Chapitre 18

Groupe symétrique

Plan du chapitre

Hypothèse

n est un entier naturel tel que $n \geq 2$.

1 Définition

1.1 Groupe des permutations $S(E)$

Définition 18.1 (Permutation)

Soit E un ensemble. On appelle permutation (de E) toute application $f : E \to E$ bijective.
L'ensemble des permutations de E est noté $S(E)$.

Exemple 1. On a $\mathrm{id}_E \in S(E)$.

Exemple 2. On suppose que E est un $\mathbb{K}$-e.v. (ou $\mathbb{K}$ vaut $\mathbb{R}$ ou $\mathbb{C}$). Dans ce cas, pour tout $\lambda \in \mathbb{K}$, $\lambda \mathrm{id}_E \in S(E)$. Pour tout vecteur $h \in E$, la translation de vecteur h

$$\begin{aligned} f_h : E &\to E \\ x &\mapsto x+h \end{aligned}$$

est une permutation de E (elle est bijective car $f_h \circ f_{-h} = f_{-h} \circ f_h = \mathrm{id}_E$).

Exemple 3. La fonction $x \mapsto x^2$ est une permutation de $\mathbb{R}_+$.

Remarque. Comme le montre l'exemple ci-dessus, une permutation n'est pas forcément une application linéaire et on peut trouver des permutations sur des ensembles qui ne sont pas des e.v.

Proposition 18.2

Soit E un ensemble. Alors $(S(E),\circ)$ est un groupe, appelé groupe des permutations de E.

Démonstration. La composée de bijections de E est bien une bijection de E, donc $\circ$ est une l.c.i. sur $S(E)$. De plus, on a vu que la composition est associative.
$\mathrm{id}_E \in S(E)$ est clairement élément neutre pour $\circ$. Enfin, si $f \in S(E)$, alors f est bijective et $f^{-1} : E \to E$ est aussi une bijection de E, donc $f^{-1} \in S(E)$. Comme $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_E$, il s'agit bien du symétrique de f pour $\circ$ dans $S(E)$. Finalement, $S(E)$ est un groupe. □

Exemple 4. Si E possède deux éléments distincts, i.e. $E = \{a,b\}$, alors

$$S(E) = \{\mathrm{id}_E, \tau\}$$

où $\tau : E \to E$ est définie par $\tau(a) = b$ et $\tau(b) = a$. La table de ce groupe est

$\circ$	id_E	τ
id_E		
τ		

Remarque. Le groupe ci-dessus est en particulier abélien (la table est symétrique selon la diagonale), mais en général $(S(E),\circ)$ n'est pas abélien.

Dans la suite de ce chapitre, on s'intéresse à $S(E)$ lorsque $E = [\![1,n]\!]$. On note alors cet ensemble S_n.

1.2 Groupe symétrique S_n

Définition 18.3 (Groupe symétrique)

L'ensemble des permutations de $[\![1,n]\!]$ est appelé groupe symétrique (à n éléments) et est noté S_n.
Autrement dit, $(S_n,\circ)$ est le groupe des bijections de $[\![1,n]\!]$ dans $[\![1,n]\!]$.

Si $n = 1$, alors $[\![1,n]\!] = \{1\}$ et la seule bijection de $\{1\}$ dans lui-même est $\mathrm{id}_{\{1\}}$. Ainsi, $S_1 = \left\{\mathrm{id}_{\{1\}}\right\}$. Ce cas étant trivial, on suppose dans ce chapitre que $n \geq 2$ (voir hypothèse en début de chapitre). De plus, dans la suite, on notera juste "id" plutôt que "$\mathrm{id}_{[\![1,n]\!]}$".

Exemple 5. $S_2 = \{\mathrm{id}, \tau\}$, où $\tau : [\![1,2]\!] \to [\![1,2]\!]$ est définie par $\tau(1) = 2$ et $\tau(2) = 1$. La table de ce groupe est

$\circ$	id	τ
id		
τ		

Notation. On représente une permutation $\sigma \in S_n$ par la liste des éléments de $[\![1,n]\!]$ sur une première ligne, et en-dessous la liste $\sigma(i)$ pour $i \in [\![1,n]\!]$:

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

Exemple 6. L'écriture $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$ signifie que $\sigma \in S_5$ et que

$$\sigma(1) = 5 \qquad \sigma(2) = 3 \qquad \sigma(3) = 2 \qquad \sigma(4) = 1 \qquad \sigma(5) = 4$$

Exemple 7. La permutation $\tau \in S_2$ ci-dessus s'écrit $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

Remarque. $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix}$ n'est pas une permutation : elle n'est ni injective ni surjective. *Pour être une permutation, il faut que la deuxième ligne contienne une et une seule fois tous les entiers de* 1 *à* n.

Proposition 18.4

S_n possède $n!$ éléments.

Démonstration. Sera vue au chapitre "Dénombrement". □

1.3 "Produit" de permutations

Étant donnés deux permutations $\sigma, \tau \in S_n$, on note leur composition

$$\sigma\tau := \sigma \circ \tau$$

et on parlera du "produit" de σ et de τ. Plus généralement, on emploiera la notation multiplicative :

$$\sigma^2 := \sigma\sigma = \sigma \circ \sigma \qquad \sigma^k = \underbrace{\sigma \circ \cdots \circ \sigma}_{k \text{ fois}}$$

La notation permet facilement le calcul d'un produit de permutations :

Exemple 8. Si $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ alors

$$\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}$$

$$\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}$$

On remarque en particulier que $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$. Plus généralement :

Proposition 18.5

Si $n \geq 3$, alors S_n n'est pas commutatif.

Cependant, S_2 est commutatif : sa table est en effet symétrique selon la diagonale.

2 Cycles et transpositions

2.1 Définitions

Définition 18.6 (p-cycle)

Soit $p \in [\![2,n]\!]$ et $a_1,\dots,a_p \in [\![1,n]\!]$ deux à deux distincts. On considère la permutation $\sigma \in S_n$ définie par

$$\sigma(a_1)=a_2 \qquad \sigma(a_2)=a_3 \qquad \cdots \qquad \sigma(a_p)=a_1$$

$$\forall x \in [\![1,n]\!] \setminus \{a_1,\dots,a_p\} \qquad \sigma(x)=x$$

On dit alors que σ est un p-cycle (ou cycle de longueur p) et on note $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_p \end{pmatrix}$.
L'ensemble $\{a_1,\dots,a_p\}$ est appelé support du p-cycle σ.

Exemple 9. Dans S_5, le 3-cycle $\begin{pmatrix} 1 & 5 & 4 \end{pmatrix}$ a pour support $\{1,4,5\}$ et s'écrit

$$\begin{pmatrix} 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}$$

et le 5-cycle $\begin{pmatrix} 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ a pour support $\{1,2,3,4,5\}$ et s'écrit

$$\begin{pmatrix} 3 & 5 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}$$

Remarque. Un cycle admet plusieurs écritures différentes, tant que l'ordre est conservé :

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

Définition 18.7 (Transposition)

Un 2-cycle est appelé une transposition.
En d'autres termes, une transposition est une permutation qui échange deux éléments distincts de $[\![1,n]\!]$ en laissant les autres invariants.
Si $\tau \in S_n$ est la transposition qui échange i et j, on note $\tau = \begin{pmatrix} i & j \end{pmatrix}$.

Exemple 10. Dans S_5, la transposition $\begin{pmatrix} 2 & 3 \end{pmatrix}$ est

$$\begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}$$

Remarque. Si $\tau = \begin{pmatrix} i & j \end{pmatrix}$ est une transposition, alors $\tau^2 = \begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} i & j \end{pmatrix} = \dots$

Définition 18.8

Soit $\sigma \in S_n$. On appelle point fixe (de σ) tout élément $i \in [\![1,n]\!]$ tel que $\sigma(i)=i$.

Autrement dit, un point fixe de σ est un élément laissé invariant par σ.

Remarque. Étant donné un cycle $c = \begin{pmatrix} a_1 & a_2 & \cdots & a_p \end{pmatrix}$, les entiers $a_1,\dots,a_p$ ne sont pas des points fixes de c. Par contre, si on note $A=\{a_1,\dots,a_p\}$ le support de p, alors tout entier $i \notin A$ est un point fixe de c.

2.2 Décomposition d'une permutation en cycles

Proposition 18.9

Deux cycles à supports disjoints commutent.

Démonstration. Soit $\sigma_1, \sigma_2 \in S_n$ deux cycles à supports disjoints. Soit A_1, A_2 les supports respectifs de σ_1, σ_2, de sorte que $A_1 \cap A_2 = \varnothing$. Montrons que $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

□

Théorème 18.10

Toute permutation $\sigma \neq \mathrm{id}$ peut se décomposer en un produit de cycles à support disjoints.
Cette décomposition est unique à l'ordre près des cycles dans le produit.

Si on appelle $c_1, \ldots, c_m$ ces cycles à supports disjoints, alors ces cycles commutent deux à deux par la Proposition 18.9. On peut donc écrire sans ambiguité :

$$\sigma = \prod_{k=1}^{m} c_k = \quad c_1 \ldots c_m \quad = \quad c_m \ldots c_1 \quad = \quad c_2 c_1 c_3 \ldots c_m$$

Remarque. Si $\sigma = \mathrm{id}$, on peut dire par convention que $\mathrm{id} = \prod_{k=1}^{0} (\cdots)$ et donc que id est le produit de zéro cycle.

La démonstration du Théorème 18.10 n'est pas exigible. Cependant, étant donnée une permutation σ, il faut savoir trouver les cycles $c_1, \ldots, c_m$ qui la constituent, cf la méthode plus bas.

Définition 18.11 (Orbite)

Soit $\sigma \in S_n$. On appelle <u>orbite</u> de $i \in [\![1, n]\!]$ la famille $\left(\sigma^k(i)\right)_{k\in\mathbb{N}} = \left(i, \sigma(i), \sigma^2(i), \ldots\right)$, qu'on peut écrire

$$i \to \sigma(i) \to \sigma^2(i) \to \ldots$$

Méthode (Décomposer une permutation en produit de cycles)

On considère une permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$. On cherche des cycles $c_1, \ldots, c_m$ tels que $\sigma = \prod_{k=1}^{m} c_k$. On regarde successivement tous les entiers i de 1 à n.

- Si $\sigma(i) = i$, i.e. i est un point fixe de σ, alors il n'y a rien à faire : le point i ne sera pas dans le support des cycles $c_1, \ldots, c_m$.
  - On "barre" alors la colonne d'indice i dans la permutation σ.
- Si $\sigma(i) \neq i$, alors on détermine l'orbite de i : $i \to \sigma(i) \to \sigma^2(i) \to \ldots$, jusqu'à retomber sur i. Si $p \geq 1$ est le plus petit indice tel que $\sigma^p(i) = i$, alors

$$c = \begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \cdots & \sigma^{p-1}(i) \end{pmatrix}$$

  est un des cycles de la décomposition de σ. On notera que c'est un p-cycle.
  - On "barre" alors les colonnes d'indice i, $\sigma(i)$, ..., $\sigma^{p-1}(i)$ dans la permutation σ.
- Si on arrive sur un indice i déjà barré, on l'ignore et on passe au suivant.

Une fois arrivé à $i = n$, on regroupe tous les cycles obtenus : leur produit est égal à σ.

Exemple 11. Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 2 & 5 & 4 & 1 \end{pmatrix}$ en produit de cycles à supports disjoints.

Remarque.

- Une fois décomposé sous forme de cycles, on lit très facilement les orbites de tout élément $i \in [\![1, n]\!]$.
- Attention ! Si $\sigma = \begin{pmatrix} 1 & 3 & 7 \end{pmatrix}\begin{pmatrix} 2 & 6 & 4 \end{pmatrix}$, alors $\sigma(5) = \ldots$
- Les entiers qui n'apparaissent pas dans la décomposition de σ sont précisément les points fixes de σ.
- Par ailleurs, la notation des cycles a un inconvénient : s'il y a ambiguité, il faut préciser dans quel ensemble le cycle appartient. Le cycle $\begin{pmatrix} 1 & 3 & 7 \end{pmatrix}\begin{pmatrix} 2 & 6 & 4 \end{pmatrix}$ de S_7 n'est pas le même que le cycle $\begin{pmatrix} 1 & 3 & 7 \end{pmatrix}\begin{pmatrix} 2 & 6 & 4 \end{pmatrix}$ de S_{11} (ce dernier a pour points fixes 5, 8, 9, 10 et 11).

2.3 Décomposition d'une permutation en transpositions

Lemme 18.12 (Décomposition d'un cycle en produit de transpositions)

Soit un cycle $c = \begin{pmatrix} a_1 & a_2 & \cdots & a_p \end{pmatrix}$. Alors

$$c = \begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} a_2 & a_3 \end{pmatrix}\begin{pmatrix} a_3 & a_4 \end{pmatrix}\cdots\begin{pmatrix} a_{p-1} & a_p \end{pmatrix}$$

Attention à l'ordre ! Les transpositions ci-dessus ne commutent pas.

Idée de la preuve. On pose $\sigma = (\ a_1 \quad a_2\ )(\ a_2 \quad a_3\ )(\ a_3 \quad a_4\ )\cdots(\ a_{p-1} \quad a_p\ )$. Il suffit de vérifier que pour tout $i \in [\![1,n]\!]$, on a bien $c(i) = \sigma(i)$.
On notera que si $i \notin \{a_1,\dots,a_p\}$, alors $c(i) = i = \sigma(i)$. □

Théorème 18.13 (Décomposition d'une permutation en produit de transpositions)

Toute permutation σ peut se décomposer en produit de transpositions.

Démonstration. Si $\sigma = \mathrm{id}$, on peut écrire que $\sigma = (\ 1 \quad 2\ )(\ 1 \quad 2\ )$, donc on a le résultat.
Si $\sigma \neq \mathrm{id}$, alors on peut décomposer σ en produit de cycles : il existe $m \geq 1$ tel que

$$\sigma = \prod_{k=1}^{m} c_k$$

Ensuite, par le Lemme 18.12, chaque cycle $c_1,\dots,c_m$ se décompose en produit de transpositions. Ainsi, σ s'écrit comme un produit de transpositions. □

Exemple. Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 2 & 5 & 4 & 1 \end{pmatrix}$ en produit de transpositions.

Remarque. Il n'y a pas unicité de la décomposition de σ en produit de transposition. Par exemple si $\sigma = \tau_1 \dots \tau_m$ avec m transpositions, on a

$$\sigma = \tau_1 \dots \tau_m \mathrm{id} = \tau_1 \dots \tau_m (\ 1 \quad 2\ )(\ 1 \quad 2\ )$$

3 Signature

3.1 Parité d'une permutation

On a vu que la décomposition en produit de transpositions n'est pas unique. Par contre, on admet que la parité du nombre de transpositions est unique. Cela justifie que la notion suivante soit bien définie :

Définition 18.14 (Permutation paire, impaire)

Soit $\sigma \in S_n$.

- On dit que σ est une permutation paire si une (ou de manière équivalente toute) décomposition de σ en produit de transpositions fait intervenir un nombre *pair* de transpositions.
- On dit que σ est une permutation impaire si une (ou de manière équivalente toute) décomposition de σ en produit de transpositions fait intervenir un nombre *impair* de transpositions.

Exemple 12. Comme $(\ 1 \quad 3 \quad 7\ ) = (\ 1 \quad 3\ )(\ 3 \quad 7\ )$, le 3-cycle $(\ 1 \quad 3 \quad 7\ )$ est pair.

3.2 Morphisme signature

On rappelle que $(\{-1,1\},\times)$ est un groupe (c'est le groupe des inversibles de $\mathbb{Z}$).

Théorème 18.15

Il existe un unique morphisme de groupes ε de $(S_n,\circ)$ dans $(\{-1,1\},\times)$ tel que pour toute transposition $\tau\in S_n$, on a

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

Cette application $\varepsilon : S_n \to \{-1,1\}$ est appelée la signature.

Plus généralement, si $\sigma\in S_n$, on dit que $\varepsilon(\sigma)$ est la signature de σ. On a $\varepsilon(\sigma)\in\{-1,1\}$ par définition.

Comme ε est un morphisme de groupes, on a en particulier, pour tous $\sigma,\sigma'\in S_n$,

$$\varepsilon(\mathrm{id})=1$$

$$\varepsilon(\sigma\sigma')=\varepsilon(\sigma)\varepsilon(\sigma')$$

$$\varepsilon(\sigma^{-1})=\varepsilon(\sigma)^{-1}=\varepsilon(\sigma) \qquad \text{car } \varepsilon(\sigma)\in\{-1,1\}$$

Proposition 18.16

Soit $\sigma\in S_n$. La permutation σ est paire si et seulement si $\varepsilon(\sigma)=1$.
La permutation σ est impaire si et seulement si $\varepsilon(\sigma)=-1$.

Démonstration. Si σ est paire, alors il existe $m\in\mathbb{N}^*$ et des transpositions $\tau_1,\dots,\tau_{2m}$ telles que $\sigma=\prod_{k=1}^{2m}\tau_k$. Alors comme ε est un morphisme

$$\varepsilon(\sigma)=\prod_{k=1}^{2m}\varepsilon(\tau_k)=\prod_{k=1}^{2m}(-1)=(-1)^{2m}=1$$

Tandis que si σ est impaire, alors il existe $m\in\mathbb{N}$ et des transpositions $\tau_1,\dots,\tau_{2m+1}$ telles que $\sigma=\prod_{k=1}^{2m+1}\tau_k$. Alors comme ε est un morphisme

$$\varepsilon(\sigma)=\prod_{k=1}^{2m+1}\varepsilon(\tau_k)=\prod_{k=1}^{2m+1}(-1)=(-1)^{2m+1}=-1$$

□

Proposition 18.17

Si σ est un p-cycle, alors $\varepsilon(\sigma)=(-1)^{p-1}$.

Démonstration.

□

Exemple 13. Calculer la signature de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$.