

Fiche de cours

Groupe symétrique

$\mathfrak{S}_n$, cycles et supports, transpositions, signature, ordre d'une permutation

définitions · théorèmes et hypothèses · méthodes · démonstrations exigibles

1 LE GROUPE SYMÉTRIQUE $\mathfrak{S}_n$

Définition. Soit $n \in \mathbb{N}^*$. On appelle **permutation** de $\llbracket 1 ; n \rrbracket$ toute bijection de $\llbracket 1 ; n \rrbracket$ sur lui-même. L'ensemble de ces permutations, muni de la composition $\circ$, est noté $\mathfrak{S}_n$: c'est le **groupe symétrique** d'indice n .

Propriété — c'est bien un groupe. $(\mathfrak{S}_n, \circ)$ est un groupe, de neutre id ; l'inverse de σ est sa bijection réciproque σ^{-1} . C'est le groupe $\mathfrak{S}_X$ du chapitre 12 pour $X = \llbracket 1 ; n \rrbracket$. De plus $\text{Card } \mathfrak{S}_n = n!$, et $\mathfrak{S}_n$ n'est pas abélien dès que $n \geq 3$.

Notation — les deux écritures. Une permutation $\sigma \in \mathfrak{S}_n$ est entièrement déterminée par la liste de ses images. On l'écrit en **tableau** sur deux lignes, la seconde ligne donnant les images de la première :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \quad \text{signifie} \quad \sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 2, \sigma(5) = 4.$$

C'est la notation $[\sigma(1), \dots, \sigma(n)]$ du chapitre 12, disposée verticalement. La seconde notation, en **produit de cycles**, est introduite plus bas.

✗ ATTENTION — le sens de la composition

Par définition, $(\sigma \circ \tau)(i) = \sigma(\tau(i))$: on lit un produit de permutations **de droite à gauche**, c'est τ qui agit en premier. L'erreur la plus fréquente du chapitre est d'évaluer $\sigma \circ \tau$ en faisant agir σ d'abord. On note aussi $\sigma\tau$ pour $\sigma \circ \tau$ et σ^k pour $\sigma \circ \dots \circ \sigma$ (k facteurs), avec $\sigma^0 = \text{id}$ et $\sigma^{-k} = (\sigma^{-1})^k$.

Méthode — composer, inverser. pour $\sigma \circ \tau$, on remplit la seconde ligne case par case : sous i on écrit $\sigma(\tau(i))$, en lisant d'abord $\tau(i)$ dans le tableau de τ , puis son image par σ . Pour σ^{-1} , on échange les deux lignes du tableau de σ , puis on réordonne les colonnes par ordre croissant de la première ligne.

2 CYCLES ET SUPPORTS

Définition. Le **support** de $\sigma \in \mathfrak{S}_n$ est $\text{Supp}(\sigma) = \{i \in \llbracket 1 ; n \rrbracket, \sigma(i) \neq i\}$. Ses éléments sont les points *déplacés* par σ ; les autres sont les **points fixes**. Ainsi $\text{Supp}(\sigma) = \emptyset \iff \sigma = \text{id}$.

Propriété. Pour $\sigma \in \mathfrak{S}_n$: $\sigma(\text{Supp}(\sigma)) = \text{Supp}(\sigma)$ et $\text{Supp}(\sigma^{-1}) = \text{Supp}(\sigma)$.

Définition. Soient $p \geq 2$ et $a_1, \dots, a_p$ des éléments deux à deux distincts de $\llbracket 1 ; n \rrbracket$. Le **cycle** $c = (a_1 a_2 \dots a_p)$ est la permutation définie par

$$c(a_1) = a_2, \quad c(a_2) = a_3, \quad \dots, \quad c(a_{p-1}) = a_p, \quad c(a_p) = a_1, \quad c(i) = i \text{ pour } i \notin \{a_1, \dots, a_p\}.$$

L'entier p est la **longueur** du cycle ; on dit que c est un **p -cycle**, et $\text{Supp}(c) = \{a_1, \dots, a_p\}$ est de cardinal p . Un 2-cycle $(a b)$ est appelé **transposition** : il échange a et b et fixe tout le reste.

Propriété — propriétés d'un p -cycle. Soit $c = (a_1 \dots a_p)$.

- La notation n'est pas unique : $(a_1 a_2 \dots a_p) = (a_2 \dots a_p a_1) = \dots$ — il y a exactement p écritures, obtenues par permutation circulaire. On convient d'écrire le plus petit élément en premier.
- $c^{-1} = (a_p a_{p-1} \dots a_1)$. En particulier, pour une transposition, $(a b)^{-1} = (a b)$: **une transposition est son propre inverse**.
- $c^k(a_j) = a_{j+k}$, les indices étant pris modulo p ; par conséquent $c^p = \text{id}$ et $c^k \neq \text{id}$ pour $1 \leq k \leq p-1$.
- Le nombre de p -cycles de $\mathfrak{S}_n$ est $\frac{n!}{(n-p)!p} = \binom{n}{p}(p-1)!$; en particulier $\mathfrak{S}_n$ possède $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions.

Théorème — cycles à supports disjoints. Si $\sigma, \sigma' \in \mathfrak{S}_n$ ont des supports disjoints, alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Idée de preuve. Soit $i \in \llbracket 1 ; n \rrbracket$. Si $i \notin \text{Supp}(\sigma) \cup \text{Supp}(\sigma')$, les deux membres valent i . Si $i \in \text{Supp}(\sigma)$, alors $\sigma(i) \in \text{Supp}(\sigma)$ donc i et $\sigma(i)$ sont fixes par σ' , et les deux membres valent $\sigma(i)$; on échange les rôles si $i \in \text{Supp}(\sigma')$.

✖ ATTENTION

Deux permutations *quelconques* ne commutent pas. $(1\ 4\ 7)$ et $(4\ 8)$ ont des supports qui se rencontrent, et en effet $(1\ 4\ 7) \circ (4\ 8) = (1\ 4\ 8\ 7)$ tandis que $(4\ 8) \circ (1\ 4\ 7) = (1\ 8\ 4\ 7)$: ces deux cycles sont différents. L'hypothèse « supports disjoints » n'est pas décorative.

Théorème — décomposition en cycles — admis. Soit $\sigma \in \mathfrak{S}_n$, $\sigma \neq \text{id}$. Il existe des cycles $c_1, \dots, c_r$ de longueurs ≥ 2 , à supports deux à deux disjoints, tels que

$$\sigma = c_1 \circ c_2 \circ \dots \circ c_r.$$

Cette écriture est *unique* à l'ordre près des facteurs, et ces facteurs *commutent* entre eux (théorème précédent), de sorte que l'ordre dans lequel on les écrit est indifférent. Les supports des c_i sont les orbites de σ de cardinal ≥ 2 . La démonstration de l'existence et de l'unicité n'est pas exigible.

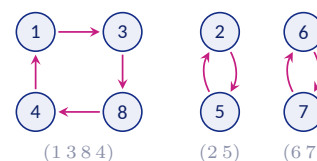


Figure 1 — Les orbites de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 1 & 2 & 7 & 6 & 4 \end{pmatrix}$ dans $\mathfrak{S}_8$:
 $\sigma = (1\ 3\ 8\ 4)(2\ 5)(6\ 7)$.

Méthode — décomposer en cycles. partir du plus petit point non encore rencontré, disons a , et écrire la suite $a, \sigma(a), \sigma^2(a), \dots$ jusqu'à revenir à a : on obtient un cycle. Reprendre avec le plus petit point restant, et s'arrêter quand tous les points ont été parcourus (les points fixes ne donnent pas de facteur). On vérifie le résultat en comptant : la somme des longueurs des cycles obtenus, augmentée du nombre de points fixes, doit valoir n .

3 GÉNÉRATION PAR LES TRANSPOSITIONS

Théorème — toute permutation est produit de transpositions — exigible. Soit $n \geq 2$. Toute permutation $\sigma \in \mathfrak{S}_n$ s'écrit comme un produit de transpositions (id étant, par convention, le produit vide, ou encore $(1\ 2) \circ (1\ 2)$). Autrement dit, les transpositions engendrent $\mathfrak{S}_n$. Plus précisément, pour tout p -cycle,

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

produit de $p - 1$ transpositions.

Idée de preuve (exigible). On vérifie la formule encadrée en évaluant les deux membres en chaque point : pour $j \leq p - 1$, le membre de droite envoie a_j sur a_1 par $(a_1\ a_j)$, puis a_1 sur a_{j+1} par $(a_1\ a_{j+1})$, les autres facteurs ne touchant pas aux points atteints ; et $a_p \mapsto a_1$ par le dernier facteur appliqué. On conclut en combinant cette formule avec la décomposition en cycles à supports disjoints : tout $\sigma \neq \text{id}$ est produit de cycles, donc produit de transpositions.

✖ ATTENTION

Cette décomposition n'est **pas unique** : le nombre de facteurs lui-même varie. Par exemple $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 1)(2\ 3) = (1\ 3)(1\ 2)(1\ 2)(1\ 2)$. Ce qui est invariant, c'est la *parité* du nombre de facteurs : c'est précisément ce que dit la signature.

Remarque. Les transpositions $(1\ k)$, $k \in \llbracket 2; n \rrbracket$, suffisent déjà à engendrer $\mathfrak{S}_n$: il en va de même des transpositions d'éléments consécutifs $(k\ k + 1)$. On le démontre en exercice.

4 SIGNATURE

Théorème — existence et unicité de la signature — admis. Soit $n \geq 2$. Il existe un *unique* morphisme de groupes

$$\varepsilon : (\mathfrak{S}_n, \circ) \longrightarrow (\{-1, 1\}, \times) \quad \text{tel que} \quad \varepsilon(\tau) = -1 \text{ pour toute transposition } \tau.$$

On l'appelle la **signature**. Une permutation est dite **paire** si $\varepsilon(\sigma) = 1$, **impaire** si $\varepsilon(\sigma) = -1$. La démonstration de l'existence et de l'unicité n'est pas exigible.

Propriété — règles de calcul. Pour $\sigma, \sigma' \in \mathfrak{S}_n$ et $k \in \mathbb{Z}$:

■ FORMULAIRE

- $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \varepsilon(\sigma')$ (morphisme); $\varepsilon(\text{id}) = 1$; $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$; $\varepsilon(\sigma^k) = \varepsilon(\sigma)^k$;
- si $\sigma = \tau_1 \circ \dots \circ \tau_m$ est un produit de m transpositions, alors $\varepsilon(\sigma) = (-1)^m$;
- $\varepsilon(\sigma \circ \sigma' \circ \sigma^{-1}) = \varepsilon(\sigma')$: la signature est invariante par conjugaison.

Le deuxième point justifie l'affirmation précédente : si σ est produit de m transpositions et de m' transpositions, alors $(-1)^m = (-1)^{m'}$, donc $m \equiv m' \pmod{2}$.

Théorème — signature d'un cycle — exigible. Un p -cycle a pour signature $\boxed{(-1)^{p-1}}$. En particulier une transposition est impaire, un 3-cycle est pair.

Idée de preuve (exigible). Le théorème de génération écrit un p -cycle comme produit de $p - 1$ transpositions; comme ε est un morphisme valant -1 sur chaque transposition, $\varepsilon((a_1 \dots a_p)) = (-1)^{p-1}$.

Propriété — signature par la décomposition en cycles. Si $\sigma = c_1 \circ \dots \circ c_r$ avec c_i un p_i -cycle (supports disjoints), alors

$$\varepsilon(\sigma) = \prod_{i=1}^r (-1)^{p_i-1} = (-1)^{p_1+\dots+p_r-r} = (-1)^{n-m},$$

où m désigne le nombre total d'orbites de σ (points fixes compris).

Propriété — signature par les inversions. On appelle **inversion** de σ tout couple (i, j) avec $i < j$ et $\sigma(i) > \sigma(j)$, et l'on note $I(\sigma)$ leur nombre. Alors $\varepsilon(\sigma) = (-1)^{I(\sigma)}$. *Démonstration faite en exercice; on peut aussi retenir que $0 \leq I(\sigma) \leq \frac{n(n-1)}{2}$, la borne supérieure étant atteinte par la seule permutation $i \mapsto n+1-i$.*

Méthode — calculer une signature. trois voies, à choisir selon la forme de l'énoncé.

- Si σ est donnée en tableau : décomposer en cycles, puis appliquer $\prod (-1)^{p_i-1}$. C'est la méthode la plus rapide et la plus sûre.
- Si σ est donnée en produit de transpositions ou de cycles quelconques (supports non nécessairement disjoints) : la signature du produit est le produit des signatures — inutile de réduire le produit.
- Pour un petit n , ou si l'énoncé y invite : compter les inversions et conclure par $(-1)^{I(\sigma)}$.

Remarque — le groupe alterné. ε étant un morphisme de groupes, $\text{Ker } \varepsilon = \{\sigma \in \mathfrak{S}_n, \varepsilon(\sigma) = 1\}$ est un sous-groupe de $\mathfrak{S}_n$ (chapitre 12) : c'est l'ensemble des permutations paires. Pour $n \geq 2$, il est de cardinal $\frac{n!}{2}$ car ε est surjectif. On le note $\mathfrak{A}_n$ et on l'appelle **groupe alterné**; cette terminologie ne figure pas au programme, mais l'objet $\text{Ker } \varepsilon$, lui, se manipule sans difficulté avec le cours du chapitre 12.

5 ORDRE D'UNE PERMUTATION

Définition. Soit $\sigma \in \mathfrak{S}_n$. Comme $\mathfrak{S}_n$ est fini, les puissances σ^k ne peuvent être toutes distinctes et il existe $k \geq 1$ tel que $\sigma^k = \text{id}$. Le plus petit tel entier est appelé **ordre** de σ , noté ici $o(\sigma)$. La notion d'ordre d'un élément d'un groupe ne figure pas explicitement au programme; elle est introduite ici pour ce chapitre, et son calcul est un exercice classique.

Théorème — ordre et longueurs des cycles. Soit $\sigma \neq \text{id}$, de décomposition en cycles à supports disjoints $c_1 \circ \dots \circ c_r$, de longueurs $p_1, \dots, p_r$. Alors

$$o(\sigma) = \text{ppcm}(p_1, \dots, p_r), \quad \text{et} \quad \sigma^k = \text{id} \iff o(\sigma) \mid k.$$

Idée de preuve. Les c_i commutent, donc $\sigma^k = c_1^k \circ \dots \circ c_r^k$; les supports restant disjoints, $\sigma^k = \text{id}$ équivaut à $c_i^k = \text{id}$ pour tout i , c'est-à-dire à $p_i \mid k$ pour tout i (propriété du p -cycle). L'ensemble des tels k est donc l'ensemble des multiples communs des p_i : son plus petit élément positif est leur ppcm.

► SAVOIR-FAIRE

- Composer, inverser, élever à une puissance en notation tableau ou en notation cycles, dans le bon ordre.
- Passer du tableau au produit de cycles à supports disjoints, et réciproquement; lire le support, les points fixes, les orbites.
- Écrire une permutation comme produit de transpositions par la formule du cours.
- Calculer une signature par les trois méthodes; en déduire la parité du nombre de transpositions nécessaires.
- Calculer l'ordre d'une permutation par le ppcm des longueurs des cycles; résoudre $\sigma \circ x = \tau$ dans $\mathfrak{S}_n$.

★ EXEMPLE — une permutation traitée de bout en bout

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 7 & 1 & 3 & 5 & 2 & 8 \end{pmatrix} \in \mathfrak{S}_9$.

- **Cycles.** $1 \mapsto 4 \mapsto 7 \mapsto 5 \mapsto 1$, puis $2 \mapsto 9 \mapsto 8 \mapsto 2$, puis $3 \mapsto 6 \mapsto 3$: $\sigma = (1\ 4\ 7\ 5)(2\ 9\ 8)(3\ 6)$. Contrôle : $4 + 3 + 2 = 9$, aucun point fixe.
- **Transpositions.** $(1\ 4\ 7\ 5) = (1\ 5)(1\ 7)(1\ 4)$, $(2\ 9\ 8) = (2\ 8)(2\ 9)$, d'où σ comme produit de $3 + 2 + 1 = 6$ transpositions.
- **Signature.** $\varepsilon(\sigma) = (-1)^{4-1}(-1)^{3-1}(-1)^{2-1} = (-1)(+1)(-1) = +1$: σ est paire. Contrôle par $(-1)^6 = +1$, et par les inversions : $I(\sigma) = 20$, pair.
- **Ordre.** $o(\sigma) = \text{ppcm}(4, 3, 2) = 12$.

6 LES PETITS CAS : $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$

Propriété. Deux permutations de même *type* (c'est-à-dire dont les décompositions en cycles à supports disjoints ont les mêmes longueurs) ont même signature et même ordre. Le tableau ci-dessous recense les types et leurs effectifs; il sert de contrôle systématique, la somme d'une colonne devant valoir $n!$.

Type	Exemple	Signature	Ordre	Dans $\mathfrak{S}_4$	Dans $\mathfrak{S}_5$
id	id	+1	1	1	1
une transposition	(1 2)	-1	2	6	10
deux transpositions	(1 2)(3 4)	+1	2	3	15
un 3-cycle	(1 2 3)	+1	3	8	20
un 4-cycle	(1 2 3 4)	-1	4	6	30
un 3-cycle et une transposition	(1 2 3)(4 5)	-1	6	—	20
un 5-cycle	(1 2 3 4 5)	+1	5	—	24
total				$24 = 4!$	$120 = 5!$

Remarque. Dans $\mathfrak{S}_3$: id, les trois transpositions (1 2), (1 3), (2 3), et les deux 3-cycles (1 2 3), (1 3 2) — soit $6 = 3!$ éléments. Les permutations paires y sont id, (1 2 3) et (1 3 2) : $\text{Ker } \varepsilon$ est de cardinal $3 = \frac{3!}{2}$, conformément à la remarque précédente. En reprenant les notations du chapitre 12, $\sigma = [2, 3, 1]$ est le 3-cycle (1 2 3) et $\tau = [2, 1, 3]$ est la transposition (1 2).

✖ PIÈGES

- Composer dans le mauvais sens : dans $\sigma \circ \tau$, c'est τ qui agit d'abord.
- Croire la décomposition en transpositions unique (elle ne l'est pas), ou croire qu'un p -cycle « est » p transpositions : il en faut $p - 1$.
- Appliquer « les cycles commutent » à deux cycles dont les supports se rencontrent.
- Confondre $\varepsilon(\sigma)$ et la parité du nombre de cycles : c'est $(-1)^{n-m}$, où m compte toutes les orbites, points fixes inclus.
- Confondre longueur du cycle et ordre de la permutation : $o((1\ 2\ 3)(4\ 5)) = 6$, et non 3 ni 5.
- Oublier que la notation $(a_1 \dots a_p)$ exige des a_i deux à deux distincts, et qu'elle admet p écritures.