

# Chapitre 31

## Groupe symétrique

### Plan du chapitre

<b>1</b>	<b>Définition</b>	<b>1</b>
1.1	Groupe des permutations $S(E)$	1
1.2	Groupe symétrique $S_n$	2
1.3	“Produit” de permutations	3
<b>2</b>	<b>Cycles et transpositions</b>	<b>4</b>
2.1	Définitions	4
2.2	Décomposition d’une permutation en cycles	5
2.3	Décomposition d’une permutation en transpositions	6
<b>3</b>	<b>Signature</b>	<b>7</b>
3.1	Parité d’une permutation	7
3.2	Morphisme signature	8
<b>4</b>	<b>Hors programme : tables de groupe et Sudoku</b>	<b>9</b>
<b>5</b>	<b>Méthodes pour les exercices</b>	<b>10</b>

#### Hypothèse

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

### 1 Définition

#### 1.1 Groupe des permutations $S(E)$

##### Définition 31.1 – Permutation

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

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

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

**Exemple 2.** Toute symétrie d’un e.v. est une permutation.

**Exemple 3.** 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 31.2**

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.  $\text{id}_E$  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,  $S(E)$  est un groupe.  $\square$

**Exemple 4.** Si  $E$  possède exactement deux éléments  $a$  et  $b$ , alors

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

où  $\tau : E \rightarrow E$  est définie par  $\tau(a) = b$  et  $\tau(b) = a$ . On peut définir la table de ce groupe par :

$\circ$	$\text{id}_E$	$\tau$
$\text{id}_E$		
$\tau$		

**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  $E = \llbracket 1, n \rrbracket$ .

## 1.2 Groupe symétrique $S_n$

**Définition 31.3 – 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 " $\text{id}_{\llbracket 1, n \rrbracket}$ ".

**Exemple 5.**  $S_2 = \{\text{id}, \tau\}$ , où  $\tau : \llbracket 1, 2 \rrbracket \rightarrow \llbracket 1, 2 \rrbracket$  est définie par  $\tau(1) = 2$  et  $\tau(2) = 1$ . La table de ce groupe est similaire à celle ci-dessus.

**Notation.** 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  $i \in \llbracket 1, n \rrbracket$  :

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

**Exemple 6.** 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

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

**Exemple 7.** La permutation  $\tau \in S_2$  de l'exemple 5 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  $n$ .

**Théorème 31.4**

$S_n$  possède  $n!$  éléments.

*Démonstration.* Sera vue au chapitre "Dénombrement". □

**Définition 31.5**

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

**Exemple 8.** Dans l'Exemple 6, la permutation  $\sigma$  admet 2 pour unique point fixe. L'application  $\tau$  qui suit n'admet pas de point fixe. Dans  $S_n$ , l'application  $\text{id}$  admet  $n$  points fixes.

**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  $\sigma$  et de  $\tau$ . Plus généralement, on emploiera la notation multiplicative :

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

La notation d'une permutation est assez lourde, mais elle permet facilement le calcul d'un produit :

**Exemple 9.** Si  $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$  et  $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$  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 :

**Théorème 31.6**

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

Cependant,  $S_2$  est commutatif : on peut le voir sur sa table, qui est symétrique selon la diagonale.

**Remarque.** Si  $x$  est un point fixe de  $\sigma_1$  et  $\sigma_2$ , alors c'est un point fixe de  $\sigma_1\sigma_2$  et de  $\sigma_2\sigma_1$ . Cependant, comme le montre l'exemple ci-dessus, il est tout à fait possible que  $\sigma_1\sigma_2$  et/ou  $\sigma_2\sigma_1$  admettent des points fixes que ne possèdent pas  $\sigma_1$  ni  $\sigma_2$ .

## 2 Cycles et transpositions

### 2.1 Définitions

#### Définition 31.7 – $p$ -cycle

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

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

$$\forall x \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_p\} \quad \sigma(x) = x$$

On dit alors que  $\sigma$  est un  $p$ -cycle (ou cycle de longueur  $p$ ).

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

**Notation.** Avec les notations de la définition, le  $p$ -cycle  $\sigma$  se note

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

Cette écriture signifie que  $\sigma(a_1) = a_2$ ,  $\sigma(a_2) = a_3$ , ...,  $\sigma(a_p) = a_1$ , et que tous les autres entiers de  $\llbracket 1, n \rrbracket$  sont des points fixes.

**Exemple 10.** Dans l'ensemble  $S_5$ , le 5-cycle  $( 3 \ 5 \ 1 \ 4 \ 2 )$  a pour support  $\{1, 2, 3, 4, 5\}$  et s'écrit

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

et, toujours dans  $S_5$ , le 3-cycle  $( 1 \ 5 \ 4 )$  a pour support  $\{1, 4, 5\}$  et s'écrit

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

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

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

#### Théorème 31.8

Si  $\sigma$  est un  $p$ -cycle, alors  $\sigma^p = \text{id}$ .

#### Définition 31.9 – 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  $\tau = ( i \ j )$ .

**Remarque.** Si  $\tau$  est une transposition, alors  $\tau^2 = \text{id}$ .

**Exemple 11.** Dans  $S_n$ , calculer  $\sigma = ( 1 \ 2 )( 2 \ 3 ) = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ & & & & \cdots & \end{pmatrix} = \dots$

## 2.2 Décomposition d'une permutation en cycles

### Théorème 31.10

Deux cycles à supports disjoints commutent.

*Démonstration.* Soit  $\sigma_1, \sigma_2 \in S_n$  deux cycles dont on note  $A_1, A_2$  les supports. Par hypothèse, ces supports sont disjoints :  $A_1 \cap A_2 = \emptyset$ . Montrons que  $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$ . Soit  $x \in \llbracket 1, n \rrbracket$ . Montrons que  $\sigma_1 \sigma_2(x) = \sigma_2 \sigma_1(x)$ .

□

### Théorème 31.11

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

La démonstration du Théorème 31.11 n'est pas exigible. Si on appelle  $c_1, \dots, c_m$  ces cycles à supports disjoints, alors ces cycles commutent deux à deux par le Théorème 31.10. On peut donc écrire sans ambiguïté :

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

**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  $\text{id} = \prod_{\emptyset} (\cdots)$ .

### Définition 31.12 – 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**

On considère une permutation  $\sigma$ . On cherche des cycles  $c_1, \dots, c_m$  tels que  $\sigma = \prod_{k=1}^m c_k$ . On regarde successivement tous les entiers  $i$  de 1 à  $n$ .

- 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  $i + 1$ . Sinon, on calcule  $\sigma(i)$ .
- Si  $\sigma(i) = i$ , i.e.  $i$  est un point fixe de  $\sigma$ , 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  $\sigma$  est :

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

On l'écrit 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  $\sigma$ .

**Exemple 12.** 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  $\sigma$  sont précisément les points fixes de  $\sigma$ .
- Une fois décomposé sous forme de cycles, on lit très facilement les orbites de tout élément  $i \in \llbracket 1, n \rrbracket$ .

**Exemple 13.** Décomposer en produit de cycles la permutation  $\sigma = ( 1 \ 2 )( 2 \ 3 ) = \dots\dots\dots$

**Exemple 14.** Soit  $\sigma = ( 1 \ 3 \ 4 \ 6 )$ . Décomposer en produit de cycles la permutation  $\sigma^2 = \dots\dots\dots$

**2.3 Décomposition d'une permutation en transpositions**

**Lemme 31.13 – 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 :

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

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

*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 31.14 – Décomposition d'une permutation en produit de transpositions**

Toute permutation  $\sigma$  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  $\sigma$  en produit de cycles : il existe  $m \geq 1$  tel que

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

Ensuite, par le Lemme 31.13, chaque cycle  $c_1, \dots, c_m$  se décompose en produit de transpositions. Ainsi,  $\sigma$  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  $\sigma$  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

#### 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 31.15 – Permutation paire, impaire**

Soit  $\sigma \in S_n$ .

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

**Exemple 15.** Comme  $(1\ 3\ 7) = (1\ 3)(3\ 7)$ , le 3-cycle  $(1\ 3\ 7)$  est pair.

### 3.2 Morphisme signature

#### Définition 31.16

Soit  $\sigma \in S_n$ . On appelle signature de  $\sigma$  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  $\tau$  est une transposition, alors  $\varepsilon(\tau) = -1$ .

#### Théorème 31.17

La signature  $\varepsilon$  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  $\tau \in S_n$

*Démonstration.* Admise. □

Comme  $\varepsilon$  est un morphisme de groupes, on obtient l'assertion suivante :

#### Corollaire 31.18

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 31.19

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

*Démonstration.*

□



**Exemple 16.** 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

Par la propriété 31.4, 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  $S_3$  :

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

On trouve ainsi les éléments suivants pour  $S_3$  (notations non officielles sauf pour l’identité) :

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

On a vu précédemment la table du groupe  $S_2$ . On peut construire également la table de  $S_3$ . Donnons d’abord une définition :

### Définition 31.20 – Hors-programme : table de groupe

Soit  $(G, \top)$  un groupe de cardinal  $n \in \mathbb{N}^*$ . On associe à chaque élément de  $G$  un indice dans  $\llbracket 1, n \rrbracket$  :  $G = \{a_1, \dots, a_n\}$ .

On définit la table (de groupe) de  $G$  comme étant un tableau  $T$  à  $n$  lignes et  $n$  colonnes : la case de la ligne  $i$  et de la colonne  $j$  est donné par :  $T_{ij} = a_i \top a_j$  (c’est donc un élément de  $G$ ).

En particulier, si  $G$  est abélien, alors  $T_{ij} = T_{ji}$  : la table est symétrique selon la diagonale.

Pour  $S_3$ , la table aura donc la forme suivante :

$\overset{\circ}{\top}$	id	$\tau_{12}$	$\tau_{13}$	$\tau_{23}$	$c_{123}$	$c_{132}$
id						
$\tau_{12}$						
$\tau_{13}$						
$\tau_{23}$						
$c_{123}$			(*)			
$c_{132}$						

$S_3$  n’est pas commutatif, il faut donc prendre garde au sens de composition. Par exemple la case marquée d’un (\*) correspond à  $c_{123} \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ \phantom{1} & \phantom{2} & \phantom{3} \end{pmatrix} \begin{pmatrix} 1 & 3 \\ \phantom{1} & \phantom{3} \end{pmatrix}$ . Comme  $\circ$  (qu’on omet d’écrire) est une l.c.i. sur  $S_3$  le produit  $c_{123} \tau_{13}$  correspond à une et une seule permutation de  $S_3$ . On pourrait la trouver et faire de même pour toutes les cases, mais cela fait tout de même beaucoup de calculs. On va voir qu’on peut remplir cette table... en jouant au Sudoku.

**Théorème 31.21 – Hors-programme : règles de remplissage d’une table de groupe**

Soit  $G = \{a_1, \dots, a_n\}$  un groupe de cardinal  $n \in \mathbb{N}^*$ . On considère sa table de groupe  $T$ .

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 contenir deux fois le même élément.
3. S’il ne reste plus qu’une case vide sur une ligne ou une colonne, on peut donc en déduire par élimination comment remplir cette case.

Justifions l’assertion 2 : supposons par l’absurde qu’une même ligne  $i$  contient deux fois le même élément aux colonnes  $j$  et  $k$  (avec  $j \neq k$ ), alors

$$T_{ij} = T_{ik} \implies a_i \top a_j = a_i \top a_k \implies a_j = a_k \quad \text{car } a_i \text{ est régulier}$$

Et donc  $a_j = a_k$ , 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 :

$\top$	id	$\tau_{12}$	$\tau_{13}$	$\tau_{23}$	$c_{123}$	$c_{132}$
id	id	$\tau_{12}$	$\tau_{13}$	$\tau_{23}$	$c_{123}$	$c_{132}$
$\tau_{12}$	$\tau_{12}$	id		$c_{123}$		
$\tau_{13}$	$\tau_{13}$		id			
$\tau_{23}$	$\tau_{23}$			id		
$c_{123}$	$c_{123}$					
$c_{132}$	$c_{132}$					

Enfin, on peut également exploiter la structure de  $S_n$  : grâce au morphisme signature  $\varepsilon$ , on sait que “paire  $\times$  paire” donnera “paire”, que “impaire  $\times$  paire” donnera “impaire” etc.

**Exercice 1.** En utilisant les règles ci-dessus et SANS calculer de produit, 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  $\tau c$  et  $c\tau$  associés à UNE transposition  $\tau$  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 transpositions ou de cycles à supports disjoints.

### Méthode

Pour calculer la signature d’une permutation, on peut la décomposer en cycles ou en transpositions.