \dots x_n$ les éléments de E, une permutation est du type : $\forall\ i \in \mathbb{N}_n$, $\varphi : x_i \mapsto x_j$, qui se résume en $j = \sigma(i)$ avec $i, j \in \mathbb{N}_n$.
Finalement les permutations peuvent « se voir » comme des applications bijectives de $\mathbb{N}_n$ sur $\mathbb{N}_n$.

$\rightsquigarrow$ L'ensemble des applications forme un groupe avec la loi $\circ$.
Une fois passé la question : « comment coder (de plusieurs façons) les éléments de ce groupe ? », nous voyons que toutes les permutations se décomposent :
— en produit de cycles (de manière unique)
— en produit de transpositions (non unique)

$\rightsquigarrow$ Bien que le nombre de transpositions qui décompose une permutation σ n'est pas unique, il n'est pas quelconque : sa parité est imposé par σ. Cette imposition s'appelle la signature de σ. Le groupe $(S_n, \circ)$ se décompose (toujours - pour tout $n \in \mathbb{N}$) donc en un sous-groupe le groupe alterné $(A_n, \circ)$ ($\sigma \in A_n \Leftrightarrow \epsilon(\sigma) = 1$), multiplié par l'image de ϵ (i.e. $\{-1, 1\}$).
$\epsilon(\sigma)$ peut se calculer avec la décomposition en produit de cycles (ou orbites).

Savoir-faire et Truc & **Astuce du chapitre**

— Savoir-faire - Notation classique
— Savoir-faire - Permutation et graphe
— Savoir-faire - Comment décrire une permutation en produit de cycles

Notations

	Propriétés	*Remarques*
$\mathbb{N}_{p-1}$, $\sigma(a_i) = a_{i+1}$ et $\sigma(a_p) =$	Les cycles à supports disjoints commutent	$(a_p\ a_1\ a_2 \cdots\ a_{p-1}) = \dots$
$\sigma(a_i) = a_{i+1}$ et $\sigma(a_p) = a_1$ $= b$ si $b \notin \{a_1, a_2 \dots a_p\}$ (support	σ se décompose en produit de cycles à support disjoints. $\sigma^p = \mathrm{id}$	$(a_1\ a_2\ a_3) = (a_1\ a_2) \circ (a_2\ a_3) \dots$
ous-groupe contenant S	$< S >= H \iff [H$ groupe et $S \subset H'$ (groupe)$\Rightarrow H \subset H']$	$< \tau_{i,j} >= S_n$
e σ	$\epsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^k = (-1)^{n-p}$	si $\sigma = \prod i = 1^k \tau_i$ ou $\sigma = c_1 \circ \dots c_p$ (τ transposition - c_i cycles)

Retour sur les problèmes

137. S_3 est (le plus) petit groupe non commutatif (6 éléments).

138. Voir un cours de grands... ou sur wikipédia, ou avec un peu de chance un prochain DS...

139. Cela aide à mieux comprendre, pas forcément à être le plus rapide. Voir TD.

140. On appelle le rang d'un groupe G est le plus petit cardinal d'une partie génératrice de G :

$$\mathrm{rg}\, G = \min\{|X| \mid < X >= G\}$$

Ici par exemple S_n est de rang 2.

141. La signature d'ordre 3 ne marche pas en toute généralité. D'ordre 4, en exploité les nombres i et $-i$?