Groupe symétrique

1 **Permutations.** 1

2 **Cycles.** 2

3 **Transpositions.** 3

4 **Théorèmes de décomposition.** 3

5 **Signature.** 4

Exercices 5

Dans tout ce chapitre, n sera un entier naturel non nul.

1 Permutations.

Définition 1.

Une bijection de $[\![1, n]\!]$ dans lui même est appelée une **permutation** de $[\![1, n]\!]$.
L'ensemble des permutations de $[\![1, n]\!]$ sera noté S_n.

On peut représenter une permutation $\sigma \in S_n$ à l'aide du tableau

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

Exemple 2.

Soient

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}.$$

Calculer $\sigma \circ \sigma'$, $\sigma' \circ \sigma$, σ^2 et σ^{-1}.

Proposition 3.

1. $(S_n, \circ)$ est un groupe, appelé **groupe symétrique**.
2. S_n est fini et son cardinal vaut $n!$
3. Ce groupe n'est pas abélien dès que $n \geq 3$.

Notation multiplicative : pour $\sigma, \sigma' \in S_n$, on pourra noter $\sigma\sigma'$ la permutation $\sigma \circ \sigma'$.

Définition 4 (Un peu de vocabulaire sur les permutations).

Soit $\sigma \in S_n$.

1. On dit que x est un **point fixe** de σ si $\sigma(x) = x$.
2. On appelle **support** de σ l'ensemble des éléments de $[\![1, n]\!]$ qui ne sont pas un point fixe. Notation (locale) pour le support de γ : $\mathrm{supp}(\gamma)$.
3. Deux permutations σ et σ' sont dites **conjuguées** s'il existe $\alpha \in S_n$ tel que $\sigma' = \alpha\sigma\alpha^{-1}$.

Proposition 5.

Deux permutations dont les supports sont disjoints commutent.

Preuve. Notons A et A' les supports. On peut faire un dessin patate ici, ça permet de visualiser les trois cas à traiter.

— Le cas où x n'est ni dans A ni dans A' est très simple : x est alors un point fixe pour σ et pour σ', et on a $\sigma\sigma'(x) = x = \sigma'\sigma(x)$.

— Traitons le cas où $x \in A$ et $x \notin A'$. Alors x est fixé par σ'. On a donc $\sigma\sigma'(x) = \sigma(x)$. Pour conclure, il suffit de prouver que $\sigma'(\sigma(x)) = \sigma(x)$, c'est-à-dire que $\sigma(x) \notin A'$. On prouve cela en raisonnant par l'absurde. Supposons que $\sigma(x) \in A'$. Alors $\sigma(x) \notin A$ (hypothèse) puis $\sigma(x)$ est fixe par σ, d'où $\sigma(\sigma(x)) = \sigma(x)$ puis $\sigma(x) = x$ par injectivité de σ. Ceci contredit le fait que x appartient à A.

— Le cas où $x \in A'$ et $x \notin A$ est symétrique du précédent.

$\square$

2 Cycles.

Définition 6.

Soit p un entier supérieur à 2.
Une permutation γ est appelée un p-**cycle** s'il existe p éléments distincts $a_1, \ldots, a_p$ de $[\![1, n]\!]$ tels que

$$a_1 \overset{\gamma}{\mapsto} a_2 \overset{\gamma}{\mapsto} a_3 \cdots \overset{\gamma}{\mapsto} a_p \overset{\gamma}{\mapsto} a_1$$

$$\text{et} \qquad \forall b \in [\![1, n]\!] \setminus \{a_1, \cdots, a_p\} \quad \gamma(b) = b.$$

On note alors $\gamma = (a_1\ a_2\ \cdots\ a_p)$. Il est clair que $\mathrm{supp}(\gamma) = \{a_1, \ldots, a_p\}$.

Notation.

Soit $\gamma = (a_1\ a_2\ \ldots\ a_p)$ un p-cycle. Il y a p façons de décrire γ comme un p-cycle :

$$\gamma = (a_1\ a_2\ \ldots\ a_p) = (a_2\ \ldots\ a_p\ a_1) = (a_3\ \ldots\ a_p\ a_1\ a_2) = \cdots = (a_p\ a_1\ \ldots\ a_{p-1}).$$

On peut aussi écrire les choses ainsi : pour tout entier a dans le support de γ,

$$\gamma = \left(a\ \gamma(a)\ \gamma^2(a)\ \cdots\ \gamma^{p-1}(a)\right).$$

Exemple 7 (Calculs sur un cycle).

Soit $\gamma = (a_1 \ \dots \ a_p)$ un p-cycle. Déterminer γ^{-1} et γ^p.

Preuve.
- On démontre tranquillement que $\gamma^{-1} = (a_p \cdots a_1)$.
- Ici l'écriture de γ sous la forme $(a\gamma(a)\cdots\gamma^{p-1}(a))$, va être commode pour vérifier que $\gamma^p = \mathrm{id}$.
  - Si b est fixe pour γ, il l'est pour γ^p.
  - $\gamma^p(a) = \gamma(\gamma^{p-1}(a)) = a$.
  - Soit $j \in [\![0, p-1]\!]$. On a
$$\gamma^p(\gamma^j(a)) = \gamma^j(\gamma^p(a)) = \gamma^j(a).$$

□

Exemple 8 (Conjugué d'un cycle).

Soit $\gamma = (a_1 \ \dots \ a_p)$ un cycle et $\sigma \in S_n$. Montrer que $\sigma\gamma\sigma^{-1} = (\sigma(a_1) \ \sigma(a_2) \ \dots \ \sigma(a_p))$.
Une conséquence de ce calcul : tous les p-cycles sont conjugués.

Preuve. Notons $\gamma' = (\sigma(a_1) \ \dots \ \sigma(a_p))$. Son support est $\mathrm{supp}(\gamma') = \{\sigma(a_1), \dots, \sigma(a_p)\}$.
- Soit $b \in [\![1, n]\!] \setminus \mathrm{supp}(\gamma')$. Alors $\sigma^{-1}(b) \notin \mathrm{supp}(\gamma)$: c'est un point fixe de γ. Ainsi,
$$\sigma\gamma\sigma^{-1}(b) = \sigma\left(\gamma(\sigma^{-1}(b))\right) = \sigma\left(\sigma^{-1}(b)\right) = b.$$
- Considérons maintenant un élément du support de γ' : $\sigma(a_j)$ avec $j \in [\![1, p]\!]$. On a
$$\sigma\gamma\sigma^{-1}(\sigma(a_j)) = \sigma\gamma(a_j) = \sigma(a_{j+1}),$$
avec la convention naturelle $a_{p+1} = a_1$.

On a bien prouvé ci-dessus que
$$\forall x \in [\![1, n]\!] \quad \sigma\gamma\sigma^{-1}(x) = \gamma'(x).$$
Pour la conséquence, on prend deux p-cycles $(a_1 \cdots a_p)$ et $(b_1 \cdots b_p)$, et on crée une bijection σ de $[\![1, n]\!]$ dans lui-même en lui demandant d'envoyer les a_i sur les b_i. □

3 Transpositions.

Définition 9.

Une permutation τ qui est un 2-cycle sera appelée une **transposition**.
Une transposition est donc une permutation de la forme (a, b) où $\{a, b\}$ est une paire de $[\![1, n]\!]$.

Proposition 10 (Involutivité).

Si τ est une transposition, alors
$$\tau^2 = \mathrm{id} \quad \text{et } \tau^{-1} = \tau.$$

Lemme 11 (Décomposition d'un cycle en produit de transpositions)**.**

Soit $\gamma = (a_1 \ \dots \ a_p)$ un p-cycle. Alors

$$\gamma = (a_1 \ a_2)(a_2 \ a_3)\dots(a_{p-1} \ a_p) \quad \text{ou} \quad \gamma = (a_1 \ a_p)(a_1 \ a_{p-1})\dots(a_1 \ a_2)$$

On retrouve ici l'exemple minimal qui nous a servi à démontrer que S_3 n'est pas abélien :

$$(1\ 2)(2\ 3) = (1\ 2\ 3) \quad \text{et} \quad (2\ 3)(1\ 2) = (3\ 2)(2\ 1) = (3\ 2\ 1) = (1\ 3\ 2).$$

4 Théorèmes de décomposition.

Théorème 12 (Décomposition en produit de cycles à supports disjoints)**.**

Soit $\sigma \in S_n$. Il existe $\gamma_1, \dots, \gamma_r$ r cycles à supports disjoints tels que

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_r.$$

Les γ_i commutent. Cette décomposition est unique à l'ordre des facteurs près.

Preuve. Il va falloir partitionner $\{1, \cdots, n\}$ et prouver que sur chaque cluster, σ agit comme un cycle.
• Une relation d'équivalence sur $\{1, \cdots, n\}$.
Pour i et j dans cet ensemble, on note $i \sim j$ s'il existe $k \in \mathbb{Z}$ tel que $j = \sigma^k(i)$. On prouve facilement que ceci est une relation d'équivalence.
• On a donc une partition de $\{1, \cdots, n\}$ en classes d'équivalences pour $\sim$. Soit $x \in \{1, \cdots, n\}$. On va prouver qu'il existe un entier p tel que

$$[x] = \left\{x, \sigma(x), \dots, \sigma^{p-1}(x)\right\}.$$

L'application $k \mapsto \sigma^k(x)$ nous y aide : c'est une application de $\mathbb{Z}$ dans $[x]$ qui ne saurait être injective : il existe $q < q'$ tels que $\sigma^q(x) = \sigma^{q'}(x)$, soit $\sigma^{q'-q}(x) = x$. On peut poser

$$p = \min\{k \in \mathbb{N}^* \mid \sigma^k(x) = x\},$$

bien défini comme partie non vide et minorée. Reste à prouver l'égalité d'ensemble : pour l'inclusion non triviale, faire la division euclidienne par p.
• Créer les cycles. On note r le nombre de classes d'équivalences non réduite à un singleton. Sur une classe d'équivalence de cardinal p, le point précédent montre que σ agit comme un p-cycle : il n'y a plus qu'à poser les choses. Les supports des cycles sont disjoints deux à deux car ce sont les classes d'équivalence. □

Exemple 13 (Une décomposition)**.**

On considère la permutation de S_8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 1 & 7 & 8 & 6 & 2 & 3 \end{pmatrix}.$$

1. Décomposer σ en produit de cycles à supports disjoints.
2. Déterminer σ^4, σ^{12} et σ^{666}

Corollaire 14.

Toute permutation est un produit de transpositions.
La décomposition n'est pas unique et les transpositions ne commutent pas nécessairement.

Exemple 15 (une décomposition).

Décomposer en produit de transpositions la permutation

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

5 Signature.

Définition 16.

Soit $\sigma \in S_n$.

1. Une paire $\{i, j\}$ de $[\![1, n]\!]$ est une **inversion** pour σ si $i - j$ et $\sigma(i) - \sigma(j)$ sont de signe opposé.
2. Le nombre d'inversions de σ est noté $\mathrm{Inv}(\sigma)$.
3. On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$.

Exemple 17.

Après avoir calculé son nombre d'inversions, donner la signature de

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

Proposition 18.

1. L'identité a pour signature 1.
2. Les transpositions ont pour signature -1.

Preuve. Contrairement à ce que l'on pourrait dire trop vite, le nombre d'inversions d'une transposition $\tau = (ab)$ avec $a < b$ n'est pas 1...

- Si $\{i, j\}$ est une paire d'indices, et que $\{i, j\} \cap \{a, b\} = \emptyset$, alors $\{i, j\}$ n'est pas une inversion.
- Une paire $\{a, j\}$ avec $j \notin \{a, b\}$ est une inversion ssi $(\tau(j) - \tau(a))(j - a) < 0$, c'est-à-dire ssi $(j - b)(j - a) < 0$ soit $j \in [\![a + 1, b - 1]\!]$.
- C'est pareil pour les paires $\{i, b\}$ avec $i \notin \{a, b\}$.
- Reste enfin à considérer la paire $\{a, b\}$ qui est une inversion.

Ainsi, le nombre d'inversions d'une transposition est

$$\mathrm{Inv}(\tau) = 2|[\![a+1, b-1]\!]| + 1 = 2(b-a-1) + 1 = 2(b-a) - 1.$$

On a bien un nombre d'inversions impair : $\varepsilon(\tau) = -1$.

□

Proposition 19 (La signature écrite comme un produit)**.**

$$\forall \sigma \in S_n \quad \varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i-j},$$

le produit étant indexé par l'ensemble de toutes les paires $\{i, j\}$ (donc $i \neq j$) de $[\![1, n]\!]$.

Preuve. Pour une paire $\{i, j\}$ on écrit

$$\frac{\sigma(i) - \sigma(j)}{i-j} = (-1)^{x_{\{i,j\}}} \left| \frac{\sigma(i) - \sigma(j)}{i-j} \right|.$$

Le produit donne

$$\prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i-j} = (-1)^{\sum\limits_{\{i,j\}} x_{\{i,j\}}} \times \frac{\prod\limits_{\{i,j\}} |\sigma(i) - \sigma(j)|}{\prod\limits_{\{i,j\}} |i-j|}$$

D'une part, $\sum\limits_{\{i,j\}} x_{\{i,j\}} = \mathrm{Inv}(\sigma)$. D'autre part, en remarquant que

$$f_\sigma : \left\{ \begin{array}{ccc} \mathcal{P}_2(\{1, ..., n\}) & \to & \mathcal{P}_2(\{1, ..., n\}) \\ \{i, j\} & \mapsto & \{\sigma(i), \sigma(j)\} \end{array} \right.$$

est une bijection, on peut poser le changement d'indices $\{u, v\} = \{\sigma(i), \sigma(j)\}$ et ceci prouve que le quotient de valeurs absolues vaut 1. □

Théorème 20.

La signature est un morphisme de groupes de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$:

$$\forall \sigma, \sigma' \in S_n \quad \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$$

Preuve. Découle de la propriété précédente. □

Corollaire 21 (un peu plus précis mais pas au programme)**.**

Pour $n \geq 2$, la signature est l'unique morphisme de groupes non trivial de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Preuve. Soit $f : S_n \to \mathbb{C}^*$ un morphisme de groupes. On va prouver que $f = \mathbf{1}$ ou que $f = \varepsilon$. On va fixer une transposition τ dans S_n et organiser la discussion autour de $f(\tau)$.
• $\tau^2 = \mathrm{id}$ donc $f(\tau^2) = f(\tau)^2 = 1$, ce qui donne $f(\tau) \in \{-1, 1\}$.

• Si $f(\tau) = 1$, alors f prend la valeur 1 sur toutes les transpositions. En effet, on a vu que toutes les transpositions sont conjuguées ! Si τ' est une autre transposition, il existe $\sigma \in S_n$ telle que $\tau' = \sigma\tau\sigma^{-1}$ ce qui conduit à $f(\tau') = f(\tau)$ par propriété de morphisme. Puisque toute permutation s'écrit comme un produit de transpositions, la propriété de morphisme conduite à $f = \mathbf{1}$.
• Si $f(\tau) = -1$ alors f prend la valeur -1 sur toutes les transpositions, et par théorème, c'est forcément la signature. □

Exemple 22.

Soit $p \geq 2$. Que vaut la signature d'un p-cycle ?

Exercices

37.1 **[♦◇◇]** Écrire explicitement S_1, S_2 et S_3.

37.2 **[♦◇◇]** Soit n et p deux entiers naturels supérieurs à 2 tels que $p \leq n$.
Combien S_n contient-il de p-cycles ?

37.3 **[♦♦◇]** Sous-groupe alterné
Notons A_n l'ensemble des permutations de signature égale à 1.
Justifier qu'il s'agit là d'un sous-groupe de S_n et que si $n \geq 2$, $|A_n| = \frac{n!}{2}$.

37.4 **[♦♦◇]** Calculer $\varepsilon(\sigma)$, signature de σ, où

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}.$$

37.5 **[♦♦♦]** (*) Théorème de Cayley
Soit G un groupe fini de cardinal n.

1. Pour $a \in G$, on pose
$$\tau_a : \left\{ \begin{array}{ccc} G & \to & G \\ x & \mapsto & ax \end{array} \right. .$$
l'opérateur de translation à gauche associé à a. Vérifier que pour tout a dans G, τ_a est un automorphisme de G.
2. Vérifier que
$$\Phi : \left\{ \begin{array}{ccc} G & \to & S_G \\ a & \mapsto & \tau_a \end{array} \right.$$
est un morphisme de groupes injectif.
3. En déduire que G est isomorphe à un sous-groupe de S_n.

37.6 **[♦♦♦]** Centre de S_n
On note $Z(S_n)$ le centre de S_n, c'est-à-dire l'ensemble des permutations qui commutent avec toutes les autres.

1. Que vaut $Z(S_2)$?
2. Montrer que $Z(S_n)$ est trivial dès que $n \geq 3$.
