

# Structures algébriques

13 décembre 2022

# Plan

## 1 Loi de composition interne

- 1 Définition
- 2 Élément neutre
- 3 Éléments symétrisable

## 2 Structure de groupe

## 3 Groupe symétrique

# 1. Définition

## Définition : loi de composition interne

Soit  $E$  un ensemble non vide.

On appelle **loi de composition interne** sur  $E$  toute application

$$\star : \begin{cases} E \times E & \longrightarrow & E \\ (x, y) & \longmapsto & x \star y \end{cases}$$

## Définition : associativité, commutativité, distributivité

Une loi de composition interne  $\star$  sur un ensemble  $E$  est dite

## Définition : associativité, commutativité, distributivité

Une loi de composition interne  $\star$  sur un ensemble  $E$  est dite

■ **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter  $x \star y \star z$ .)

## Définition : associativité, commutativité, distributivité

Une loi de composition interne  $\star$  sur un ensemble  $E$  est dite

- **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter  $x \star y \star z$ .)

- **commutative** lorsque

$$\forall (x, y) \in E^2, x \star y = y \star x.$$

## Définition : associativité, commutativité, distributivité

Une loi de composition interne  $\star$  sur un ensemble  $E$  est dite

- **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter  $x \star y \star z$ .)

- **commutative** lorsque

$$\forall (x, y) \in E^2, x \star y = y \star x.$$

## Définition : associativité, commutativité, distributivité

Une loi de composition interne  $\star$  sur un ensemble  $E$  est dite

- **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter  $x \star y \star z$ .)

- **commutative** lorsque

$$\forall (x, y) \in E^2, x \star y = y \star x.$$

Si  $\star$  et  $\top$  sont deux lois de composition interne sur  $E$ , on dit que  $\star$  est **distributive** sur  $\top$  lorsque

$$\forall (x, y, z) \in E^3, x \star (y \top z) = (x \star y) \top (x \star z) \text{ et } (y \top z) \star x = (y \star x) \top (z \star x).$$

## 2. Élément neutre

### Définition : Élément neutre

Soit  $\star$  une loi de composition interne sur  $E$  et  $e$  un élément de  $E$ .

On dit que  $e$  est **élément neutre** pour  $\star$  si pour tout  $x \in E$ ,  $x \star e = e \star x = x$ .

## 2. Élément neutre

### Définition : Élément neutre

Soit  $\star$  une loi de composition interne sur  $E$  et  $e$  un élément de  $E$ .  
On dit que  $e$  est **élément neutre** pour  $\star$  si pour tout  $x \in E$ ,  $x \star e = e \star x = x$ .

### Propriété : Unicité de l'élément neutre

S'il existe, l'élément neutre est unique.

### 3. Éléments symétrisable

#### Définition : Éléments symétrisables

Soit  $\star$  une loi de composition interne sur  $E$ , admettant un élément neutre  $e \in E$ .

### 3. Éléments symétrisable

#### Définition : Éléments symétrisables

Soit  $\star$  une loi de composition interne sur  $E$ , admettant un élément neutre  $e \in E$ .

Un élément  $x$  de  $E$  est dit **symétrisable** pour  $\star$  si on a  $y \in E$  tel que

$$x \star y = y \star x = e.$$

### 3. Éléments symétrisable

#### Définition : Éléments symétrisables

Soit  $\star$  une loi de composition interne sur  $E$ , admettant un élément neutre  $e \in E$ .

Un élément  $x$  de  $E$  est dit **symétrisable** pour  $\star$  si on a  $y \in E$  tel que

$$x \star y = y \star x = e.$$

#### Propriété : Unicité du symétrique

Si  $\star$  est une loi de composition interne associative sur  $E$ , alors pour tout  $x \in E$  symétrisable, l'élément  $y$  de  $E$  tel que  $x \star y = y \star x = e$  est unique et appelé **symétrique** de  $x$  pour  $\star$  dans  $E$ .

### 3. Éléments symétrisable

Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

### 3. Éléments symétrisable

#### Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

Si  $x$  et  $y$  sont symétrisables, alors

### 3. Éléments symétrisable

#### Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

Si  $x$  et  $y$  sont symétrisables, alors

- $x \star y$  l'est aussi. De plus,  $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$ .

#### Corollaire :

### 3. Éléments symétrisable

#### Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

Si  $x$  et  $y$  sont symétrisables, alors

- $x \star y$  l'est aussi. De plus,  $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$ .
- $\text{sym}(x)$  l'est aussi et  $\text{sym}(\text{sym}(x)) = x$ .

#### Corollaire :

### 3. Éléments symétrisable

#### Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

Si  $x$  et  $y$  sont symétrisables, alors

- $x \star y$  l'est aussi. De plus,  $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$ .
- $\text{sym}(x)$  l'est aussi et  $\text{sym}(\text{sym}(x)) = x$ .

#### Corollaire :

- En notation additive : si  $x$  est symétrisable, alors pour tout  $n \in \mathbb{N}$ ,  $nx$  l'est aussi et  $n(-x) = -(nx)$  noté  $(-n)x$ .

### 3. Éléments symétrisable

#### Propriété :

Soit  $\star$  une loi de composition interne associative sur  $E$ .

Si  $x$  et  $y$  sont symétrisables, alors

- $x \star y$  l'est aussi. De plus,  $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$ .
- $\text{sym}(x)$  l'est aussi et  $\text{sym}(\text{sym}(x)) = x$ .

#### Corollaire :

- En notation additive : si  $x$  est symétrisable, alors pour tout  $n \in \mathbb{N}$ ,  $nx$  l'est aussi et  $n(-x) = -(nx)$  noté  $(-n)x$ .
- En notation multiplicative : si  $x$  est inversible, alors pour tout  $n \in \mathbb{N}$ ,  $x^n$  l'est aussi et  $(x^{-1})^n = (x^n)^{-1}$  noté  $x^{-n}$ .

# Plan

## 1 Loi de composition interne

## 2 Structure de groupe

- 1 Définition
- 2 Sous-groupes
- 3 Morphismes de groupes

## 3 Groupe symétrique

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

## Propriété : Exemples de groupes usuels

- $(\mathbb{C}, +)$  et  $(\mathbb{C}^D, +)$  avec  $D$  ensemble non vide ont une structure de groupe additif abélien.

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

## Propriété : Exemples de groupes usuels

- i  $(\mathbb{C}, +)$  et  $(\mathbb{C}^D, +)$  avec  $D$  ensemble non vide ont une structure de groupe additif abélien.
- ii  $(\mathbb{C}^*, \times)$  a une structure de groupe multiplicatif abélien.

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

## Propriété : Exemples de groupes usuels

- i  $(\mathbb{C}, +)$  et  $(\mathbb{C}^D, +)$  avec  $D$  ensemble non vide ont une structure de groupe additif abélien.
- ii  $(\mathbb{C}^*, \times)$  a une structure de groupe multiplicatif abélien.
- iii  $(\mathfrak{S}(E), \circ)$  a une structure de groupe, non commutatif en général.

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

## Propriété : Exemples de groupes usuels

- i  $(\mathbb{C}, +)$  et  $(\mathbb{C}^D, +)$  avec  $D$  ensemble non vide ont une structure de groupe additif abélien.
- ii  $(\mathbb{C}^*, \times)$  a une structure de groupe multiplicatif abélien.
- iii  $(\mathfrak{S}(E), \circ)$  a une structure de groupe, non commutatif en général.  
Si  $E = \llbracket 1, n \rrbracket$ ,  $\mathfrak{S}(E)$  est noté  $\mathfrak{S}_n$  appelé **groupe symétrique** d'ordre  $n$ .

# 1. Définition

## Définition : Groupe

On appelle **groupe** tout couple  $(G, \star)$  où  $G$  est un ensemble tel que

- $\star$  est une loi de composition interne sur  $G$
- $\star$  est associative
- $G$  admet un élément neutre pour  $\star$
- Tout élément de  $G$  admet un symétrique dans  $G$  pour  $\star$ .

Si, de plus,  $\star$  est commutative, on dit que  $(G, \star)$  est un **groupe commutatif** ou **groupe abélien**.

## Propriété : Exemples de groupes usuels

- i  $(\mathbb{C}, +)$  et  $(\mathbb{C}^D, +)$  avec  $D$  ensemble non vide ont une structure de groupe additif abélien.
- ii  $(\mathbb{C}^*, \times)$  a une structure de groupe multiplicatif abélien.
- iii  $(\mathfrak{S}(E), \circ)$  a une structure de groupe, non commutatif en général.  
Si  $E = \llbracket 1, n \rrbracket$ ,  $\mathfrak{S}(E)$  est noté  $\mathfrak{S}_n$  appelé **groupe symétrique** d'ordre  $n$ .

## 2. Sous-groupes

### a. Définition

#### Définition : Sous-groupe

Soit  $(G, \star)$  groupe.

## 2. Sous-groupes

### a. Définition

#### Définition : Sous-groupe

Soit  $(G, \star)$  groupe.

On dit que  $H$  est un **sous-groupe** de  $(G, \star)$  si  $H \subset G$  et  $(H, \star|_{H^2})$  est un groupe.

## 2. Sous-groupes

### a. Définition

#### Définition : Sous-groupe

Soit  $(G, \star)$  groupe.

On dit que  $H$  est un **sous-groupe** de  $(G, \star)$  si  $H \subset G$  et  $(H, \star|_{H^2})$  est un groupe.

On note  $H < G$ .

## 2. Sous-groupes

### a. Définition

#### Définition : Sous-groupe

Soit  $(G, \star)$  groupe.

On dit que  $H$  est un **sous-groupe** de  $(G, \star)$  si  $H \subset G$  et  $(H, \star|_{H^2})$  est un groupe.

On note  $H < G$ .

#### Propriété : Sous-groupes triviaux

Soit  $(G, \star)$  groupe.

$G$  et  $\{e_G\}$  sont des sous-groupes de  $(G, \star)$  appelés **sous-groupes triviaux**.

## b. Caractérisation

Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

## b. Caractérisation

Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

**i**  $H$  est un sous-groupe de  $(G, \star)$

## b. Caractérisation

### Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

**i**  $H$  est un sous-groupe de  $(G, \star)$

$$\text{ii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ est stable par inverse} : \forall x \in H, \text{sym}(x) \in H \end{array} \right.$$

## b. Caractérisation

### Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

**i**  $H$  est un sous-groupe de  $(G, \star)$

$$\text{ii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ est stable par inverse} : \forall x \in H, \text{sym}(x) \in H \end{array} \right.$$

$$\text{iii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star \text{sym}(y) \in H \end{array} \right.$$

## b. Caractérisation

### Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

**i**  $H$  est un sous-groupe de  $(G, \star)$

$$\text{ii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ est stable par inverse} : \forall x \in H, \text{sym}(x) \in H \end{array} \right.$$

$$\text{iii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star \text{sym}(y) \in H \end{array} \right.$$

### Propriété : Exemples de groupes usuels

**i**  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{R}^D, +)$  ont une structure de groupe additif abélien.

## b. Caractérisation

### Propriété :

Soit  $(G, \star)$  un groupe. Les propositions suivantes sont équivalentes :

**i**  $H$  est un sous-groupe de  $(G, \star)$

$$\text{ii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ est stable par inverse} : \forall x \in H, \text{sym}(x) \in H \end{array} \right.$$

$$\text{iii} \left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star \text{sym}(y) \in H \end{array} \right.$$

### Propriété : Exemples de groupes usuels

**i**  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{R}^D, +)$  ont une structure de groupe additif abélien.

**ii**  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{Q}_+^*, \times)$ ,  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{R}_+^*, \times)$ ,  $(\mathbb{U}, \times)$ ,  $(\mathbb{U}_n, \times)$  pour  $n \in \mathbb{N}^*$  ont une structure de groupe multiplicatif abélien.

## c. Intersection et réunion

### Propriété :

Soit  $(G, \star)$  un groupe et  $(H_i)_{i \in I}$  une famille de sous-groupes de  $(G, \star)$ . Alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $(G, \star)$ .

## c. Intersection et réunion

Propriété :

Soit  $(G, \star)$  un groupe et  $(H_i)_{i \in I}$  une famille de sous-groupes de  $(G, \star)$ . Alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $(G, \star)$ .

Propriété :

Soit  $(G, \star)$  un groupe,  $H, K$  sont des sous groupes de  $(G, \star)$ , alors

$$H \cup K \text{ sous-groupe de } G \iff H \subset K \text{ ou } K \subset H.$$

## d. Sous-groupes de $(\mathbb{Z}, +)$

Définition :

Pour tout  $a \in \mathbb{Z}$ , on note  $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$ .

## d. Sous-groupes de $(\mathbb{Z}, +)$

### Définition :

Pour tout  $a \in \mathbb{Z}$ , on note  $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$ .

### Théorème : Division euclidienne dans $\mathbb{Z}$

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

$q$  est le **quotient** et  $r$  est le **reste** de la division euclidienne de  $a$  par  $b$ .

## d. Sous-groupes de $(\mathbb{Z}, +)$

### Définition :

Pour tout  $a \in \mathbb{Z}$ , on note  $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$ .

### Théorème : Division euclidienne dans $\mathbb{Z}$

Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z}^2$  tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

$q$  est le **quotient** et  $r$  est le **reste** de la division euclidienne de  $a$  par  $b$ .

### Propriété : Sous-groupes de $(\mathbb{Z}, +)$

Les sous-groupes de  $(\mathbb{Z}, +)$  sont exactement les  $a\mathbb{Z}$  pour  $a \in \mathbb{N}$ . De plus, si  $Z \neq \{0\}$ ,  $a = \min(\mathbb{Z} \cap \mathbb{N}^*)$ .

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

#### Définition :

Lorsque  $(G, \star) = (G', \bullet)$ , on parle d'**endomorphisme** de groupes.

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

#### Définition :

Lorsque  $(G, \star) = (G', \bullet)$ , on parle d'**endomorphisme** de groupes.

Lorsque  $f$  est bijective, on parle d'**isomorphisme**.

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

#### Définition :

Lorsque  $(G, \star) = (G', \bullet)$ , on parle d'**endomorphisme** de groupes.

Lorsque  $f$  est bijective, on parle d'**isomorphisme**.

Lorsqu'il existe un isomorphisme entre  $G$  et  $G'$ , on dit que  $G$  et  $G'$  sont **isomorphes**.

## 3. Morphismes de groupes

### a. Définition

#### Définition :

Soient  $(G, \star)$  et  $(G', \bullet)$  deux groupes.

$f : (G, \star) \rightarrow (G', \bullet)$  est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \bullet f(y)$$

#### Définition :

Lorsque  $(G, \star) = (G', \bullet)$ , on parle d'**endomorphisme** de groupes.

Lorsque  $f$  est bijective, on parle d'**isomorphisme**.

Lorsqu'il existe un isomorphisme entre  $G$  et  $G'$ , on dit que  $G$  et  $G'$  sont **isomorphes**.

Lorsque  $f$  est bijective et  $G = G'$ , on parle d'**automorphismes**.

## b. Propriétés

### Propriété :

Si  $f : (G, \star) \rightarrow (G', \bullet)$  est un morphisme de groupes, alors  $f(e_G) = e_{G'}$  et pour tout  $x \in G$ ,  $f(\text{sym}(x)) = \text{sym}(f(x))$ .

## b. Propriétés

### Propriété :

Si  $f : (G, \star) \rightarrow (G', \bullet)$  est un morphisme de groupes, alors  $f(e_G) = e_{G'}$  et pour tout  $x \in G$ ,  $f(\text{sym}(x)) = \text{sym}(f(x))$ .

### Propriété : Image directe ou réciproque d'un sous-groupe par un morphisme de groupe

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes,  $H$  un sous groupe de  $(G, \star)$  et  $H'$  un sous-groupe de  $(G', \bullet)$ .

Alors  $f(H)$  est un sous-groupe de  $(G', \bullet)$  et  $f^{(-1)}(H')$  est un sous-groupe de  $(G, \star)$ .

## b. Propriétés

### Propriété :

Si  $f : (G, \star) \rightarrow (G', \bullet)$  et  $g : (G', \bullet) \rightarrow (G'', \Delta)$  sont des morphismes de groupes, alors  $g \circ f$  en est encore un.

## b. Propriétés

### Propriété :

Si  $f : (G, \star) \rightarrow (G', \bullet)$  et  $g : (G', \bullet) \rightarrow (G'', \Delta)$  sont des morphismes de groupes, alors  $g \circ f$  en est encore un.

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un isomorphisme de groupes.  
Alors  $f^{-1}$  est un isomorphisme du groupe  $(G', \bullet)$  sur le groupe  $(G, \star)$ .

## b. Propriétés

### Propriété :

Si  $f : (G, \star) \rightarrow (G', \bullet)$  et  $g : (G', \bullet) \rightarrow (G'', \Delta)$  sont des morphismes de groupes, alors  $g \circ f$  en est encore un.

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un isomorphisme de groupes.  
Alors  $f^{-1}$  est un isomorphisme du groupe  $(G', \bullet)$  sur le groupe  $(G, \star)$ .

### Propriété :

On note  $\text{Aut}(G)$  l'ensemble des automorphismes du groupe  $(G, \star)$ .  
Alors  $(\text{Aut}(G), \circ)$  a une structure de groupe.

## c. Noyau, image

### Définition : Image et noyau d'un morphisme de groupes

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

## c. Noyau, image

### Définition : Image et noyau d'un morphisme de groupes

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

- On appelle **noyau** de  $f$  :

$$\text{Ker } f = f^{-1}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\}.$$

Ainsi,  $x \in \text{Ker } f \iff f(x) = e_{G'}.$

## c. Noyau, image

### Définition : Image et noyau d'un morphisme de groupes

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

- On appelle **noyau** de  $f$  :

$$\text{Ker } f = f^{-1}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\}.$$

Ainsi,  $x \in \text{Ker } f \iff f(x) = e_{G'}$ .

- On appelle **image** de  $f$  :

$$\text{Im } f = f(G) = \{f(x), x \in G\}.$$

Ainsi,  $y \in \text{Im } f \iff \exists x \in G, y = f(x)$ .

## c. Noyau, image

Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupe.

## c. Noyau, image

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupe.

- $f$  est injectif si et seulement si  $\text{Ker } f = \{e_G\}$ .

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

Alors  $\text{Ker } f$  est un sous-groupe de  $(G, \star)$  et  $\text{Im } f$  est un sous-groupe de  $(G', \bullet)$ .

## c. Noyau, image

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupe.

- $f$  est injectif si et seulement si  $\text{Ker } f = \{e_G\}$ .
- $f$  est surjectif si et seulement si  $\text{Im } f = G'$ .

### Propriété :

Soit  $f : (G, \star) \rightarrow (G', \bullet)$  un morphisme de groupes.

Alors  $\text{Ker } f$  est un sous-groupe de  $(G, \star)$  et  $\text{Im } f$  est un sous-groupe de  $(G', \bullet)$ .

# Plan

- 1 Loi de composition interne
- 2 Structure de groupe
- 3 Groupe symétrique**
  - 1 Permutations
  - 2 Morphisme de signature et sous-groupe alterné

## a. Définition

### Définition : Permutation, groupe symétrique

Si  $E$  est un ensemble, on appelle **permutation** de  $E$  toute bijection de  $E$  dans  $E$ . On note  $\mathfrak{S}(E)$  leur ensemble.

## a. Définition

### Définition : Permutation, groupe symétrique

Si  $E$  est un ensemble, on appelle **permutation** de  $E$  toute bijection de  $E$  dans  $E$ . On note  $\mathfrak{S}(E)$  leur ensemble.

Si  $E = \llbracket 1, n \rrbracket$  où  $n \in \mathbb{N}^*$ , on note  $\mathfrak{S}_n$  appelé **groupe symétrique d'ordre  $n$  (ou de degré  $n$ )** cet ensemble.

## a. Définition

### Définition : Permutation, groupe symétrique

Si  $E$  est un ensemble, on appelle **permutation** de  $E$  toute bijection de  $E$  dans  $E$ . On note  $\mathfrak{S}(E)$  leur ensemble.

Si  $E = \llbracket 1, n \rrbracket$  où  $n \in \mathbb{N}^*$ , on note  $\mathfrak{S}_n$  appelé **groupe symétrique d'ordre  $n$  (ou de degré  $n$ )** cet ensemble.

Si  $\sigma \in \mathfrak{S}_n$ , on note  $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ .

## a. Définition

### Définition : Permutation, groupe symétrique

Si  $E$  est un ensemble, on appelle **permutation** de  $E$  toute bijection de  $E$  dans  $E$ . On note  $\mathfrak{S}(E)$  leur ensemble.

Si  $E = \llbracket 1, n \rrbracket$  où  $n \in \mathbb{N}^*$ , on note  $\mathfrak{S}_n$  appelé **groupe symétrique d'ordre  $n$  (ou de degré  $n$ )** cet ensemble.

Si  $\sigma \in \mathfrak{S}_n$ , on note  $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ .

### Propriété :

$(\mathfrak{S}_n, \circ)$  est un groupe d'ordre (ie de cardinal)  $n!$ , non abélien dès que  $n \geq 3$ .

## a. Définition

### Définition : Permutation, groupe symétrique

Si  $E$  est un ensemble, on appelle **permutation** de  $E$  toute bijection de  $E$  dans  $E$ . On note  $\mathfrak{S}(E)$  leur ensemble.

Si  $E = \llbracket 1, n \rrbracket$  où  $n \in \mathbb{N}^*$ , on note  $\mathfrak{S}_n$  appelé **groupe symétrique d'ordre  $n$  (ou de degré  $n$ )** cet ensemble.

Si  $\sigma \in \mathfrak{S}_n$ , on note  $\sigma = \left( \begin{array}{cccc} 1 & 2 & 3 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(n) \end{array} \right) \cdots$ .

### Propriété :

$(\mathfrak{S}_n, \circ)$  est un groupe d'ordre (ie de cardinal)  $n!$ , non abélien dès que  $n \geq 3$ .

## b. Ordre d'une permutation

Définition : Ordre d'une permutation

L'ordre d'une permutation  $\sigma$  est le plus petit  $k \in \mathbb{N}^*$  tel que  $\sigma^k = \text{id}$ .

## b. Ordre d'une permutation

Définition : Ordre d'une permutation

L'ordre d'une permutation  $\sigma$  est le plus petit  $k \in \mathbb{N}^*$  tel que  $\sigma^k = \text{id}$ .

Propriété :

L'ordre d'une permutation de  $\mathfrak{S}_n$  est bien défini et vaut au plus l'ordre  $n!$  de ce groupe.

## b. Ordre d'une permutation

Définition : Ordre d'une permutation

L'ordre d'une permutation  $\sigma$  est le plus petit  $k \in \mathbb{N}^*$  tel que  $\sigma^k = \text{id}$ .

Propriété :

L'ordre d'une permutation de  $\mathfrak{S}_n$  est bien défini et vaut au plus l'ordre  $n!$  de ce groupe.

## c. Orbites et support

### Définition : Orbites

Soit  $\sigma \in \mathfrak{S}_n$ . La relation binaire définie sur  $\llbracket 1, n \rrbracket$  par

$$x \sim y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence dont les classes d'équivalence sont les **orbites** de  $\sigma$ .

Si  $x \in \llbracket 1, n \rrbracket$ ,

$$\mathcal{O}(x) = \left\{ \sigma^k(x), k \in \mathbb{Z} \right\}.$$

## c. Orbites et support

Propriété :

Soit  $\sigma \in \mathfrak{S}_n$ ,  $x \in \llbracket 1, n \rrbracket$ . Alors il existe  $\ell \in \mathbb{N}$  tel que  
 $\mathcal{O}(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$  (deux à deux distincts).

## c. Orbites et support

### Propriété :

Soit  $\sigma \in \mathfrak{S}_n$ ,  $x \in \llbracket 1, n \rrbracket$ . Alors il existe  $\ell \in \mathbb{N}$  tel que  $\mathcal{O}(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$  (deux à deux distincts).

### Définition : Support

Si  $\sigma \in \mathfrak{S}_n$ , son **support** est l'ensemble des éléments de  $\llbracket 1, n \rrbracket$  qui **ne sont pas** invariants par  $\sigma$ .

## c. Orbites et support

### Propriété :

Soit  $\sigma \in \mathfrak{S}_n$ ,  $x \in \llbracket 1, n \rrbracket$ . Alors il existe  $\ell \in \mathbb{N}$  tel que  $\mathcal{O}(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$  (deux à deux distincts).

### Définition : Support

Si  $\sigma \in \mathfrak{S}_n$ , son **support** est l'ensemble des éléments de  $\llbracket 1, n \rrbracket$  qui **ne sont pas** invariants par  $\sigma$ .

### Propriétés :

- i  $\text{Supp}(\sigma)$  est stable par  $\sigma$ .
- ii Deux permutations à supports disjoints commutent.

## d. Transpositions, cycles

### Définition : Transposition

Une **transposition**  $\tau$  est une permutation qui échange deux éléments  $i$  et  $j$  de  $\llbracket 1, n \rrbracket$ , et laisse les autres invariants  $ie$  dont le support est  $\{i, j\}$ .

## d. Transpositions, cycles

### Définition : Transposition

Une **transposition**  $\tau$  est une permutation qui échange deux éléments  $i$  et  $j$  de  $\llbracket 1, n \rrbracket$ , et laisse les autres invariants  $ie$  dont le support est  $\{i, j\}$ .

On la note  $\tau = (i j)$  ou parfois  $\tau_{i,j}$ .

## d. Transpositions, cycles

### Définition : Transposition

Une **transposition**  $\tau$  est une permutation qui échange deux éléments  $i$  et  $j$  de  $\llbracket 1, n \rrbracket$ , et laisse les autres invariants  $ie$  dont le support est  $\{i, j\}$ .

On la note  $\tau = (i j)$  ou parfois  $\tau_{i,j}$ .

$$\begin{cases} \tau_{i,j}(i) = j \\ \tau_{i,j}(j) = i \\ \tau_{i,j}(k) = k \quad \text{si } k \notin \{i, j\} \end{cases}$$

## d. Transpositions, cycles

### Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

## d. Transpositions, cycles

### Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  **$p$ -cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_n$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants

## d. Transpositions, cycles

### Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  **$p$ -cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_p$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants *ie* dont le support est  $\{i_1, \dots, i_p\}$  et telle que

$$c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$$

## d. Transpositions, cycles

## Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  $p$ -**cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_p$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants *ie* dont le support est  $\{i_1, \dots, i_p\}$  et telle que

$$c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$$

$p$  est appelé **longueur** du cycle  $c$ .

## d. Transpositions, cycles

## Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  $p$ -**cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_p$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants *ie* dont le support est  $\{i_1, \dots, i_p\}$  et telle que

$$c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$$

$p$  est appelé **longueur** du cycle  $c$ .

On note  $c = (i_1 i_2 \dots i_p)$ .

## d. Transpositions, cycles

## Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  $p$ -**cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_p$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants *ie* dont le support est  $\{i_1, \dots, i_p\}$  et telle que

$$c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$$

$p$  est appelé **longueur** du cycle  $c$ .

On note  $c = (i_1 i_2 \dots i_p)$ .

## Propriété :

i

$$\begin{aligned}(i_1 i_2 \dots i_p) &= (i_1 i_p) (i_1 i_{p-1}) \dots (i_1 i_2) \\ &= (i_1 i_2) (i_2 i_3) \dots (i_{p-1} i_p).\end{aligned}$$

## d. Transpositions, cycles

## Définition : Cycle

Soit  $p \in \mathbb{N}$  tel que  $2 \leq p \leq n$ .

On appelle  **$p$ -cycle** une permutation  $c$  de  $\mathfrak{S}_n$  qui permute circulairement  $p$  éléments  $i_1, i_2, \dots, i_p$  de  $\llbracket 1, n \rrbracket$  et laisse les autres invariants *ie* dont le support est  $\{i_1, \dots, i_p\}$  et telle que

$$c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$$

$p$  est appelé **longueur** du cycle  $c$ .

On note  $c = (i_1 \ i_2 \ \dots \ i_p)$ .

## Propriété :

$$\begin{aligned} \text{i} \quad (i_1 \ i_2 \ \dots \ i_p) &= (i_1 \ i_p) (i_1 \ i_{p-1}) \dots (i_1 \ i_2) \\ &= (i_1 \ i_2) (i_2 \ i_3) \dots (i_{p-1} \ i_p). \end{aligned}$$

ii Un  $p$ -cycle est d'ordre  $p$ .

## d. Transpositions, cycles

### Théorème :

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

## d. Transpositions, cycles

### Théorème :

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

### Corollaire :

Toute permutation se décompose en produit de transpositions.

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

On note  $I(\sigma)$  le nombre d'inversions par  $\sigma$ .

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

On note  $I(\sigma)$  le nombre d'inversions par  $\sigma$ .

On appelle **signature** de  $\sigma$  le nombre  $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$ .

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

On note  $I(\sigma)$  le nombre d'inversions par  $\sigma$ .

On appelle **signature** de  $\sigma$  le nombre  $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$ .

Une permutation  $\sigma$  est dite **paire** lorsque  $I(\sigma)$  est pair et donc  $\varepsilon(\sigma) = 1$ . Elle est dite **impaire** dans le cas contraire.

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

On note  $I(\sigma)$  le nombre d'inversions par  $\sigma$ .

On appelle **signature** de  $\sigma$  le nombre  $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$ .

Une permutation  $\sigma$  est dite **paire** lorsque  $I(\sigma)$  est pair et donc  $\varepsilon(\sigma) = 1$ . Elle est dite **impaire** dans le cas contraire.

Méthode : Détermination pratique du nombre d'inversions

Pour chaque nombre de la deuxième ligne (image), on compte le nombre de nombres plus petits situés à sa droite. Et on fait la somme.

## a. Signature d'une permutation

### Définition : Inversions, signature

Soit  $\sigma \in \mathfrak{S}_n$ . On appelle **inversion** par  $\sigma$  tout couple  $(i, j)$  tel que  $i < j$  et  $\sigma(i) > \sigma(j)$ .

On note  $I(\sigma)$  le nombre d'inversions par  $\sigma$ .

On appelle **signature** de  $\sigma$  le nombre  $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$ .

Une permutation  $\sigma$  est dite **paire** lorsque  $I(\sigma)$  est pair et donc  $\varepsilon(\sigma) = 1$ . Elle est dite **impaire** dans le cas contraire.

Méthode : Détermination pratique du nombre d'inversions

Pour chaque nombre de la deuxième ligne (image), on compte le nombre de nombres plus petits situés à sa droite. Et on fait la somme.

Propriété :

Toute transposition est impaire.

## a. Signature d'une permutation

### Lemme : Expression de la signature

Soit  $\sigma \in \mathfrak{S}_n$ .

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

où  $\mathcal{P} = \left\{ \{i, j\} \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq n \text{ et } i \neq j \right\}$  désigne l'ensemble des paires d'entiers distincts compris entre 1 et  $n$ .

## a. Signature d'une permutation

### Lemme : Expression de la signature

Soit  $\sigma \in \mathfrak{S}_n$ .

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i, j\} \in \mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

où  $\mathcal{P} = \left\{ \{i, j\} \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq n \text{ et } i \neq j \right\}$  désigne l'ensemble des paires d'entiers distincts compris entre 1 et  $n$ .

### Théorème : Morphisme de signature

Soit  $n \geq 2$ . L'application

$$\varepsilon : \begin{array}{l} (\mathfrak{S}_n, \circ) \longrightarrow (\{-1, 1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma \longmapsto \varepsilon(\sigma) \end{array}$$

est un morphisme de groupe, ie

## a. Signature d'une permutation

## Lemme : Expression de la signature

Soit  $\sigma \in \mathfrak{S}_n$ .

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

où  $\mathcal{P} = \left\{ \{i, j\} \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq n \text{ et } i \neq j \right\}$  désigne l'ensemble des paires d'entiers distincts compris entre 1 et  $n$ .

## Théorème : Morphisme de signature

Soit  $n \geq 2$ . L'application

$$\varepsilon : \begin{array}{l} (\mathfrak{S}_n, \circ) \longrightarrow (\{-1, 1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma \longmapsto \varepsilon(\sigma) \end{array}$$

est un morphisme de groupe, i.e. tsi  $\sigma, \sigma' \in \mathfrak{S}_n$ ,  $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$ .

## a. Signature d'une permutation

### Propriétés :

- i** Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.

## a. Signature d'une permutation

### Propriétés :

- i Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.
- ii Si  $\sigma \in \mathfrak{S}_n$  se décompose en produit de  $N$  transpositions,  $\varepsilon(\sigma) = (-1)^N$ .  
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.

## a. Signature d'une permutation

### Propriétés :

- i Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.
- ii Si  $\sigma \in \mathfrak{S}_n$  se décompose en produit de  $N$  transpositions,  $\varepsilon(\sigma) = (-1)^N$ . En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.
- iii  $\varepsilon$  est le seul morphisme de groupes de  $\mathfrak{S}_n$  dans  $\{-1, 1\}$  tel que  $\varepsilon(\tau) = -1$  pour toute transposition  $\tau$ . (C'est en fait aussi le seul morphisme de groupe surjectif.)

## a. Signature d'une permutation

### Propriétés :

- i** Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.
- ii** Si  $\sigma \in \mathfrak{S}_n$  se décompose en produit de  $N$  transpositions,  $\varepsilon(\sigma) = (-1)^N$ .  
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.
- iii**  $\varepsilon$  est le seul morphisme de groupes de  $\mathfrak{S}_n$  dans  $\{-1, 1\}$  tel que  $\varepsilon(\tau) = -1$  pour toute transposition  $\tau$ . (C'est en fait aussi le seul morphisme de groupe surjectif.)
- iv** Si  $c$  est un  $p$ -cycle,  $\varepsilon(c) = (-1)^{p-1}$ .

## a. Signature d'une permutation

### Propriétés :

- i** Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.
- ii** Si  $\sigma \in \mathfrak{S}_n$  se décompose en produit de  $N$  transpositions,  $\varepsilon(\sigma) = (-1)^N$ . En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.
- iii**  $\varepsilon$  est le seul morphisme de groupes de  $\mathfrak{S}_n$  dans  $\{-1, 1\}$  tel que  $\varepsilon(\tau) = -1$  pour toute transposition  $\tau$ . (C'est en fait aussi le seul morphisme de groupe surjectif.)
- iv** Si  $c$  est un  $p$ -cycle,  $\varepsilon(c) = (-1)^{p-1}$ .
- v** Si  $\sigma \in \mathfrak{S}_n$ ,  $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ .

## b. Groupe alterné (HP)

### Définition : Groupe alterné

Le sous-groupe  $\mathfrak{A}_n = \text{Ker}(\varepsilon)$  des permutations paires de  $\mathfrak{S}_n$  est appelé ***groupe alterné d'ordre  $n$  (ou de degré  $n$ ).***

## b. Groupe alterné (HP)

### Définition : Groupe alterné

Le sous-groupe  $\mathfrak{A}_n = \text{Ker}(\varepsilon)$  des permutations paires de  $\mathfrak{S}_n$  est appelé **groupe alterné d'ordre  $n$  (ou de degré  $n$ )**.

### Propriété :

Pour tout  $n \geq 2$ ,  $|\mathfrak{A}_n| = \frac{n!}{2}$ .