Chap 2 Le groupe des permutations

I Premières définitions

Un groupe est un ensemble G, muni d'une loi interne, notée en général multiplicativement : $(g_1, g_2) \longmapsto g_1 g_2$, avec un élément neutre ($ge = eg = g$, $\forall g$) et un inverse pour tout élément $gg^{-1} = g^{-1}g = e$).

Par exemple $(\mathbb{R}, +)$, $(GL_n(\mathbb{R}), \circ)$, des groupes finis ...

On appelle $\mathcal{S}_n$ l'ensemble des permutations de $\{1, 2, \dots, n\}$. C'est à dire les bijections σ de $\{1, \dots, n\}$ dans lui-même.

Par exemple : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \Rightarrow \sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 1, \sigma(5) = 2$.

C'est un groupe :
- la loi interne c'est la composition (notée $\sigma_1 \sigma_2$, plutôt que $\sigma_1 \circ \sigma_2$)
- l'élément neutre c'est la permutation id.
- $\sigma \in \mathcal{S}_n$ est une bijection, donc il y a une bijection réciproque σ^{-1}.

Une permutation σ est un cycle si $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_k) = i_1$ et les autres i sont invariants. On la note alors $(i_1\ i_2 \cdots i_k)$.

Par exemple dans $\mathcal{S}_5$, $\sigma = (1\,3\,4)$ est la permutation : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$

La permutation vue en exemple plus haut est égale à $(1\,3\,4)(2\,5)$ $= (2\,5)(1\,3\,4)$.

II Décompositions

$\boxed{\text{Les cycles disjoints commutent}}$

(facile à vérifier, exercice)

Proposition

$\boxed{\text{Toute permutation est produit de cycles disjoints.}}$

Dem

On pose $i_1 = \sigma(1)$, puis $i_2 = \sigma(i_1)$, ... etc. Forcément à un moment ça boucle. Donc là, soit on a épuisé tout $\{1, \dots, n\}$ et σ est un cycle complet, soit il reste des i. On recommence avec eux. Ainsi de suite, on finit par épuiser $\{1, \dots, n\}$. ◻

La longueur d'un cycle est le nbr d'éléments qui sont bougés par le cycle : longueur $(1\,3\,4) = 3$, longueur $(2\,5) = 2$.

Une transposition est un cycle de longueur 2, i.e. un échange $i \leftrightarrow j$.

Thm

$\boxed{\text{Toute permutation est produit de transpositions}}$

Dem

Il suffit de le montrer pour les cycles. Mais justement

$(i_1\, i_2 \cdots i_k) = (i_1\, i_2)(i_2\, i_3)\cdots(i_{k-1}\, i_k)$ (exercice). $\boxed{\Xi}$

Notez que les transpositions dans cette décomposition ne sont pas, en général, disjointes ; la décomposition n'est pas unique.

III Signature

Quand on a un groupe G et un autre F, on parle de morphisme de groupe : $\varphi : G \to F$. si

$$\varphi(e_G) = e_F$$

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G.$$

(en particulier, $\varphi(g^{-1}) = \varphi(g)^{-1}$ car $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_F$ donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.)

On regarde les morphismes de $\mathcal{S}_n$ dans $(\mathbb{R}^*, \times)$.

Théorème

Il n'y a qu'un seul morphisme nontrivial de $\mathcal{S}_n$ dans $\mathbb{R}^*$.

Dem

Soit τ une transposition, on a $\tau^2 = id$ donc $\varphi(\tau)^2 = 1 \Rightarrow$

$\varphi(\tau) = \pm 1$, pour chaque τ.

Notez que $(k\,j)(i\,k)(k\,j) = (i\,j)$ (exercice), donc $\varphi(k\,j)^2\,\varphi(i\,k) = \varphi(i\,j)$

$\Rightarrow \varphi((ik)) = \varphi((ij)) \quad \forall i,j,k.$

Mais $(ij) = (ji)$ donc $\varphi((ji)) = \varphi((jl))$.

On a montré que tous les $\varphi((ij))$ sont égaux.

S'ils sont tous égaux à 1 alors $\varphi = Id$ (trivial).

Il ne reste que le cas $\varphi(\tau) = -1 \ \forall \tau$, qui fixe tout. $\boxed{\equiv}$

Normalement faut vérifier que ça détermine bien un morphisme qui existe vraiment, car le problème c'est que la décomp. en produit de transpositions n'est pas unique. Je ne le fais pas.

Cet unique morphisme s'appelle la <u>signature</u> et est noté ε.

On voit que $\varepsilon(\text{cycle long. } k) = (-1)^{k-1}$ et etc pour σ quelconque.

Par exemple, $\sigma = (134)(25) \Rightarrow \varepsilon(\sigma) = (-1)^2(-1)^1 = -1$.