

Chapitre 32

Groupe symétrique

Plan du chapitre

1	Définition	1
1.1	Groupe des permutations $S(E)$	1
1.2	Groupe symétrique S_n	2
1.3	Produit de permutations et points fixes	3
2	Cycles et transpositions	3
2.1	Définitions	3
2.2	Décomposition d'une permutation en produit de cycles à supports disjoints	4
2.3	Décomposition d'une permutation en produit de transpositions	7
3	Signature d'une permutation	8
3.1	Parité d'une permutation	8
3.2	Morphisme signature	8
4	Hors programme : tables de groupe et Sudoku	10
5	Méthodes pour les exercices.	12

Hypothèse

n est un entier naturel vérifiant $n \geq 2$.

1 Définition

1.1 Groupe des permutations $S(E)$

Définition 32.1 – Permutation

Soit E un ensemble. On appelle permutation (de E) toute application $f : E \rightarrow E$ bijective.

Notation. L'ensemble des permutations de E est noté $S(E)$.

Exemple 1. \circ $\text{id}_E \in S(E)$.

- \circ Toute symétrie d'un e.v. est une permutation.
- \circ L'application $f : x \mapsto x^3$ est une permutation de \mathbb{R} , ou encore, par restriction, de $[-1, 1]$ ou encore de $[0, 1]$.

Théorème 32.2

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. id_E est clairement l'élément neutre de $S(E)$ pour \circ . Enfin, si $f \in S(E)$, alors f est bijective et f^{-1} est aussi une bijection de E , donc $f^{-1} \in S(E)$. Comme $f \circ f^{-1} = f^{-1} \circ f = \text{id}_E$, il s'agit bien du symétrique de f pour \circ dans $S(E)$. Finalement, $(S(E), \circ)$ est un groupe. \square

Dans la suite de ce chapitre, on s'intéresse à $S(E)$ lorsque $E = \llbracket 1, n \rrbracket$.

1.2 Groupe symétrique S_n

Définition 32.3 – Groupe symétrique

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

Si $n = 1$, alors $\llbracket 1, n \rrbracket = \{1\}$ et la seule bijection de $\{1\}$ dans lui-même est $\text{id}_{\{1\}}$. Ainsi, $S_1 = \{\text{id}_{\{1\}}\}$. 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 " $\text{id}_{\llbracket 1, n \rrbracket}$ ". Les permutations sont en général notées σ ou τ .

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

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

σ étant bijective, la seconde ligne doit inclure tous les entiers de 1 à n *une et une seule fois*.

Exemple 2. S_2 est l'ensemble des bijections de $\{1, 2\}$ dans $\{1, 2\}$. Il n'y a que deux manières de construire une permutation de S_2 : l'identité et une autre permutation qu'on peut noter τ :

$$\text{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

τ est donc la permutation qui échange 1 et 2.

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

$$\sigma(1) = 5 \quad \sigma(2) = 2 \quad \sigma(3) = 1 \quad \sigma(4) = 3 \quad \sigma(5) = \dots$$

Théorème 32.4

S_n possède $n!$ éléments.

Démonstration. Sera vue au chapitre "Dénombrement". \square

1.3 Produit de permutations et points fixes

Dans le groupe (S_n, \circ) , on emploie généralement la notation multiplicative : étant donné deux permutations σ et σ' , on note leur composition

$$\sigma\sigma' := \sigma \circ \sigma'$$

et on parlera du “produit” de σ et de σ' . De même on note $\sigma^k := \underbrace{\sigma \circ \dots \circ \sigma}_{k \text{ fois}}$ pour tout $k \in \mathbb{N}^*$ et on considère que

$$\sigma^0 = \text{id}.$$

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

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

On remarque en particulier que $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$.

Théorème 32.5

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

Définition 32.6

Soit $\sigma \in S_n$. On appelle point fixe de σ tout point x de $\llbracket 1, n \rrbracket$ tel que $\sigma(x) = x$.

Exemple 5. Dans l'Exemple 4, la permutation σ_1 admet 1 pour unique point fixe et σ_2 n'en a pas.

2 Cycles et transpositions

2.1 Définitions

Définition 32.7 – p -cycle

Soit $p \in \llbracket 2, n \rrbracket$ et $\sigma \in S_n$. On dit que σ est p -cycle (ou cycle de longueur p) s'il existe $a_1, \dots, a_p \in \llbracket 1, n \rrbracket$ deux à deux distincts tels que :

$$\left\{ \begin{array}{l} \sigma(a_1) = a_2 \\ \sigma(a_2) = a_3 \\ \vdots \\ \sigma(a_{p-1}) = a_p \\ \sigma(a_p) = a_1 \end{array} \right. \quad \text{et} \quad \forall x \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_p\} \quad \sigma(x) = x$$

L'ensemble $\{a_1, \dots, a_p\}$ est appelé support du p -cycle σ . Tous les points x qui ne sont pas dans le support sont des points fixes de σ . Ainsi, pour déterminer complètement σ , il suffit que l'on donne les valeurs de σ sur son support. Cela justifie la notation suivante :

Notation d'un p -cycle. Avec les notations de la définition, le p -cycle σ se note

$$\sigma = (a_1 \ a_2 \ \dots \ a_p)$$

Exemple 6. Dans l'ensemble S_5 , le 3-cycle $(5 \ 1 \ 4)$ a pour support $\{1, 4, 5\}$ et s'écrit en notation exhaustive :

$$(5 \ 1 \ 4) = \left(\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{array} \right)$$

Dans l'ensemble S_7 , le 4-cycle $(1 \ 2 \ 3 \ 4)$ a pour support $\{1, 2, 3, 4\}$ et s'écrit en notation exhaustive :

$$(1 \ 2 \ 3 \ 4) = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{array} \right)$$

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

$$(1 \ 2 \ 3 \ 4) = (2 \ 3 \ 4 \ 1) = (3 \ 4 \ 1 \ 2) = (4 \ 1 \ 2 \ 3)$$

De même, le cycle $(5 \ 1 \ 4)$ admet plusieurs écritures équivalentes données par :

$$(5 \ 1 \ 4) = \dots\dots\dots$$

Définition 32.8 – Transposition

Un 2-cycle est appelé une transposition. En d'autres termes, une transposition est une permutation qui échange deux éléments distincts de $\llbracket 1, n \rrbracket$ en laissant les autres invariants.

Si $\tau \in S_n$ est la transposition qui échange i et j , on peut donc la noter $\tau = (i \ j)$.

Exemple 7. Dans S_n , calculer $\sigma = (1 \ 2)(2 \ 3) = \left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & \dots & n \\ & & & & \dots & \end{array} \right) = \dots\dots\dots$

Théorème 32.9

Si σ est un p -cycle, alors $\sigma^p = \text{id}$.
 En particulier, si τ est une transposition, alors $\tau^2 = \text{id}$.

2.2 Décomposition d'une permutation en produit de cycles à supports disjoints

Théorème 32.10

Deux cycles à supports disjoints commutent.

Démonstration.

□

Théorème 32.11

Toute permutation σ peut se décomposer en un produit de cycles à support disjoints.
 Cette décomposition est unique à l'ordre près des cycles dans le produit.

□

Démonstration. Admise.

Si on appelle c_1, \dots, c_m ces cycles à supports disjoints, alors ces cycles commutent deux à deux par le Théorème 32.10. On peut donc écrire sans ambiguïté :

$$\sigma = \prod_{k=1}^m c_k = c_1 c_2 c_3 \cdots c_m = c_2 c_1 c_3 \cdots c_m = \dots \quad (\text{etc.})$$

Remarque. Par convention, un produit vide de permutation donne l'élément neutre pour le produit, c'est-à-dire la permutation id. La décomposition de la permutation id est donc $\text{id} = \prod_{\emptyset} (\dots)$.

Définition 32.12 – Orbite

Soit $\sigma \in S_n$ et $i \in \llbracket 1, n \rrbracket$. On appelle orbite de i la famille $(\sigma^k(i))_{k \in \mathbb{N}} = (i, \sigma(i), \sigma^2(i), \dots)$, qu'on écrit

$$i \rightarrow \sigma(i) \rightarrow \sigma^2(i) \rightarrow \dots$$

On peut montrer que cette suite d'entiers finit toujours par retomber sur i : on continue donc d'écrire les entiers de l'orbite jusqu'à revenir au point de départ i , et ensuite on s'arrête.

Méthode – Décomposer une permutation en produit de cycles

Soit $\sigma \in S_n$. On cherche des cycles à supports disjoints c_1, \dots, c_m tels que $\sigma = c_1 c_2 \dots c_m$. 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 le point i ne sera pas dans le support des cycles c_1, \dots, c_m . On passe à l'entier $i + 1$.
- Si $\sigma(i) \neq i$, alors on détermine l'orbite de i , i.e. $i \rightarrow \sigma(i) \rightarrow \sigma^2(i) \rightarrow \dots$, jusqu'à retomber sur i . Si $p \geq 1$ est le plus petit indice tel que $\sigma^p(i) = i$, alors l'un des cycles de la décomposition de σ est :

$$c = (i \ \sigma(i) \ \sigma^2(i) \ \dots \ \sigma^{p-1}(i))$$

On l'écrit et on passe à l'entier $i + 1$.

- Si l'entier i est déjà présent parmi les cycles qu'on a obtenu, il n'y a rien à faire et on passe à l'entier $i + 1$.

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

Exemple 8. 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. • Les entiers qui n'apparaissent pas dans la décomposition de σ sont précisément les points fixes de σ .

- Une fois décomposé sous forme de cycles, on lit très facilement les orbites de tout élément $i \in \llbracket 1, n \rrbracket$.

Exemple 9. Décomposer en produit de cycles la permutation $\sigma = (1 \ 2)(2 \ 3)$.

Exemple 10. Soit $\sigma = (1 \ 3 \ 4 \ 6)$. Décomposer en produit de cycles la permutation σ^2 .

La décomposition d'une permutation en produit de cycles permet aussi de rendre les calculs de puissance plus simples.

Exemple 11. Soit $\sigma = (1\ 4\ 5)(3\ 2\ 7\ 6)$. Calculer σ^3 .

2.3 Décomposition d'une permutation en produit de transpositions

Lemme 32.13 – Décomposition d'un cycle en produit de transpositions

Soit $a_1, \dots, a_p \in \llbracket 1, n \rrbracket$ des entiers distincts. Le cycle $(a_1\ a_2\ \dots\ a_p)$ peut se réécrire :

$$(a_1\ a_2\ \dots\ a_p) = (a_1\ a_2)(a_2\ a_3)(a_3\ a_4)\dots(a_{p-1}\ a_p)$$

Les transpositions ci-dessus ne commutent pas (les supports de deux transpositions adjacentes ne sont pas disjoints)



Idée de la preuve. On pose $c = (a_1\ a_2\ \dots\ a_p)$ et $\sigma = (a_1\ a_2)(a_2\ a_3)\dots(a_{p-1}\ a_p)$. Il suffit de vérifier que pour tout $i \in \llbracket 1, n \rrbracket$, on a bien $c(i) = \sigma(i)$. On notera que si $i \notin \{a_1, \dots, a_p\}$, alors $c(i) = i = \sigma(i)$. \square

Théorème 32.14 – Décomposition d'une permutation en produit de transpositions

Toute permutation σ peut se décomposer en produit de transpositions (pas nécessairement distinctes).

Démonstration. Si $\sigma = \text{id}$, on peut écrire que $\sigma = (1\ 2)(1\ 2)$, donc on a le résultat. Si $\sigma \neq \text{id}$, 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 32.13, chaque cycle c_1, \dots, c_m se décompose en produit de transpositions. Ainsi, σ s'écrit comme un produit de transpositions. \square

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 $\sigma = \tau_1 \cdots \tau_m$ avec m transpositions, on a

$$\sigma = \tau_1 \cdots \tau_m \text{id} = \tau_1 \cdots \tau_m (1 \ 2)(1 \ 2)$$

De plus, ces transpositions ne peuvent commuter que si leurs supports sont disjoints (comme tous les cycles).

3 Signature d'une permutation

3.1 Parité d'une permutation

Lemme 32.15

Soit $\sigma \in S_n$. On considère deux décompositions quelconques de σ en produits de transpositions :

$$\sigma = \tau_1 \cdots \tau_p = \tau'_1 \cdots \tau'_q$$

avec $p, q \in \mathbb{N}^*$ et $\tau_1, \dots, \tau_p, \tau'_1, \dots, \tau'_q$ des transpositions de S_n . Les entiers p et q ont alors nécessairement la même parité.

Démonstration. Admise. □

Autrement dit, ou bien toute décomposition de σ fera intervenir un nombre pair de transpositions, ou bien toute décomposition de σ fera intervenir un nombre impair de transpositions. Cela justifie la définition suivante :

Définition 32.16 – 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 $(1 \ 3 \ 7) = (1 \ 3)(3 \ 7)$, le 3-cycle $(1 \ 3 \ 7)$ est pair.

3.2 Morphisme signature

Définition 32.17

Soit $\sigma \in S_n$. On appelle signature de σ la valeur notée :

$$\varepsilon(\sigma) := \begin{cases} 1 & \text{si } \sigma \text{ est paire} \\ -1 & \text{si } \sigma \text{ est impaire} \end{cases}$$

Remarque. $\varepsilon(\text{id}) = 1$. Si τ est une transposition, alors $\varepsilon(\tau) = -1$.

Théorème 32.18

La signature ε est un morphisme de groupes de (S_n, \circ) dans le groupe $(\{-1, 1\}, \times)$.
C'est de plus l'unique morphisme qui vaut -1 en toute transposition τ de S_n

Démonstration. Admise. □

Comme ε est un morphisme de groupes, on obtient l'assertion suivante :

Corollaire 32.19

Pour tous $\sigma, \sigma' \in S_n$, on a

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

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

La dernière égalité découle du fait que $\varepsilon(\sigma) \in \{-1, 1\}$, donc $\varepsilon(\sigma)$ est son propre inverse.

Théorème 32.20

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

Démonstration. □

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

4 Hors programme : tables de groupe et Sudoku

Soit (G, \times) un groupe avec un nombre fini d'éléments. Comme \times est une l.c.i. sur G , pour tous $x, y \in G$, le produit xy est un des éléments de G .

Une table de groupe permet de recenser pour chaque couple $(x, y) \in G^2$, à quel élément de G correspond le produit xy . Par exemple, si $G = \mathbb{U}_3 = \{1, j, \bar{j}\}$, la table de G sera de la forme :

\times	1	j	\bar{j}
1	1	j	\bar{j}
j	j	\bar{j}	1
\bar{j}	\bar{j}	1	j

où on a utilisé le fait que $j^2 = \bar{j}$ et $j\bar{j} = j^3 = 1$.

Théorème 32.21

Un groupe G est abélien si et seulement si sa table est symétrique par rapport à sa diagonale (celle qui relie le coin en haut à gauche au coin en bas à droite).

Lorsque le groupe n'est pas abélien, il faut préciser l'ordre dans lequel on fait le produit. En général, le premier élément du produit est l'élément de la ligne et le second celui de la colonne :

$\uparrow \times$...	a	...	b	...
\vdots					
a				x	
\vdots					
b		y			
\vdots					

avec $\begin{cases} x \text{ l'élément de } G \text{ tel que } x = ab \\ y \text{ l'élément de } G \text{ tel que } y = ba \end{cases}$

Exemple 14. On reprend le groupe $S_2 = \{\text{id}, \tau\}$ avec la loi \circ vu à l'Exemple 2. La table de ce groupe est donnée par :

$\uparrow \circ$	id	τ
id	id	τ
τ	τ	id

Remarque. On obtient donc que S_2 est un groupe abélien. On aurait pu ne pas préciser le sens du produit dans cette table.

Par le Théorème 32.4, on sait que S_3 contient $3! = 6$ éléments. Afin de tous les trouver, on peut chercher toutes les façons possibles de "remplir" une permutation de S_3 :

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

On trouve ainsi les 6 éléments suivants de S_3 (notations non officielles sauf pour l'identité) :

$$\begin{aligned} \text{id} & \quad c_{123} := \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} & \quad c_{132} := \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \\ \tau_{12} := \begin{pmatrix} 1 & 2 \end{pmatrix} & \quad \tau_{13} := \begin{pmatrix} 1 & 3 \end{pmatrix} & \quad \tau_{23} := \begin{pmatrix} 2 & 3 \end{pmatrix} \end{aligned}$$

Pour S_3 , la table aura donc la forme suivante :

$\uparrow \circ$	id	τ_{12}	τ_{13}	τ_{23}	c_{123}	c_{132}
id						
τ_{12}						
τ_{13}						
τ_{23}						
c_{123}						
c_{132}						

On pourrait calculer tous les produits possibles pour remplir cette table, mais cela fait tout de même beaucoup de calculs. On va voir qu'on peut remplir cette table... en jouant au Sudoku.

Théorème 32.22 – Règles de remplissage d'une table de groupe

Pour remplir une table de groupe :

1. La ligne (resp. la colonne) correspondant à l'élément neutre se calcule de manière immédiate.
2. Une même ligne (resp une même colonne) ne peut pas contenir deux fois le même élément.

Justifions l'assertion 2 : on note a_i l'élément du groupe G qui correspond à la ligne i (ou la colonne i) de la table. Supposons par l'absurde que la ligne i contient deux fois le même élément aux colonnes j et k (avec $j \neq k$), alors on a :

$$a_i a_j = a_i a_k$$

et comme a_i est régulier (car G est un groupe), on en déduit que $a_j = a_k$, ce qui est absurde.

Avec la règle 1, on peut déjà remplir partiellement la table. Ensuite, dans le cas particulier S_3 , on sait que $\tau_{12}\tau_{12} = \text{id}$ et idem pour les autres transpositions. Enfin, un calcul simple donne $\tau_{12}\tau_{23} = c_{123}$. On a donc :

$\uparrow \circ$	id	τ_{12}	τ_{13}	τ_{23}	c_{123}	c_{132}
id	id	τ_{12}	τ_{13}	τ_{23}	c_{123}	c_{132}
τ_{12}	τ_{12}	id		c_{123}		
τ_{13}	τ_{13}		id			
τ_{23}	τ_{23}			id		
c_{123}	c_{123}					
c_{132}	c_{132}					

Enfin, on peut également exploiter la structure de S_n : grâce au morphisme signature ε , on sait que "paire \circ paire" donnera "paire", que "impaire \circ paire" donnera "impaire" etc.

Exercice 1. En utilisant les règles ci-dessus et SANS calculer de produit supplémentaire, remplir la portion de la table qui concerne les produits de deux transpositions.

Exercice 2. En utilisant les règles ci-dessus et en calculant uniquement les deux produits τc et $c \tau$ associés à UNE transposition τ et à UN 3-cycle c (ceux que vous voulez), remplir tout le reste de la table.

5 Méthodes pour les exercices

Méthode

Il faut savoir décomposer une permutation en produit de cycles à supports disjoints. Cela permet notamment de calculer plus facilement les puissance d'une permutation.

Méthode

Il faut savoir décomposer une permutation en produit de transpositions. Cela permet notamment de calculer plus facilement la signature d'une permutation.