Le groupe symétrique

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

1 Le groupe $\mathfrak{S}_n$

Définition 1 *On note* $\mathfrak{S}_n = (\mathrm{Bij}(\llbracket 1,n\rrbracket), \circ)$ ([1]) *le groupe (pour la composition) des bijections de l'ensemble* $\llbracket 1,n\rrbracket$.

$\mathfrak{S}_n$ est le *groupe symétrique* d'indice n. C'est donc un ensemble de cardinal $n!$.

Notation 1

- *Si* $\sigma \in \mathfrak{S}_n$ *on écrit* $\sigma = \left(\begin{smallmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n)\end{smallmatrix}\right)$ *ou plu simplement* $\sigma = (1 \dots n)$.
- $\mathrm{Id}_n = \mathrm{Id}_{\llbracket 1,n\rrbracket}$ *est le neutre de* $\mathfrak{S}_n$ *pour* $\circ$.

On a les cas particuliers

- $\mathfrak{S}_1 = \{\mathrm{Id}_1\}$;
- $\mathfrak{S}_2 = \left\{\mathrm{Id}_2, \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1\end{smallmatrix}\right)\right\}$: ils sont commutatifs.

Remarque 1 $\mathfrak{S}_n$ *est non commutatif pour* $n \geq 3$.

1.1 Transpositions

$n \geq 2$. Soient $k, l \in \llbracket 1,n\rrbracket$, $k \neq l$.

On définit la *transposition* $\tau_{k,l}$ par :

$$\tau_{k,l}(k) = l,\ \tau_{k,l}(l) = k,\ \tau_{k,l}(x) = x \text{ si } x \notin \{k,l\}.$$

$\tau_{k,l}$ est aussi notée (k/l).

On remarque que $\tau_{k,l} \circ \tau_{k,l} = \mathrm{Id}_n$, mais $\tau_{k,l} \neq \mathrm{Id}_n$. On dit que $\tau_{k,l}$ est *d'ordre 2* dans le groupe $\mathfrak{S}_n$.

On montre par récurrence sur n :

Théorème 1 *Toute permutation σ se décompose comme un produit de transpositions :*

$$\sigma = \tau_1 \circ \dots \circ \tau_p.$$

On dit que les transpositions *engendrent* le groupe $\mathfrak{S}_n$. Cette décomposition n'est bien sûr pas unique, puisque p. ex. $\tau_1 = \tau_1 \circ \tau_1 \circ \tau_1 \dots$

Remarque 2 *Pour tous* $k, l \in \llbracket 1,n\rrbracket$, $k < l$,

$$\begin{aligned}(k/l) &= (k/k+1) \circ \dots \circ (l-2/l-1) \circ (l-1/l) \\ &\quad \circ (l-2/l-1) \circ \dots \circ (k/k+1)\end{aligned}$$

est le produit de $2(l-k)-1$ *transpositions du type* $(i/i+1)$ *— un nombre* impair.

Ainsi, les transpositions du type $(i/i+1)$ engendrent également $\mathfrak{S}_n$.

[1] "$\mathfrak{S}$" est un magnifique "S" gothique.

2 Applications (anti)symétriques

X est un ensemble, $(G,+)$ est un groupe abélien, f est une application de X^n dans G, $\sigma \in \mathfrak{S}_n$. On définit

$$\sigma^*(f) : \left| \begin{array}{ccc} X^n & \to & G \\ (x_1, \dots, x_n) & \mapsto & f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) \end{array}\right. .$$

(Les x_i sont "mélangés" à l'aide de la permutation σ avant l'application de f.)

On vérifie immédiatement

Proposition 1 *Si* $\sigma_1, \sigma_2 \in \mathfrak{S}_n$,

$$\sigma_1^*(\sigma_2^*(f)) = (\sigma_1 \circ \sigma_2)^*(f).$$

Remarque 3

- $\mathrm{Id}_n^*(f) = f$;
- $\sigma^*(-f) = -\sigma^*(f)$.

Définition 2 *f est symétrique (*resp. *antisymétrique) si pour toute transposition τ on a*

$$\tau^*(f) = f \ (\text{resp. } -f). \tag{1}$$

Remarque 4 *Compte tenu de la rem. 2, il suffit de vérifier* (1) *pour toute transposition τ* du type $(k/k+1)$.

Exemple 1

1. $\sum : G^n \to G$; $(x_1, \dots, x_n) \mapsto \sum_{i=1}^n x_i$ *est symétrique ;*
2. $\varphi : G^2 \to G$; $(x_1, x_2) \mapsto x_2 - x_1$ *est antisymétrique.*

Proposition 2 *Soient* $f : X^n \to G$ *et* $\sigma \in \mathfrak{S}_n$.

1. *Si f est symétrique,* $\sigma^*(f) = f$;
2. *Si f est antisymétrique et si $\sigma \in \mathfrak{S}_n$ est le produit de p transpositions,* $\sigma^*(f) = (-1)^p f$.

Il n'est pas facile de construire des exemples d'applications antisymétriques. C'est ce qui fait l'utilité de la notion du § 3.3.

3 Signature

3.1 Nombre d'inversions

Soit $\sigma \in \mathfrak{S}_n$.

Définition 3 *Le* nombre d'inversions *de σ est*

$$I_\sigma = \mathrm{card}\,\{(i,j) \in \llbracket 1,n\rrbracket \mid i < j \text{ et } \sigma(i) > \sigma(j)\}.$$

(nombre de couple d'entiers "inversés" par la permutation σ).

On utilisera l'application auxiliaire

$$\phi : \left| \begin{array}{ccc} \mathbb{Z}^n & \to & \mathbb{Z} \\ (x_1, ..., x_n) & \mapsto & \prod_{1 \le i < j \le n} (x_j - x_i) \end{array} \right. .$$

Lemme 1 *Pour toute permutation $\sigma \in \mathfrak{S}_n$,*

$$\sigma^* (\phi) = (-1)^{I_\sigma} \phi.$$

Corollaire 1 *ϕ est antisymétrique.*

3.2 Signature

Lemme 2 *Si $\sigma \in \mathfrak{S}_n$ est le produit de p transpositions d'une part, et de q transpositions d'autre part, alors $(-1)^p = (-1)^q$.*

Autrement dit, les *parités* des entiers p et q sont les mêmes. Ainsi, les décompositions en produit de transpositions qui existent selon le th. 1 ont toutes des longueurs de *même parité*.

Ce lemme 2 permet de poser :

Définition 4 *Soit $\sigma \in \mathfrak{S}_n$. La* signature *de σ est*

$$\varepsilon (\sigma) = (-1)^p$$

si σ est le produit de p transpositions dans $\mathfrak{S}_n$.

Remarque 5 $\varepsilon (\sigma) = (-1)^{I_\sigma}$.

Il est facile de voir que

Théorème 2 *$\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un* morphisme de groupes *de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$.*

En particulier, $\varepsilon (\mathrm{Id}_n) = 1$. En fait, plus précisément :

Théorème 3 *Si $n \ge 2$, $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est le seul morphisme non trivial de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$.*

Cette notion permet de reformuler plus précisément la prop. 2.2 :

Remarque 6 *Si $f : X^n \to G$ est une application antisymétrique et si $\sigma \in \mathfrak{S}_n$,*

$$\sigma^* (f) = (-1)^{\varepsilon(\sigma)} f.$$

On dit qu'une permutation σ est paire (*resp.* impaire) si $\varepsilon (\sigma) = +1$ (*resp.* $\varepsilon (\sigma) = -1$) ([2]).

Définition 5 *On pose*

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon (\sigma) = +1\} \ ({}^3)$$

(ensemble des permutations paires).

$\mathfrak{A}_n$ est le *groupe alterné* d'indice n. Cette terminologie est légitime :

Proposition 3 *$\mathfrak{A}_n$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$.*

Preuve $\mathfrak{A}_n = \ker \varepsilon$.

[2] Cela équivaut donc à dire que σ est le produit d'un nombre pair (*resp.* impair) de transpositions.

[3] Un non moins magnifique "A" gothique.

3.3 Antisymétrisée d'une application

Soit $f : X^n \to G$ une application (quelconque). On définit $A(f) : X^n \to G$ par

$$\begin{aligned} A(f)(x_1, ..., x_n) &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon (\sigma) \sigma^* (f) (x_1, ..., x_n) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \varepsilon (\sigma) f \left(x_{\sigma(1)}, ..., x_{\sigma(n)}\right). \end{aligned}$$

$A(f)$ est l'*antisymétrisée* de l'application f. Cette appellation est justifiée en vertu du

Théorème 4 *$A(f)$ est une application antisymétrique.*

4 Cycles

Définition 6 *$\sigma \in \mathfrak{S}_n$ est un* cycle *s'il existe $p \in [\![1, n]\!]$ et a_1, ..., $a_p \in [\![1, n]\!]$ deux à deux distincts tels que*

$$\begin{aligned} \sigma (a_i) &= a_{i+1} \text{ pour } 1 \le i \le p - 1 \\ \sigma (a_p) &= a_1. \end{aligned}$$

On dit alors que σ est un *cycle d'ordre p* (ou p-cycle), ce qui est légitime. p est effectivement l'ordre de σ dans $\mathfrak{S}_n$ puisque $\sigma \neq \mathrm{Id}_n$, $\sigma^2 \neq \mathrm{Id}_n$, ..., $\sigma^{p-1} \neq \mathrm{Id}_n$, $\sigma^p = \mathrm{Id}_n$.

Remarque 7 *Un cycle d'ordre 2 est une transposition.*

Notation 2 $\sigma = (a_1 a_2 ... a_p)$ *— à ne pas confondre avec la version abrégée de la notation 1.*

Les cycles engendrent également le groupe $\mathfrak{S}_n$:

Théorème 5 *Soit $\sigma \in \mathfrak{S}_n$. σ se décompose*

$$\sigma = c_1 \circ ... \circ c_k$$

en produit de cycles deux à deux disjoints. De plus, cette décomposition est unique à l'ordre près et commutative.

Cette décomposition est très facile à obtenir en pratique. Il suffit de suivre les *orbites*[4] des éléments de $[\![1, n]\!]$ sous σ.

Exemple 2 $(3\ 6\ 4\ 5\ 1\ 8\ 7\ 9\ 2) = (1\ 3\ 4\ 5)(2\ 6\ 8\ 9)$.

Remarque 8 *Dans les conditions de la déf. 6,*

$$\sigma = (a_1 / a_2) \circ (a_2 / a_3) \circ ... \circ (a_{p-1} / a_p).$$

Ainsi, un p-cycle est le produit de $p - 1$ transpositions, donc a pour signature $(-1)^{p-1}$. Cette remarque 8, combinée au th. 5, a de nombreuses applications :

- calculs de signature ;
- calculs d'ordre ;
- décomposition en transpositions (à partir de la décomposition en cycles).

[4] Images successives par les itérés σ^i de σ.