# Chapitre 14

# Structures algébriques fondamentales

## Sommaire

OBJECTIFS

- ▷ savoir effectuer des calculs dans un groupe, anneau, ou corps
- ▷ savoir démontrer qu'un ensemble est un sous-groupe, un sous-anneau ou un sous-corps
- ▷ savoir décomposer une permutation en produit de transpositions
- ▷ savoir calculer la signature d'une permutation

# I Lois de composition interne

## 1 Définition, exemples

**Définition :** *Une* ***loi de composition interne*** $\star$ *sur un ensemble* $E$ *est une application de* $\star : E \times E \to E$. *On note plutôt* $x \star y$ *à la place de* $\star(x, y)$.

**Exemples :**

- L'addition est une loi de composition interne sur $\mathbf{N}$, $(x, y) \in \mathbf{N}^2 \mapsto x + y$.
- La multiplication est une *lci* sur $\mathbf{N}$, $(x, y) \in \mathbf{N}^2 \mapsto x.y$.
- L'addition définie par la règle du parallélogramme, est une loi de composition interne sur l'ensemble des vecteurs du plan.
- Le produit vectoriel est une loi de composition interne sur l'ensemble des vecteurs de l'espace.
- La composition des applications de $E$ dans lui-même est une loi de composition interne.
- Dans $\mathscr{P}(E)$, les opérations $\cup, \cap, \Delta$ sont des lois de composition interne.

**Vocabulaire :** *Un ensemble* $E$*, muni d'une lci* $\star$ *est appelé un magma.*

## 2 Propriétés des lois de composition interne

**Définition :** *Soit* $(E, \star)$ *un magma. On dit que* $\star$ *est*

- ***associative*** *si* $\forall (x, y, z) \in E^3,\ x \star (y \star z) = (x \star y) \star z$.
- ***commutative*** *si* $\forall (x, y) \in E^2,\ x \star y = y \star x$.

**Exemples :**

- dans les ensembles de nombres, $+$ et $\times$ sont commutatives, associatives,
- la composition des applications est associative, mais non commutative en général.
- le produit vectoriel des vecteurs de l'espace n'est pas commutatif ni associatif
- la différence symétrique $\Delta$ dans $\mathscr{P}(E)$ est commutative et associative.

## 3 Eléments remarquables de $(E, \star)$

### 3.a Élément neutre

**Définition :** *Un élément* $e$ *de* $(E, \star)$ *est dit* ***élément neutre*** *pour* $\star$ *si :* $\forall x \in E,\ x \star e = e \star x = x$

**Exemple :** $\emptyset$ est élément neutre pour la loi $\Delta$ dans $\mathscr{P}(E)$.

**Proposition 14.1.— Unicité de l'élément neutre —.** Soit $(E, \star)$ un magma. Si $E$ possède un élément neutre, il est unique.

**Démonstration** ▽
Soit $(e_1, e_2) \in E^2$ un couple d'éléments neutres : $\begin{array}{l}\forall x \in E, \quad x \star e_1 = e_1 \star x = x \\ \forall x \in E, \quad x \star e_2 = e_2 \star x = x\end{array}$ Alors

$$\begin{array}{rcl} e_1 \star e_2 & = & e_1 \text{ car } e_2 \text{ est neutre à droite} \\ e_1 \star e_2 & = & e_2 \text{ car } e_1 \text{ est neutre à gauche} \end{array}$$

Finalement $e_1 = e_2$. ▲

### 3.b Élément symétrique

**Définition :** *Soit $(E, \star)$ un magma associatif. On suppose que $E$ possède un élément neutre $e$. Soit $x \in E$. On appelle* ***symétrique*** *de $x$ tout élément $x'$ de $E$, tel que $x \star x' = x' \star x = e$.*

**Proposition 14.2.—** Soit $(E, \star)$ un magma associatif. Le symétrique d'un élément $x$, s'il existe, est unique.

**Démonstration** ▽
Soit $x \in E$ et $(x', x'')$ un couple d'éléments de $E$, symétriques de $x$. Considérons l'élément $y = (x' \star x) \star x''$. Par associativité de $\star$, on a

$$\begin{array}{rcl} y & = & (x' \star x) \star x'' = e \star x'' = x'' \\ y & = & x' \star (x \star x'') = x' \star e = x'. \end{array}$$

Il s'ensuit que $x' = x''$. ▲

### 3.c Itérés d'un élément

Lorsque la loi $\star$ est associative, on peut définir les composés de plusieurs éléments : $x_1 \star x_2 \star \cdots \star x_n$. En particulier, en composant un élément avec lui-même, on obtient la définition des

**Définition : Itérés d'un élément —.** *Soit $(E, \star)$ un magma associatif unitaire. Soit $x \in E$. On définit la suite des itérés de $x$ par :.*

- $x^{\star 0} = e$,
- *Pour tout entier naturel $n \in \mathbf{N}$, $x^{\star(n+1)} = x \star x^{\star n}$.*

**Commentaires :** en clair $x^{\star n}$ est le composé de $x$ par lui-même, $n$ fois : $x^{\star n} = \underbrace{x \star \cdots \star x}_{n \ fois}$.

## 4 Notations additives, multiplicatives

La plupart du temps les lci sont notées $+$, $\times$ ou $\star$. Le tableau suivant précise ces différentes notations :

| loi | composé de $x$ et $y$ | élément neutre | symétrique de $x$ | $n^{\text{ième}}$ itéré de $x$ |
|---|---|---|---|---|
| $\star$ | $x \star y$ | $e$ | $x'$ ou $x^{\star(-1)}$ est le symétrique de $x$ | $\underbrace{x \star \cdots \star x}_{n \ fois} = x^{\star n}$ |
| $+$ | $x + y$ | $0_E$ | $-x$ est l'opposé de $x$ | $\underbrace{x + \cdots + x}_{n \ fois} = nx$ |
| $\times$ ou . | $x \times y$ | $1_E$ | $x^{-1}$ est l'inverse de $x$ | $\underbrace{x \times \cdots \times x}_{n \ fois} = x^n$ |

**Remarque :** ce ne sont pas les seules notations possibles, par exemple, la loi de composition des applications de $E$ vers lui-même est noté $\circ$.

## 5 Étude d'une loi de composition interne

### 5.a Plan d'étude

Pour étudier une l.c.i. $\star : E \times E \to E$, vous devez :
0 vérifier qu'il s'agit bien d'une l.c.i. : le composé $x \star y$ de deux éléments de $E$ appartient-il toujours à $E$ ?
1 vérifier si $\star$ est commutative (simple) ;
2 vérifier si $\star$ est associative (pas dur) ;

3 vérifier l'existence d'un élément neutre : s'il existe, il satisfait $\forall x \in E,\ x \star e = e \star x = x$.

4 déterminer les éléments symétrisables $x$ : ce sont ceux pour lesquels le système d'inconnue $y \in E$

$$\left\{ \begin{array}{rcl} x \star y & = & e \\ y \star x & = & e \end{array} \right.$$

admet une solution.

5 Calcul des itérés d'un élément $x$. Pour cela

- calculer $x^2$, $x^3$ ;
- conjecturer l'expression de $x^n$ en fonction de $n \in \mathbf{N}$ ;
- démontrer cette relation par récurrence.

### 5.b Mise en œuvre

**Exemple :** soit $E = \mathbf{R} \setminus \{1\}$. Étudions les propriétés de la loi $\star$ définie dans $E$ par

$$\forall (x, y) \in E^2, \quad x \star y = x + y - xy.$$

0 Vérifions tout d'abord que $\star$ est une loi de composition interne dans $E$ :
Soit donc $(x, y) \in E^2$, il s'agit de prouver que $x \star y \in E$. Or

$$x \star y = 1 \iff x + y - xy = 1 \iff xy - x - y + 1 = 0 \iff (x-1)(y-1) = 0.$$

Comme $x$ et $y$ sont différents de 1, il s'ensuit que $x \star y$ l'est aussi.
De plus, on a aussi obtenu l'expression $x \star y = 1 - (1-x)(1-y)$.

1 Clairement, $\star$ est commutative puisque pour tout couple $(x, y)$ d'éléments de $E$, $x \star y = y \star x$.

2 Étudions l'associativité de $\star$. Soit $(x, y, z) \in E^3$. On a

$$\begin{array}{rcl} (x \star y) \star z & = & 1 - \big(1 - x \star y\big)\big(1 - z\big) \\ & = & 1 - (1-x)(1-y)(1-z) \end{array} \qquad \begin{array}{rcl} x \star (y \star z) & = & 1 - \big(1 - x\big)\big(1 - y \star z\big) \\ & = & 1 - (1-x)(1-y)(1-z) \end{array}$$

Ainsi, $(x \star y) \star z = x \star (y \star z)$. $\star$ est associative.

3 Étudions l'existence d'un élément neutre. S'il existe, $e$ vérifie que pour tout $x \in E$, $x \star e = x$. Raisonnons par équivalences :

$$x \star e = x \iff x + e - xe = x \iff e(1-x) = 0 \iff e = 0.$$

Ainsi, $e = 0$ est élément neutre de $E$ pour la loi $\star$.

4 Déterminons les éléments symétrisables de $E$. Soit $x \in E$. Raisonnons par équivalences :

$$\left\{ \begin{array}{rcl} x \star y & = & e \\ y \star x & = & e \end{array} \right. \iff x \star y = 0 \iff x + y - xy = 0 \iff y(1-x) = -x \iff y = \frac{x}{x-1}$$

Ainsi, tout élément $x$ de $E$ est inversible et $x^{-1} = \dfrac{x}{x-1}$.

5 Pour tout $x \in E$, on a $x^{\star 2} = x \star x = 1 - (1-x)^2$, $x^{\star 3} = 1 - \big(1 - x^{\star 2}\big)(1-x) = 1 - (1-x)^3$. Montrons par récurrence que $\forall n \in \mathbf{N}^\star, x^{\star n} = 1 - (1-x)^n$. En effet, le résultat est évident pour $n = 1$. Soit $n \in \mathbf{N}^\star$ tel que $x^{\star n} = 1 - (1-x)^n$. Alors $x^{\star(n+1)} = x \star x^{\star n} = 1 - \big(1 - x^{\star n}\big)(1-x) = 1 - (1-x)^n(1-x) = 1 - (1-x)^{n+1}$. La propriété est donc bien héréditaire.

## II Groupes

#### Exemple introductif : étude de la loi $\circ$ sur l'ensemble des bijections de $\{1, 2, 3\}$

Notons $\mathfrak{S}_3$ l'ensemble des **permutations** de $\{1, 2, 3\}$. Comme nous l'avons vu au **Chapitre 11**, $\mathfrak{S}_3$ est un ensemble fini à $6 = 3!$ éléments. La composition des applications induit une loi de composition interne sur $\mathfrak{S}_3$ car d'après la **Proposition** 6.11, la composée de deux bijections est une bijection.
D'autre part, nous avons vu que la loi $\circ$ est associative. Afin d'étudier la loi $\circ$ sur $\mathfrak{S}_3$, explicitons tout d'abord

l'ensemble $\mathfrak{S}_3$. Il est formé des 6 éléments suivants :

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Nous avons ici utilisé une notation spécifique aux permutations. Par exemple $\tau_1$ est la bijection de $\{1,2,3\}$ dans lui-même définie par :

$$\begin{aligned} \tau_1(1) &= 1 \\ \tau_1(2) &= 3 \\ \tau_1(3) &= 2. \end{aligned}$$

Nous pouvons alors représenter la loi de composition interne $\circ$ dans le tableau suivant :

| $\curvearrowright$ | $i$ | $\sigma_1$ | $\sigma_2$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
|---|---|---|---|---|---|---|
| $i$ | $i$ | $\sigma_1$ | $\sigma_2$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
| $\sigma_1$ | $\sigma_1$ | $\sigma_2$ | $i$ | $\tau_3$ | $\tau_1$ | $\tau_2$ |
| $\sigma_2$ | $\sigma_2$ | $i$ | $\sigma_1$ | $\tau_2$ | $\tau_3$ | $\tau_1$ |
| $\tau_1$ | $\tau_1$ | $\tau_2$ | $\tau_3$ | $i$ | $\sigma_1$ | $\sigma_2$ |
| $\tau_2$ | $\tau_2$ | $\tau_3$ | $\tau_1$ | $\sigma_2$ | $i$ | $\sigma_1$ |
| $\tau_3$ | $\tau_3$ | $\tau_1$ | $\tau_2$ | $\sigma_1$ | $\sigma_2$ | $i$ |

La première observation c'est que $i$ est l'élément neutre pour $(\mathfrak{S}_3, \circ)$. En effet, les premières ligne et colonne du tableau montrent que pour tout $\sigma \in \mathfrak{S}_3$, $\sigma \circ i = i \circ \sigma = \sigma$.
De plus, on peut remarquer que dans chaque ligne et chaque colonne apparaissent tous les éléments de $\mathfrak{S}_3$. Cela signifie que pour toutes permutations $\alpha, \beta \in \mathfrak{S}_3$, les équations :

$$\alpha \circ \sigma = \beta \text{ et } \sigma \circ \alpha = \beta$$

possèdent chacune une unique solution dans $\mathfrak{S}_3$. Autrement dit, pour toute permutation $\alpha \in \mathfrak{S}_3$, l'application $\Phi_\alpha$ de $\mathfrak{S}_3$ dans lui-même, qui à $\sigma \in \mathfrak{S}_3$ associe $\Phi_\alpha(\sigma) = \alpha \circ \sigma$ et l'application $\Phi^\alpha$ de $\mathfrak{S}_3$ dans lui-même, qui à $\sigma \in \mathfrak{S}_3$ associe $\Phi^\alpha(\sigma) = \sigma \circ \alpha$ sont bijectives.
En particulier, dans chaque ligne et chaque colonne apparait une fois l'élément neutre. De plus, globalement, on peut observer que les $i$ sont répartis de manière **symétrique** dans le tableau, par rapport à la diagonale. Cela signifie que tout élément possède un élément **symétrique** pour $\circ$ au sens de la définition ci-dessus.
En revanche, le tableau n'est pas globalement symétrique. Ceci ≪prouve ≫que la loi $\circ$ n'est pas commutative !

# 1 Structure de groupe

## 1.a Définition axiomatique, exemples

**Définition :** *Soit $G$ un ensemble muni d'une loi de composition interne $\star$. On dit que $(G, \star)$ est un **groupe** si :*

- $(G_0)$ *$\star$ est une loi de composition interne dans $G$.*
- $(G_1)$ *$\star$ est associative.*
- $(G_2)$ *$\star$ possède un élément neutre.*
- $(G_3)$ *tout élément possède un symétrique.*

*Si de plus la loi $\star$ est commutative, on dit que $G$ est **groupe commutatif**, ou **abélien**.*

**Remarque :** l'ensemble vide n'est pas un groupe, car il ne possède pas d'élément neutre. Autrement dit, un groupe n'est jamais vide !

**Exemples :** $\mathfrak{S}_3$ est un groupe non commutatif. Vous connaissez d'autres groupes :

- $E = \mathbf{R} \setminus \{1\}$ muni de la loi $\star$ définie dans l'exemple précédent est un groupe abélien.
- $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$.

- $(\mathbf{Q}^\star, .)$, $(\mathbf{R}^\star, .)$,$(\mathbf{C}^\star, .)$ sont des groupes commutatifs.
- $(\vec{\mathcal{P}}, +)$ et $(\vec{\mathscr{E}}, +)$ sont des groupes commutatifs
- Soit $E$ un ensemble et $\mathfrak{S}(E)$ l'ensemble des bijections de $E$ dans lui-même. $\big(\mathfrak{S}(E), \circ\big)$ est un groupe.
- $(\mathscr{P}(E), \Delta)$ est un groupe commutatif.

En revanche, $(\mathbf{N}, +)$ et $(\mathbf{R}, \times)$ ne sont pas des groupes. *Voyez-vous pourquoi ?*

### 1.b Propriétés fondamentales

Dans la suite du cours, une loi de groupe sera généralement notée $\times$. Il est important de savoir traduire toutes les propriétés énoncées, en notation $\star$ ou $+$.

**Proposition 14.3.—** Soit $(G, \times)$ un groupe. Alors
- l'élément neutre $1_G$ est unique.
- tout élément $x \in G$ admet un unique symétrique (inverse), noté $x^{-1}$.

**Démonstration** ▽
$(G, \times)$ est un magma associatif unitaire. ▲

### 1.c Règles de calcul dans un groupe

**Proposition 14.4.—** Soit $(G, \times)$ un groupe, $x \in G$. Pour tout couple $(n, m) \in \mathbf{N}^2$ d'entiers naturels, on a :

$$x^n \times x^m = x^{n+m} \text{ et } \big(x^n\big)^m = x^{n \times m}$$

**Démonstration** ▽
Soit $x \in G$ et $n \in \mathbf{N}$ fixés. Nous démontrons ces deux propriétés par récurrence sur $m$.

- **Init.** $x^n \times x^0 = x^n$.
- **Hér.** soit $m \in \mathbf{N}$ tel que $x^n \times x^m = x^{n+m}$. Alors $x^n \times x^{m+1} = x^n \times (x^m \times x) = x^{n+m} \times x = x^{n+m+1}$.
- **Ccl.** Ok !!

- **Init.** $\big(x^n\big)^0 = x^n$.
- **Hér.** soit $m \in \mathbf{N}$ tel que $\big(x^n\big)^m = x^{n \cdot m}$. Alors
  $\big(x^n\big)^{m+1} = \big(x^n\big)^m \times \big(x^n\big) = big(x^{n \cdot m}\big) \times x^n = x^{n \cdot m + n} = x^{n \cdot (m+1)}$.
- **Ccl.** Ok !! ▲

Comme tout élément du groupe est inversible, nous allons étendre ces relations au cas où les exposants sont des entiers relatifs.

— Pour $n \in \mathbf{N}$, $x^n = \underbrace{x \times \cdots \times x}_{n \ fois}$,

— Pour $n \in \mathbf{Z}^-$, $x^n = \big(x^{-1}\big)^{|n|}$.

**Proposition 14.5.—** Soit $(G, \times)$ un groupe. Alors

- $\forall (x, y) \in G^2, (x \times y)^{-1} = y^{-1} \times x^{-1}$
- $\forall x \in G, \big(x^{-1}\big)^{-1} = x$.

**Démonstration** ▽

- Soit $(x, y) \in G^2$. Alors

$$(x \times y) \times (y^{-1} \times x^{-1}) = x \times (y \times y^{-1}) \times x^{-1} = x \times 1_G \times x^{-1} = 1_G$$
$$(y^{-1} \times x^{-1}) \times (x \times y) = y^{-1} \times (x^{-1} \times x) \times y = y^{-1} \times 1_G \times y = 1_G$$

  Par conséquent, $y^{-1} \times x^{-1}$ est l'inverse de $x \times y$.

- Soit $x \in G$. Alors $x \times x^{-1} = 1_G$ et $x^{-1} \times x = 1_G$ : $x$ est bien l'inverse de $x^{-1}$. ▲

Les deux propositions précédentes s'étendent aux itérés d'exposants des entiers relatifs quelconques :

**Théorème 14.6.— Règles de calculs dans un groupe —.** Soit $(G, \times)$ un groupe, $(x, y) \in G^2$. Pour tout couple $(n, m) \in \mathbf{Z}^2$ d'entiers relatifs, on a :

- $x^n \star x^m = x^{n+m}$
- $\left(x^n\right)^m = x^{n \times m}$.

**Attention :** lorsque le groupe $G$ n'est pas commutatif, on n'a pas toujours $(x \times y)^n = x^n \times y^n$.

### 1.d Équations dans un groupe

Le premier intérêt de la notion de groupe est de permettre de former et de résoudre des équations. Plus précisément, soit $(G, \times)$ un groupe, $(a, b) \in G^2$. On peut former deux équations d'inconnue $x \in G$ :

$$\begin{aligned} a \times x &= b && (E_1) \\ x \times a &= b && (E_2) \end{aligned}$$

**Proposition 14.7.— Tout élément de $G$ est simplifiable —.** Soit $(G, .)$ un groupe. Alors

- $\left(\forall a \in G\right),\ \left(\forall (x, y) \in G^2\right),\ (a \times x = a \times y) \iff (x = y)$
- $\left(\forall a \in G\right),\ \left(\forall (x, y) \in G^2\right),\ (x \times a = y \times a) \iff (x = y)$.

**Démonstration** ▽
Soit $(a, x, y) \in G^3$, tel que $a \times x = a \times y$. Multiplions à gauche les deux membres de cette égalité par $a^{-1}$, il vient $a^{-1} \times (a \times x) = a^{-1} \times (a \times y)$. Comme $a^{-1} \times a = 1_G$, il en résulte que $x = y$. De même si $(a, x, y) \in G^3$ vérifie $x \times a = y \times a$. On obtient en multipliant à droite par $a^{-1}$, que $(x \times a) \times a^{-1} = (y \times a) \times a^{-1}$, c'est-à-dire $x = y$.
Les réciproques sont évidentes. ▲

**Proposition 14.8.— Équations dans un groupe —.** Soit $(G, .)$ un groupe, $(a, b) \in G^2$.

- L'équation $a \times x = b$ possède une unique solution dans $G$ : $x = a^{-1} \times b$.
- L'équation $x \times a = b$ possède une unique solution dans $G$ : $x = b \times a^{-1}$.

**Remarque :** Ceci explique pourquoi la table de $\mathfrak{S}_3$ est si bien remplie ! Il en est donc de même de la table de n'importe quel groupe !

**Démonstration** ▽
Soit $(a, b) \in G^2$. Pour tout $x \in G$, on a les équivalences :

$$\begin{aligned} a \times x = b &\iff a^{-1} \times a \times x = a^{-1} \times b \iff x = a^{-1} \times b \\ x \times a = b &\iff x \times a \times a^{-1} = b \times a^{-1} \iff x = b \times a^{-1} \end{aligned}$$

▲

**Défi !** Soit $(G, \times)$ un magma associatif, non vide, pour lequel chacune des équations $(E_1)$ et $(E_2)$ admette une unique solution.
Montrez que $(G, \cdot)$ est un groupe.

## 2 Sous-groupes

### 2.a Définition, caractérisation

**Définition :** *Soit $(G, \times)$ un groupe et $H$ un sous-ensemble de $G$. On dit que $H$ est un* ***sous-groupe de*** *$G$, et on note $H < G$, si :*

- *$H$ est stable pour la loi de $G$ : $\forall (x, y) \in H \times H,\ x \times y \in H$.*

- $(H, \times)$ *est un groupe.*

**Exemples : ous-groupes triviaux d'un groupe**
si $(G, \times)$ est un groupe $\{1_G\}$ et $G$ sont des sous-groupes de $G$, dits sous-groupes triviaux.

**Commentaires :** par définition, une partie $H$ de $G$ est stable pour $\times$ si le produit de deux éléments e $H$ est encore dans $H$. En ce cas, $\times$ est une loi de composition interne sur $H$.

**Remarque :** en tant que partie de $G$, $H$ «hérite» certaines propriétés de $(G, +)$. Par exemple, la loi $\times$ étant associative sur $G$, elle l'est *a fortiori* dans $H$.

**En pratique :** Pour démontrer qu'une partie $H$ de $G$ est un sous-groupe de $G$, nous utiliserons **systématiquement** la caractérisation suivante.

**Théorème 14.9.— Caractérisation des sous-groupes**
Soit $(G, \times)$ un groupe et $H$ un sous-ensemble de $G$. Alors

$$H \text{ est un sous groupe de } G \text{ si et seulement si } \begin{array}{ll} (SG_1) & \bullet \quad H \neq \emptyset \\ (SG_2) & \bullet \quad \forall (x,y) \in H \times H,\ x \times y^{-1} \in H \end{array}$$

**Remarque :** la démonstration qui suit montre que :

- $1_G$ appartient nécessairement à $H$ et que c'est l'élément neutre de $H$.
- Pour tout élément $x \in H$, son inverse $x^{-1}$ dans $G$ appartient lui aussi à $H$ et c'est l'inverse de $x$ dans $H$.

**En pratique :** Pour démontrer qu'une partie $H$ de $G$ est un sous-groupe,

- $(SG_0)]$ $\quad H \subset G$
- $(SG_1)]$ $\quad 1_G \in H$
- $(SG_2)]$ $\quad \forall (x,y) \in H^2,\ x \times y^{-1} \in H.$

Il est parfois plus commode de scinder la deuxième assertion en deux :

- $(SG_0)]$ $\quad H \subset G$
- $(SG_1)]$ $\quad 1_G \in H$
- $(SG'_2)]$ $\quad \forall x \in H,\ x^{-1} \in H.$
- $(SG''_2)]$ $\quad \forall (x,y) \in H^2,\ x \times y^{\in} H.$

**En pratique :** on peut aussi utiliser ce théorème pour montrer que $(G, \times)$ est un groupe!! vous essayez de déterminer un groupe $(\hat{G}, \times)$ dont $G$ serait un sous-groupe.

**Démonstration** $\triangledown$
CN On suppose que $(H, \times)$ est un sous-groupe de $G$.
Alors $H$ possède un élément neutre, $1_H$, donc $H \neq \emptyset$.

- Soit $x \in H$, alors $1_G \times x = 1_H \times x$, donc $1_H = 1_G$.
- Soit $x \in H$, on note $x^{-1}$ l'inverse de $x$ dans $G$ et $x'$ l'inverse de $x$ dans $H$, de sorte que $x \times x' = x \times x^{-1} = 1_G$. Comme $x$ est simplifiable, il s'ensuit que $x' = x^{-1}$.
- Soit $(x,y) \in H^2$. Alors $x \in H$ et $y^{-1} \in H$ (d'après ce qui précède). Comme $\times$ est une lci dans $H$, il en résulte finalement que $x \times y^{-1} \in H$.

CS Montrons que la condition est suffisante. Soit $H \subset G$ une partie de $G$ vérifiant $SG_0)$ et $(SG_1)$.

- Comme $H$ est non vide, il existe $a \in G$.
- D'après $SG_2)$ $a \times a^{-1} \in H$. Ainsi $1_G \in H$.
- Soit $x \in H$, alors toujours d'après $(SG_2)$, $1_G \times x^{-1} = x^{-1} \in H$.
- Soit $(x,y) \in H^2$, alors $x$ et $y^{-1}$ appartiennent à $H$ d'après ce qui précède. Par conséquent $x \times y = x \times (y^{-1})^{-1} \in H$. Ceci étant vrai pour tout couple $(x,y)$, on a établi que $H$ est stable pour la loi $\times$ de $G$. Reste à prouver que $(H, \times)$ est un groupe.

- La loi $\times$ qui est associative dans $G$, l'est *a fortiori* dans $H$.

- De plus, nous venons de démontrer que $1_G \in H$. C'est donc un élément neutre pour $(H, \times)$, car $\forall x \in H \subset G,\ x \times 1_G = 1_G \times x = x$.
- Enfin, nous avons vu que pour tout élément $x$ de $H$, $x^{-1} \in H$, donc $x$ possède un symétrique pour $\times$.

▲

### 2.b Exemples de sous-groupes

**Nb :** comme par définition, un sous-groupe est un groupe, il s'agit aussi d'exemples de groupes !!
On vérifie, à l'aide de la caractérisation des sous-groupes que

1. des sous-groupes additifs $(\mathbf{Z}, +) < (\mathbf{Q}, +) < (\mathbf{R}, +) < (\mathbf{C}, +)$.
2. des sous-groupes multiplicatifs, $(\mathbf{Q}^\star, \times) < (\mathbf{R}^\star, \times) < (\mathbf{C}^\star, \times)$.
3. et d'autres encore, $(\mathbf{R}^{+\star}, \times) < (\mathbf{R}^\star, \times)$. L'ensemble $\mathcal{U}$ des nombres complexes de module 1 est un sous groupe de $(\mathbf{C}^\star, \times)$.

**Exercice :** Montrez que l'ensemble $\mathbf{U}_n$ des racines $n^{\text{ièmes}}$ de l'unité est un sous-groupe de $\mathcal{U}$.

**Exercice : Centre d'un groupe**
Soit $(G, \times)$ un groupe. On définit le centre de $G$ par

$$Z(G) = \{a \in G \,|\, \forall x \in G,\ xa = ax\}$$

Montrez que $Z(G)$ est un sous-groupe de $G$.

### 2.c Intersection de sous-groupes

**Proposition 14.10.—** Soit $G$ un groupe, $H, K$ deux sous-groupes de $G$. Alors $H \cap K$ est un sous-groupe de $G$.

**Démonstration** ▽
Nous utilisons, bien entendu la caractérisation **Théorème** 14.9 pour démontrer que $H \cap K$ est un ss-gpe de $G$. Remarquons tout d'abord que $H \cap K$ est non vide. En effet, $H$ et $K$ étant des sous-groupes de $G$, ils contiennent nécessairement tous deux l'élément neutre de $G$, $1_G$. D'autre part, si $x, y \in H \cap K$, alors $x, y \in H$ et $x, y \in K$ , donc ( puisque $H$ est un sous-groupe) $x \times y^{-1} \in H$ et de même $x \times y^{-1} \in K$. Il en résulte que $x \times y^{-1} \in H \cap K$. ▲

En général, la réunion de deux sous-groupes n'est pas un sous-groupe. Par exemple, dans le plan vectoriel. Les droites vectorielles engendrées par des vecteurs $\vec{u}, \vec{v}$ non colinéaires forment des sous-groupes. Mais leur réunion, $\mathcal{D}(\vec{u}) \cup \mathcal{D}(\vec{v})$ n'est pas stable pour l'addition. Ce n'est donc certainement pas un sous-groupe !!
À la place de la réunion des sous-groupes $H$ et $K$, on utilise le produit (ou la somme en notation additive) des $H$ et $K$, défini dans l'exercice suivant :

**Exercice : Produit de deux sous-groupes —.** Soit $(G, \times)$ un groupe commutatif, $H$ et $K$ deux sous-groupes de $G$. On définit $HK = \{hk;\ h \in H, k \in K\}$.

1. Montrez que $HK$ est un sous-groupe de $G$ contenant $H$ et $K$.
2. Montrez que $HK$ est le plus petit sous-groupe de $G$ contenant $H$ et $K$.

**Remarque :** Lorsque la loi du groupe $G$ est $+$, on définit la somme des sous-groupes $H$ et $K$ par

$$H + K = \{h + k;\ h \in H,\ k \in K\},$$

Il s'agit du plus petit sous-groupe de $(G, +)$ contenant $H$ et $K$.

Lorsque vous serez plus à l'aise avec la structure de groupe, vous pourrez démontrer :

**Exercice :** Soit $G$ un groupe, $H$ et $K$ deux sous-groupes de $G$. Alors

$$H \cup K \text{ est un sous-groupe de } G \text{ si et seulement si } (H \subset K) \textit{ ou } (K \subset H).$$

### 2.d Étude des sous-groupes de $(\mathbf{Z}, +)$

**Proposition 14.11.—** Soit $H$ une partie de $\mathbf{Z}$.

$$H \text{ est un sous-groupe de } \mathbf{Z} \textit{ si et seulement si } \text{il existe } a \in \mathbf{Z}, \text{ tel que } H = a\mathbf{Z}$$

**Remarque :** soit $(a, b) \in \mathbf{Z}^2$ un couple d'entiers relatifs. Alors $a\mathbf{Z} \cap b\mathbf{Z}$ et $a\mathbf{Z} + a\mathbf{Z}$ sont des sous-groupes de $\mathbf{Z}$. On a déjà établi les égalités suivantes :

$$\begin{array}{lrcl} \bullet & a\mathbf{Z} + b\mathbf{Z} & = & (a \wedge b)\mathbf{Z} \\ \bullet & a\mathbf{Z} \cap b\mathbf{Z} & = & (a \vee b)\mathbf{Z} \end{array}$$

**Démonstration** ▽

- soit $a \in \mathbf{N}$, on montre aisément à l'aide de la **caractérisation des sous-groupes** que $a\mathbf{Z}$ est bien un sous-groupe de $\mathbf{Z}$.
- soit $H$ un sous-groupe de $\mathbf{Z}$. on distingue deux cas, si $H$ est réduit à $\{0\}$, alors $H = 0\mathbf{Z}$. Si $H$ n'est pas réduit à $\{0\}$, $H \cap \mathbf{N}^\star$ est non vide. Il possède un plus petit élément. Notons-le $a$.
  - ▸ il est clair que $a\mathbf{Z} \subset H$.
  - ▸ réciproquement. Soit $n \in H$. Effectuons la division euclidienne de $n$ par $a$. Il existe un couple $(q, r)$ d'entiers tels que $0 \leq r < a$ et
    $$n = aq + r$$
    Comme $n$ et $aq$ appartiennent tous deux à $H$, il découle de la stabilité des sous-groupes par différence que $r$ est aussi élément de $H$. De l'inégalité $0 \leq r < a$, on déduit alors, grâce à la minimalité de $a$, que $r$ est nul. Ainsi, $n = aq$ est divisible par $a$, *i.e.* $n \in a\mathbf{Z}$.
  - ▸ par double-inclusion, on a prouvé que $H = a\mathbf{Z}$. ▲

## 3 Morphismes de groupes

### 3.a Définition, exemples

**Définition :** *Soit $(G, \times)$, $(G', \star)$ deux groupes. On appelle* ***morphisme de groupe*** *toute application $f : G \to G'$ telle que :*

$$\forall (x, y) \in G \times G, \quad f(x \times y) = f(x) \star f(y).$$

**Commentaires :** En clair, un morphisme de groupes, c'est une application **compatible** avec les lois des groupes $G$ et $G'$.

**Exemples :**

- L'application $f : t \in \mathbf{R} \mapsto f(t) = e^t \in \mathbf{R}^{+\star}$ vérifie $\forall (s, t) \in \mathbf{R}^2, f(s + t) = f(s) \times f(t)$. C'est donc un morphisme de $(\mathbf{R}, +)$ vers $(\mathbf{R}^{+\star}, \times)$.
- L'application $g : t \in \mathbf{R}^{+\star} \mapsto \ln(t) \in \mathbf{R}$ vérifie $\forall (s, t) \in \mathbf{R}+\star^2, g(s \times t) = g(s) + g(t)$. C'est un morphisme de $(\mathbf{R}^{+\star}, \times)$ vers $(\mathbf{R}, +)$.
- $h : t \mapsto e^{2i\pi t}$ est un morphisme de $(\mathbf{R}, +)$ sur $(\mathbf{U}, \times)$.

**Exercice :** Soit $(G, \times)$ un groupe et $a \in G$. Montrez que l'application $f : \mathbf{Z} \to G$ définie par

$$\forall n \in \mathbf{Z}, \quad f(n) = a^n$$

est un morphisme de $(\mathbf{Z}, +)$ vers $(G, \times)$. En particulier, si $a \in \mathbf{Z}$, l'application qui à tout entier $n \in \mathbf{Z}$ associe $an$ est un morphisme de $\mathbf{Z}$ dans lui-même.

**Vocabulaire :**

- ■ *Lorsque $G = G'$, un morphisme $f$ de $G$ dans lui-même est aussi appelé un* ***endomorphisme*** *de $G$.*

- *si de plus $f : G \to G'$ est bijectif, on dit que $f$ est un **isomorphisme** de groupes. On dit alors que **les groupes** $(G, .)$ **et** $(G', \star)$ **sont isomorphes**.*
- *Si $f : G \to G$ est un isomorphisme de $G$ sur lui-même, on dit que $f$ est un **automorphisme** de $G$.*

### 3.b Propriétés des morphismes de groupes

Un morphisme de groupe est totalement compatible avec les lois de groupes :

**Proposition 14.12.—** Soit $(G, \times)$ et $(G', \star)$ deux groupes et $f : G \to G'$ un morphisme de groupe. Alors pour tout $(x, y) \in G^2$, on a

- $f(1_G) = 1_{G'}$
- $f(x^{-1}) = f(x)^{\star(-1)}$
- $f(x \times y) = f(x) \star f(y)$
- $f(x \times y^{-1}) = f(x) \star f(y)^{\star(-1)}$.

**Démonstration** ▽

- Comme $f$ est un morphisme, nous avons $f(1_G) = f(1_G.1_G) = f(1_G) \star f(1_G)$. D'où $f(1_G) = 1_{G'}$.
- $1_{G'} = f(x.x^{-1}) = f(x) \star f(x^{-1})$et $1_{G'} = f(x^{-1}.x) = f(x^{-1}) \star f(x)$. D'où $f(x)^{\star(-1)} = f(x^{-1})$.
- $f(x \times y^{-1}) = f(x) \star f(y^{-1}) = f(x) \star f(y)^{\star(-1)}$. ▲

**Exemple :** si $(G, .)$ est un groupe et $a \in G$ est un élément de $G$, différent du neutre, les translations $\varphi_a$ et $\varphi^a$ ne sont pas des -endo- morphismes de $G$

**Proposition 14.13.—** Soit $(G, .)$, $(G', \times)$ et $(G'', \star)$ trois groupes et $G \xrightarrow{f} G' \xrightarrow{f'} G''$ deux morphismes de groupes. Alors l'application composée $f' \circ f$ est un morphisme de groupe de $G$ vers $G''$.

**Démonstration** ▽
Soit $(x, y) \in G^2$, alors $(f' \circ f)(x.y) = f'\big(f(x.y)\big) = f'\big(f(x) \times f(y)\big) = f'\big(f(x)\big) \star f'\big(f(y)\big) = (f' \circ f)(x) \star (f' \circ f)(y)$. ▲

**Proposition-Définition 14.14.— isomorphisme réciproque —.** Soit $f : G \to G'$ un isomorphisme de groupes. L'application réciproque $f^{-1} : G' \to G$ est un isomorphisme de $G'$ sur $G$.
On dit que $f^{-1}$ est l'**isomorphisme réciproque** de $f$.

**Démonstration** ▽
Soit $\alpha,\ \beta \in G'$, notons $a$ et $b$ leurs images respectives par $f^{-1}$. Alors

$$f^{-1}(\alpha \star \beta) = f^{-1}\big(f(a) \star f(b)\big) = f^{-1}\big(f(a.b)\big) = f^{-1} \circ f(a.b) = a.b = f^{-1}(\alpha) \star f^{-1}(\beta).$$

▲

**Exemple :**

- Le logarithme $\ln : \mathbf{R}^{+\star} \to \mathbf{R}$ est un isomorphisme de $(\mathbf{R}^{+\star}, .)$ sur $(\mathbf{R}, +)$.
- L'exponentielle $\exp : \mathbf{R} \to \mathbf{R}^{+\star}$ est son isomorphisme réciproque.

### 3.c Image et noyau d'un morphisme de groupes

**Théorème-Définition 14.15.—** Soit $(G, \times)$ et $(G', \star)$ deux groupes et $f : G \to G'$ un morphisme de groupes. Alors

- $f(G) = \{f(x)\ ;\ x \in G\}$ est un sous-groupe de $G'$. On l'appelle l'**image** de $f$. On note
$$\mathsf{Im}\, f = \{f(x)\ ;\ x \in G\}$$
- $\overline{f}^{1}(\{1_{G'}\}) = \{x \in G;\ f(x) = 1_{G'}\}$ est un sous-groupe de $G$, on l'appelle le **noyau** de $f$. On note
$$\mathsf{Ker}\, f = \{x \in G;\ f(x) = 1_{G'}\}$$

**En pratique :** $\mathsf{Ker}\, f$ est constitué de l'ensemble des antécédents de l'élément neutre de $G'$ par $f$. Pour déterminer $\mathsf{Ker}\, f$, vous résolvez dans $G$ l'équation

$$f(x) = 1_{G'}$$

**Exemple :** Soit $h : t \mapsto e^{2i\pi t}$. On sait que $h$ est un morphisme de $(\mathbf{R}, +)$ sur $(\mathbf{U}, \times)$. On vérifie aisément que $\mathsf{Ker}\, h = \mathbf{Z}$.

**Théorème 14.16.—** Soit $(G, \times)$ et $(G', \star)$ deux groupes et $f : G \to G'$ un morphisme de groupes. Alors

- $f$est surjectif *si et seulement si* $\mathsf{Im}\, f = G'$
- $f$est injectif *si et seulement si* $\mathsf{Ker}\, f = \{1_G\}$

**Remarque :** soit $f : G \to G'$ un morphisme de groupes. $\mathsf{Ker}\, f$ mesure le défaut d'injectivité. En effet, pour tout couple $(x, y) \in G^2$,

$$\begin{aligned} f(x) = f(y) &\iff f(x) \star f(y)^{-1} = 1_{G'} \iff f(x) \star f(y^{-1}) = 1_{G'} \\ &\iff f(x \times y^{-1}) = 1_{G'} \\ &\iff x \times y^{-1} \in \mathsf{Ker}\, f. \end{aligned} \tag{14.1}$$

**En pratique :** pour prouver qu'un morphisme de groupe est injectif, vous vérifiez que son noyau se réduit à l'élément neutre $\mathsf{Ker}\, f = \{1_G\}$.

**Démonstration** ▽
Supposons que $\mathsf{Ker}\, f = \{1_G\}$. On montre que $f$ est injectif. Soit donc $(x, y) \in G^2$ tels que $f(x) = f(y)$. D'après (14.1) il s'ensuit que $x \times y^{-1} \in \mathsf{Ker}\, f = \{1_G\}$.D'où $x.y^{-1} = 1_G$, c'es-à-dire $x = y$.
Réciproquement, supposons $f$ injectif. Soit $x \in \mathsf{Ker}\, f$, alors $f(x) = 1_{G'} = f(1_G)$. $f$ étant injectif, on en déduit que $x = 1_G$. ▲

# III Anneaux et corps

## 1 Structure d'anneau

### 1.a Définition axiomatique

**Définition :** *Soit $A$ un ensemble muni de deux lois de composition interne, notées $+$ et $\times$*
*On dit que $(A, +, \times)$* ***est un anneau*** *si :*

- $(A1)$ *$(A, +)$ est un* ***groupe commutatif****. L'élément neutre de $+$ est noté $0_A$.*
- $(A2)$ *la loi $\times$ est* ***associative****.*
- $(A3)$ *la loi $\times$ est* ***distributive par rapport à la loi*** *$+$, c'est-à-dire :*
  $\forall (x, y, z) \in A \times A \times A,\ x \times (y + z) = x \times y + x \times z$ *et* $(x + y) \times z = x \times z + y \times z$.
- $(A4)$ *la loi $\times$ possède un* ***élément neutre****, noté $1_A$*

*Si de plus la loi $\times$ est commutative, on dit que $(A, +, \times)$ est un* ***anneau commutatif****.*

**Attention :** dans un anneau, tous les éléments ne possèdent pas d'inverses pour $\times$ . Un élément qui possède un inverse pour . sera dit **inversible**.

### 1.b Exemples

1. $(\mathbf{Z}, +, \times)$, $(\mathbf{Q}, +, \times)$est un anneau commutatif.
2. $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$, $(\mathbf{C}, +, \times)$ sont des anneaux commutatifs.
3. $(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.

**Proposition 14.17.—** Soit $(A,+,\times)$ un anneau et $X$ un ensemble non vide. L'ensemble $A^X = \mathscr{F}(X,A)$ est muni de deux lci :
Soit $(f,g) \in A^X \times A^X$, somme et produit de $f$ et $g$ sont définies par

$$f+g : \begin{array}{ccc} X & \to & A \\ x & \mapsto & (f+g)(x) = f(x)+g(x) \end{array} \quad \text{et} \quad f\times g : \begin{array}{ccc} X & \to & A \\ x & \mapsto & (f\times g)(x) = f(x)\times g(x) \end{array}$$

Alors $(A^X,+,\times)$ est un anneau. De plus il est commutatif si $A$ l'est.

**Démonstration** ▽
L'élément neutre pour l'addition est la fonction constante égale à $0_A$, l'élément neutre pour la multiplication est la fonction constante égale à $1_A$.
L'anneau $(A^X,+,\times)$ est commutatif *si et seulement si* $(A,+,\times)$ l'est.

**Exemples :** En conséquence de cette proposition, les ensembles $\mathbf{R}^{\mathbf{N}}$ ou $\mathbf{C}^{\mathbf{N}}$ des suites de nombres réels ou complexes forment des anneaux commutatifs, de même que $\mathscr{F}(I,\mathbf{R})$ et $\mathscr{F}(I,\mathbf{C})$.

### 1.c Règles de calcul dans un anneau

L'exemple type d'anneau commutatif est $(\mathbf{Z},+,\times)$.

**Proposition 14.18.— Règles de calcul dans un anneau**
Soit $(A,+,\times)$ un anneau. Pour tous $(a,b,c) \in A^3$ et $m \in \mathbf{Z}$, on a :

| | | | |
|---|---|---|---|
| *i)* | $a\times 0_A = 0_A \times a = 0_A$ | *iv)* | $(-1_A)\times a = a\times(-1_A) = -a$ |
| *ii)* | $(-a)\times b = a\times(-b) = -(a\times b)$ | *v)* | $a\times(b-c) = a\times b - a\times c$ |
| *iii)* | $(-a)\times(-b) = a\times b$ | *vi)* | $(b-c)\times a = b\times a - c\times a$ |
| *vii)* | $a\times(mb) = (ma)\times b = m(a\times b)$ | | |

**Notation :** *nous avons noté $-a$ l'opposé de $a$, $a-b$ à la place de $a+(-b)$, et pour tout $m \in \mathbf{Z}$, $m.a$ est le $m^{ième}$ itéré de $a$ pour $+$.*

**Démonstration** ▽ i $0_A \times a = (0_A+0_A)\times a = 0_A\times a + 0_A\times a$. D'où $0_A\times a = 0_A$.
ii $(-a)\times b + a\times b = (-a+a)\times b = 0_A\times b = 0_A$ et $a\times b+(-a)\times b = 0_A$. D'où $(-a)\times b = -(a\times b)$
▲

### 1.d Sommes et produits finis

Soit $(A,+,\times)$ un anneau, alors pour toute famille finie $a_0, a_1, \ldots, a_m$ d'éléments de $A$, on pose :

$$a_0 + a_1 + \cdots + a_m = \sum_{k=0}^{m} a_k \text{ et } a_0 \times a_1 \times \cdots \times a_m = \prod_{k=0}^{m} a_k.$$

En particulier, on note $m.a = \underbrace{a+\cdots+a}_{m \text{ fois}}$ et $a^m = \underbrace{a\times\cdots\times a}_{m \text{ fois}}$.
On vérifie par récurrence sur $m$ que :

$$b\times\left(\sum_{k=0}^{m} a_k\right) = \sum_{k=0}^{m} b.a_k \text{ et } \left(\sum_{k=0}^{m} a_k\right)\times b = \sum_{k=0}^{m} a_k \times b.$$

On en déduit que

$$\left(\sum_{j=0}^{m} a_j\right)\times\left(\sum_{k=0}^{n} b_k\right) = \sum_{j=0}^{m}\left(a_j \sum_{k=0}^{n} b_k\right) = \sum_{j=0}^{m}\sum_{k=0}^{n} a_j \times b_k.$$

**Proposition 14.19.— Identité géométrique**
Soit $(A,+,\times)$ un anneau, $a$ et $b$ deux éléments de $A$ qui commutent, c'est-à-dire $a\times b = b\times a$, alors :

$$\forall n\in\mathbf{N},\quad a^{n+1}-b^{n+1}=(a-b)\times\sum_{k=0}^{n}a^{n-k}\times b^{k}.$$

**Démonstration** ▽
Soit $n\in\mathbf{N}$. Comme $a$ et $b$ commutent, nous pouvons écrire :

$$\begin{aligned}(a-b)\times\sum_{k=0}^{n}a^{n-k}\times b^{k} &= \sum_{k=0}^{n}\big[\underbrace{a^{n+1-k}b^{k}}_{u_k}-\underbrace{a^{n-k}b^{k+1}}_{u_{k+1}}\big]\\ &= \sum_{k=0}^{n}\big[u_k-u_{k+1}\big]\end{aligned}$$

Le résultat en découle par *télescopage*. ▲

En particulier, comme $1_A$ commute avec tout élément $a\in A$,

**Corollaire 14.20.—** Soit $(A,+,\times)$ un anneau, alors

$$\forall a\in A,\ \forall n\in\mathbf{N}^{\star}\quad 1_A-a^n=(1_A-a)\times\sum_{k=0}^{n-1}a^k=(1_A-a)\times(1_A+a+a^2+\cdots+a^{n-1}).$$

En particulier, si $(1_A-a)$ est inversible,

$$(1_A+a+a^2+\cdots+a^{n-1})=(1_A-a^n)\times(1_A-a)^{-1}.$$

**Proposition 14.21.— Formule du binôme dans un anneau**
Soit $(A,+,.)$ un anneau, $a$ et $b$ deux éléments de $A$ qui commutent, c'est-à-dire $a.b=b.a$, alors :

$$\forall n\in\mathbf{N},\quad (a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}.$$

**Démonstration** ▽
Il suffit de recopier la preuve donnée dans $\mathbf{R}$. On fera particulièrement attention à l'endroit où intervient l'hypothèse de commutativité de $a$ et $b$. ▲

## 2 Éléments remarquables dans un anneau

### 2.a Éléments inversibles

Comme nous l'avons déjà remarqué, dans un anneau tous les éléments ne sont par inversibles, par exemple dans l'anneau $\mathbf{R}^{\mathbf{R}}$ des fonctions de $\mathbf{R}$ dans $\mathbf{R}$ les éléments inversibles sont simplement les fonctions qui ne prennent jamais la valeur 0. L'inverse d'une telle fonction est $1/f$ bien sûr !

**Proposition 14.22.—** Soit $(A,+,\times)$ un anneau, on note $A^{\times}$ l'ensemble des éléments inversibles de $A$. Alors

$(A^{\times},\times)$ est un groupe.

**Exemples :**

- $\mathbf{Z}^{\times}=\{-1,+1\}$.

- $\mathbf{R}^\times = \mathbf{R}^\star$.

**Démonstration** ▽

- On sait déjà que la loi $\times$ est une loi de composition interne dans $A^\times$ car le produit de deux éléments inversibles de $A$ est aussi inversible.
- De plus, $\times$ est associative dans $A$ *A fortiori*, $\times$ est associative dans $A^\times$.
- de même, $\times$ possède un élément neutre : $1_A$. Cet élément est inversible et il s'agit d'un élément neutre dans $A^\times$.
- Finalement, montrons que tout élément de $A^\times$ possède un inverse dans $A^\times$.
  Soit donc $a \in A^\times$, alors $a \times a^{-1} = a^{-1} \times a = 1_A$, ce qui prouve que $a^{-1}$ est inversible et $\left(a^{-1}\right)^{-1} = a$.

▲

### 2.b Diviseurs de zéro

Dans un anneau comme dans $\mathbf{Z}$, si $b = 0$ ou $a = 0$, alors $a.b = 0$. La réciproque est fausse dans un anneau quelconque comme le montre le contre-exemple suivant :
Soit $A$ l'anneau des fonctions de $\mathbf{R}$ dans $\mathbf{R}$. Soient $a$ la fonction définie par $\forall x \in \mathbf{R}$, $a(x) = x + |x|$, et $b$ la fonction définie par $b(x) = x - |x|$. Il est clair que ni $a$ ni $b$ ne sont nuls ( c'est-à-dire constamment égale à zéro). Pourtant le produit $a \times b$ est nul ! !

**Définition :** *Soit $(A, +, \times)$ un anneau non réduit à $\{0_A\}$. Soit $a \in A \setminus \{0_A\}$. On dit que $a$ est un **diviseur de zéro** s'il existe $b \in A \setminus \{0_A\}$, tel que $a \times b = 0_A$.*

**Remarque :** Un diviseur de zéro est non-inversible.

Ceci conduit à poser la définition suivante :

**Définition :** *Soit $(A, +, \times)$ un anneau non réduit à $\{0_A\}$. On dit que $A$ est **intègre** s'il n'a pas de diviseurs de zéro. Autrement dit, $A$ est intègre si :*

$$\forall (a, b) \in A \times A, \quad a \times b = 0 \Rightarrow (a = 0) \text{ ou } (b = 0).$$

**Exercice :** L'anneau $(\mathbf{C}^\mathbf{N}, +, \times)$ des suites de nombres complexes est-il intègre ?

### 2.c Éléments nilpotents et idempotents

**Définition :** *Un élément $a \in A$ est dit **idempotent** si $a^2 = a$.*

**Exemple :** Dans un anneau intègre, seuls 0 et 1 sont idempotents.

**Définition :** *Un élément $a \in A$ est dit **nilpotent** s'il existe $n \in \mathbf{N}^\star$ tel que $a^n = 0_A$.*

**Exemple :** Dans un anneau intègre, seul 0 est nilpotent.

**Exercice :** Soit $(A, +, \times)$ un anneau vérifiant la propriété universelle $\forall x \in A,\ x^2 = x$.

**1.** Montrez que $\forall x \in A,\ 2.x = 0$

**2.** Montrez que $A$ est commutatif.

**Exercice :** Soit $(A, +, \times)$ un anneau. Montrez que si $a \in A$ est nilpotent, alors $1_A - a$ est inversible.

*Solution* ▽
*Soit $n \in \mathbf{N}^\star$ tel que $a^n = 0_A$. Comme $1_A$ et $a$ commutent, l'***identité géométrique** *s'applique. Il en découle que*

$$\begin{aligned} 1_A &= 1_A - a^n = (1_A - a) \times \sum_{k=0}^{n-1} a^k \\ &= \sum_{k=0}^{n-1} a^k \times (1_A - a) \end{aligned}$$

*Ainsi, $1_A - a$ est inversible et $(1_A - a)^{-1} = \sum_{k=0}^{n-1} a^k$.* ▲

## 3 Sous-anneau

**Définition :** *Soit $(A,+,\times)$ un anneau et $B$ une partie de $A$. On dit que $B$ est un* ***sous-anneau*** *de $(A,+,\times)$ si :*

1. $1_A \in B$,
2. $\forall (a,b) \in B \times B, a+b \in B$ *(stabilité pour la loi $+$)*
3. $\forall (a,b) \in B \times B, a \times b \in B$ *(stabilité pour la loi .)*
4. *muni de ces lois de composition interne, $(B,+,\times)$ est un anneau.*

**Théorème 14.23.— Caractérisation des sous-anneaux —.** Soit $(A,+,\times)$ un anneau et $B$ une partie de $A$. Alors

$B$ est un sous-anneau de $A$ *si et seulement si*
- $(SA1)$ $1_A \in B$
- $(SA2)$ $\forall (a,b) \in B \times B,\ a-b \in B$ .
- $(SA3)$ $\forall (a,b) \in B \times B,\ a \times b \in B$

**En pratique :** Pour démontrer qu'une partie $B$ de $A$ est un sous-anneau, vous utilisez systématiquement la caractérisation.

**Exercice : Anneau des entiers de Gauss —.** On note $\mathbf{Z}[i] = \{a + i\,b\,;\ (a,b) \in \mathbf{Z}^2\}$.

1. Montrez que $\mathbf{Z}[i]$ est un sous-anneau de $\mathbf{C}$.
2. Montrez que les seuls éléments inversibles de $\mathbf{Z}[i]$ sont $1$,$-1$, $i$ et $-i$.

*Solution* $\triangledown$

1. *Pour démontrer que $\mathbf{Z}[i]$ est un sous-anneau de $\mathbf{C}$, nous utilisons la* **caractérisation des sous-anneaux**
   - $1 = 1 + i0 \in \mathbf{Z}[i]$.
   - ■*Soit $z = a+ib$ et $z' = a'+ib'$ deux éléments de $\mathbf{Z}[i]$ (i.e. $a,a',b,b' \in \mathbf{Z}$). Alors*

$$\begin{aligned} z - z' &= (a+ib) - (a'+ib') = (a-a') + i(b-b') \in \mathbf{Z}[i] \\ z \times z' &= (a+ib) \times (a'+ib') = (aa'-bb') + i(ab'+a'b) \in \mathbf{Z}[i] \end{aligned}$$

2. *Pour déterminer l'ensemble des éléments inversibles de $\mathbf{Z}[i]$, procédons par analyse-synthèse :*
   - **Analyse :** *soit $z = a+ib \in \mathbf{Z}[i]$ un élément inversible. Il existe donc $w = c+id \in \mathbf{Z}[i]$ tel que*

$$(a+ib) \times (c+id) = 1$$

*En prenant les modules au carré des deux membres de cette égalité, il vient*

$$(a^2+b^2) \times (c^2+d^2) = 1$$

*Comme les deux facteurs ci-dessus sont des entiers naturels, il en résulte que nécessairement, $a^2+b^2 = 1$, ce qui revient à dire que*

   - ▶ *soit $a^2 = 1$ et $b = 0$, et dans ce cas $z = \pm 1$*
   - ▶ *soit $a = 0$ et $b^2 = 1$, et dans ce cas, $z = \pm i$.*

*Finalement $\left(\mathbf{Z}[i]\right)^\times \subset \{\pm 1, \pm i\}$.*

   - **Synthèse :** *on vérifie aisément que $1, -1, i$ et $-i$ sont inversibles.*
   - **Conclusion :** *le groupe des éléments inversibles de $\mathbf{Z}[i]$ est*

$$\left(\mathbf{Z}[i]\right)^\times = \{\pm 1, \pm i\}$$

▲

## 4 Morphismes d'anneaux

**Définition :** *Soient $(A,+,\times)$ et $(A',\perp,\star)$ deux anneaux. On appelle* ***morphisme d'anneaux*** *toute application $f : A \to A'$ telle que :*

- $\forall (x,y) \in A \times A, \quad f(x+y) = f(x) \perp f(y).$
- $\forall (x,y) \in A \times A, \quad f(x \times y) = f(x) \star f(y).$
- $f(1_A) = 1_{A'}$

**Commentaires :** en clair, un morphisme d'anneaux est une application entre deux anneaux, compatible avec leurs structures algébriques respectives. En particulier, un morphisme d'anneaux est un morphisme de groupes de $(A,+)$ dans $(A',\perp)$

**Exemple :** l'application $z \mapsto \bar{z}$ est un (auto-)morphisme de $(\mathbf{C},+,\times)$ dans lui-même.

**Exercice : Eléments inversibles de $\mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2};\ (a,b) \in \mathbf{Z}^2\}$.**

**1.** Soit $\mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2};\ (a,b) \in \mathbf{Z}^2\}$. Montrez que $\mathbf{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbf{R}$.

**2.** On considère l'application $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}[\sqrt{2}]$ définie par

$$\forall (a,b) \in \mathbf{Z}^2, \quad \varphi(a+b\sqrt{2}) = a - b\sqrt{2}$$

Montrez que $\varphi$ est un automorphisme de $\mathbf{Z}[\sqrt{2}]$.

**3.** Pour tout $x \in \mathbf{Z}[\sqrt{2}]$, on pose $N(x) = x\,\varphi(x)$. Montrez que $N$ est un morphisme multiplicatif de $\mathbf{Z}[\sqrt{2}]$ dans $\mathbf{Z}$.

**4.** En déduire qu'un élément $x \in \mathbf{Z}[\sqrt{2}]$ est inversible *si et seulement si* $N(x) = \pm 1$. Donnez des exemples d'éléments inversibles de $\mathbf{Z}[\sqrt{2}]$.

## 5 Corps

**Définition :** *Soit $\mathbf{K}$ un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $(\mathbf{K},+,\times)$ est un corps si*

**1.** *$(\mathbf{K},+,\times)$ est un anneau commutatif non réduit à $\{0\}$,*

**2.** *$\mathbf{K}^\times = \mathbf{K} \setminus \{0\}$, c'est-à-dire que tout élément non nul est inversible.*

**Exemples :** $(\mathbf{Q},+,\times)$, $(\mathbf{R},+,\times)$, $(\mathbf{C},+,\times)$ sont des corps, $(\mathbf{Z},+,\times)$ n'est pas un corps.

**Notation :** *comme d'habitude, on note $\mathbf{K} \setminus \{0\} = \mathbf{K}^\star$.*

**Remarque :** Comme un diviseur de zéro est non nul et non-inversible, dans un corps il n'y a pas de diviseurs de zéro. Autrement dit tout corps est un anneau intègre.

**Définition :** *On appelle* ***sous-corps*** *d'un corps $(\mathbf{K},+,\times)$ toute partie $\mathbf{L}$ de $\mathbf{K}$, stable par $+$ et $\times$ qui, munie des lois induites par $+$ et $\times$ est un corps.*

**Proposition 14.24.— Caractérisation des sous-corps —.** Soit $(\mathbf{K},+,\times)$ un corps et $\mathbf{L}$ une partie de $\mathbf{K}$, non réduite à $\{0\}$.

$\mathbf{L}$ est un sous-corps de $\mathbf{K}$ *si et seulement si*
- $(SC1)$ $\quad 1_{\mathbf{K}} \in \mathbf{L}$
- $(SC2)$ $\quad \forall (x,y) \in \mathbf{L} \times \mathbf{L},\ x - y \in \mathbf{L}$
- $(SC3)$ $\quad \forall (x,y) \in \mathbf{L} \times \mathbf{L}^\star,\ x \times y^{-1} \in \mathbf{L}$

.

**Exercice :** Soit $\mathbf{K}$ et $\mathbf{K}'$ deux corps et $\varphi : \mathbf{K} \to \mathbf{K}'$ un morphisme d'anneaux. Montrez que

**1.** $\varphi$ est injectif.

**2.** $\forall x \in \mathbf{K}^\star,\ \varphi(x^{-1}) = \big(\varphi(x)\big)^{-1}$.

# IV Étude du groupe symétrique

Les résultats de cette section seront particulièrement utile lors de notre étude des déterminants au troisième trimestre.

## 1 Structure de $\mathfrak{S}_n$

### 1.a Définition du groupe symétrique d'ordre $n$

**Définition :** *Soit $n \in \mathbf{N}^\star$, on note $\mathfrak{S}_n$ l'ensemble des permutations de $[\![1, n]\!]$.*

Comme nous l'avons vu au **Chapitre 11**, $\mathfrak{S}_n$ est un ensemble fini de cardinal $n!$, de plus :

**Proposition 14.25.—** Soit $n \in \mathbf{N}^\star$, $(\mathfrak{S}_n, \circ)$ est un groupe pour la composition des applications, appelé **groupe symétrique**. L'élément neutre est l'application identité.

**Démonstration** ▽

- la loi $\circ$ est une loi de composition interne de $\mathfrak{S}_n$ car la composée de deux bijections est une bijection.
- la loi $\circ$ est associative
- la loi $\circ$ possède $id$ comme élément neutre
- toute permutation $\sigma$ de $[\![1, n]\!]$ admet pour inverse son application réciproque. ▲

### 1.b Représentation des permutations

Comme nous l'avons vu dans l'**Exemple introductif**, une permutation $\sigma : [\![1, n]\!] \to [\![1, n]\!]$ peut être représentée de la façon suivante :

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

**Exemple :** Dans $\mathfrak{S}_5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$, représente la permutation définie par

$$\sigma(1) = 5, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 2, \sigma(5) = 1.$$

**En pratique :** Cette notation est particulièrement utile pour déterminer la composée de deux permutations :

**Exercice :** Dans $\mathfrak{S}_9$ déterminez la composée $\sigma_2 \circ \sigma_1$, lorsque

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 7 & 8 & 3 & 1 & 4 & 6 & 9 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 9 & 7 & 3 & 4 & 1 & 6 & 8 \end{pmatrix}$$

*Solution* ▽

*On peut présenter le calcul de $\sigma_2 \circ \sigma_1$, sur plusieurs lignes :*

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 7 & 8 & 3 & 1 & 4 & 6 & 9 \\ 3 & 2 & 1 & 6 & 9 & 5 & 7 & 4 & 8 \end{array}$$

▲

### 1.c Pour $n \geq 3$, $\mathfrak{S}_n$ est non commutatif

Lorsque $n = 1$, $\mathfrak{S}_1$ est réduit à l'identité, il est donc commutatif!! Lorsque $n = 2$ $\mathfrak{S}_2$ contient l'identité et la *transposition* $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ : $\mathfrak{S}_2 = \{id, \tau\}$ est donc aussi abélien. Ce n'est plus le cas, dès que $n$ est supérieur à 3 :

**Proposition 14.26.—** Soit $n \geq 3$, $\mathfrak{S}_n$ n'est pas commutatif.

**Démonstration** ▽

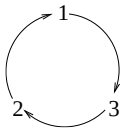
Soient $\sigma_1$ et $\sigma_2$ les permutations de $[\![1, n]\!]$ définies par

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}$$

Alors $\sigma_1 \circ \sigma_2(1) = 2$, tandis que $\sigma_2 \circ \sigma_1(1) = 3$. En particulier, $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$. ▲

### 1.d Cycles et transpositions

Considérons la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. L'action de $\sigma$ peut être aisément visualisée dans le schéma ci-contre.




On dit que $\sigma$ est une *permutation circulaire*, ou encore un *cycle*. Plus généralement,

**Définition :** *Soit $(n,p) \in \mathbf{N}^2$ tel que $2 \leq p \leq n$. Soit $S = \{a_1, \ldots, a_p\}$ une partie de $[\![1,n]\!]$ à $p$ éléments. On définit la permutation $c \in \mathfrak{S}_n$ par*

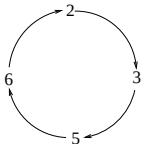
$$\boxed{c(a_1) = a_2, c(a_2) = a_3, \ldots, c(a_p) = a_1, \text{ et pour tout } k \notin S,\ c(k) = k}$$

*$c$ est appelé un **cycle de longueur** $p$, et $S = \{a_1, \ldots, a_p\}$ est le **support** de $c$.*

**Notation :** *On note simplement $c = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix}$.*

**Exemple :** dans $\mathfrak{S}_6$

- $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 6 & 2 \end{pmatrix}$ est un cycle de longueur 4. On peut le représenter par le schéma ci-contre :
- $c = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 \end{pmatrix}$ est un cycle de longueur 5 : $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 1 & 5 & 4 \end{pmatrix}$




**Remarques :** soit $c = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix}$ un $p$-cycle de $\mathfrak{S}_n$.

**1.** cette notation de $c$ n'est pas unique, par exemple $c = \begin{pmatrix} a_2 & a_3 & \cdots & a_p & a_1 \end{pmatrix}$ !

**2.** l'inverse de $c$ est donné par $c^{-1} = \begin{pmatrix} a_p & \cdots & a_3 & a_2 & a_1 \end{pmatrix}$

**3.** deux cycles de supports disjoints commutent.

**Définition :** *Soit $n \in \mathbf{N}^\star$, on appelle **transposition** de $\mathfrak{S}_n$ tout cycle de longueur 2.*

**Notation :** *On note aussi $\tau_{i,j}$ la transposition $(i\ j)$.*

**Remarque :** la transposition $\tau = (i\ j)$ échange $i$ et $j$. En particulier $\tau_{i,j} = \tau_{j,i}$ et elle vérifie la fameuse identité canadienne $\tau \circ \tau = id$.

## 2 Décomposition d'une permutation en produit de transpositions

### 2.a Décomposition d'un cycle

Soit $c = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix}$ un $p$ cycle de $\mathfrak{S}_n$, alors

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix} = \begin{pmatrix} a_2 & a_3 & \cdots & a_p \end{pmatrix}$$

En itérant ce procédé, on obtient l'égalité suivante :

$$\begin{pmatrix} a_{p-1} & a_p \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix} = id$$

En composant à gauche par $\begin{pmatrix} a_p & a_{p-1} \end{pmatrix}$, …, $\begin{pmatrix} a_1 & a_2 \end{pmatrix}$, on en déduit :

**Lemme 14.27.—** Soit $c = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix}$ un $p$ cycle de $\mathfrak{S}_n$, alors

$$\boxed{\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}}$$

### 2.b Cas général

**Théorème 14.28.—** Soit $n \in \mathbf{N}^\star$.
Toute permutation $\sigma$ de $\mathfrak{S}_n$ est décomposable en un produit d'au plus $n-1$ transpositions.

**Démonstration** $\triangledown$
la démonstration sera par récurrence sur $n \in \mathbf{N}^\star$.

- **Initialisation :** lorsque $n = 1, 2$, il n'y a rien a faire !
- **Hérédité :** soit $n \geq 1$ tel que toute permutation de $[\![1, n]\!]$ se décompose en un produit d'au plus $n-1$ transpositions. Soit $\sigma \in \mathfrak{S}_{n+1}$ une permutation de $[\![1, n+1]\!]$. Deux cas se présentent :

  ⌣ **Lucky** si $\sigma(n+1) = n+1$.
  En ce cas, la restriction de $\sigma$ à $[\![1, n]\!]$ est une permutation de $[\![1, n]\!]$. Par hypothèse de récurrence, elle s'écrit comme composée d'au plus $n-1$ transpositions. Comme $\sigma$ laisse $n+1$ invariant, il s'agit en fait d'une décomposition de $\sigma$.

  ⌢ **Unlucky** si $\sigma(n+1) = a \in [\![1, n]\!]$.
  En ce cas, considérons $\sigma' = (n+1\ a) \circ \sigma$. On vérifie immédiatement que $\sigma'$ est une permutation qui laisse $n+1$ invariant. D'après le **Lucky case**, $\sigma'$ s'exprime comme la composée d'au plus $n-1$ transpositions. En composant à gauche par $(n+1\ a)$, on en déduit que $\sigma$ s'écrit comme le produit d'au plus $n$ transpositions.

  Dans tous les cas, $\sigma$ est décomposable en un produit d'au plus $n$ transpositions.
- **Conclusion :** Par récurrence, nous avons prouvé que toute permutation de $[\![1, n]\!]$ se décompose en un produit d'au plus $n-1$ transpositions. ▲

**En pratique :** Cette démonstration est constructive : elle fournit un algorithme permettant de décomposer une permutation en produit de transpositions.

### 2.c Mise en œuvre

Soit $\sigma$ la permutation de $\mathfrak{S}_8$ définie par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 7 & 4 & 8 & 1 & 5 & 2 \end{pmatrix}$ On remet les éléments $1, 2, \ldots, n$ dans l'ordre à l'aide de transpositions :

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \\ 6 & 3 & 7 & 4 & \mathbf{8} & 1 & 5 & \mathbf{2} & \circlearrowleft \sigma \\ 6 & 3 & \mathbf{7} & 4 & 2 & 1 & \mathbf{5} & 8 & \circlearrowleft \tau_{2,8} \\ \mathbf{6} & 3 & 5 & 4 & 2 & \mathbf{1} & 7 & 8 & \circlearrowleft \tau_{5,7} \\ 1 & 3 & \mathbf{5} & 4 & \mathbf{2} & 6 & 7 & 8 & \circlearrowleft \tau_{1,6} \\ 1 & \mathbf{3} & \mathbf{2} & 4 & 5 & 6 & 7 & 8 & \circlearrowleft \tau_{2,5} \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \circlearrowleft \tau_{2,3} \end{array}$$

Ainsi, $\tau_{2,3} \circ \tau_{2,5} \circ \tau_{1,6} \circ \tau_{5,7} \circ \tau_{2,8} \circ \sigma = id$. Par conséquent

$$\sigma = \tau_{2,8} \circ \tau_{5,7} \circ \tau_{1,6} \circ \tau_{2,5} \circ \tau_{2,3}$$

**Exercice :** Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 7 & 5 & 2 & 1 & 8 & 6 \end{pmatrix}$

**1.** Décomposez $\sigma$ en produits de cycles à supports disjoints.

**2.** Décomposez $\sigma$ en produits de transpositions.

## 3 Signature d'une permutation

### 3.a Nombre d'inversions d'une permutation

**Définition :** *Soit $\sigma \in \mathfrak{S}_n$ une permutation et $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$. On dit que $\sigma$ réalise une inversion sur le couple $(i, j)$ –ou plus simplement que $\sigma$ inverse $i$ et $j$– si $\sigma(i) > \sigma(j)$.*

**Notation :** *On note $I(\sigma)$ le nombre d'inversions de $\sigma$, i.e. le nombre de couples $(i,j) \in [\![1,n]\!]^2$ tels que $i<j$ et $\sigma(i)>\sigma(j)$.*

**Exemple :** Calculons le nombre d'inversions de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

- le couple $(1,4)$ est inversé,
- les couples $(2,3)$ et $(2,4)$ sont inversés,
- le couple $(3,4)$ est inversé.

Par suite $I(\sigma) = 4$.

**En pratique :** pour calculer le nombre d'inversions, vous ajoutez, pour chaque terme de la deuxième ligne, le nombre de valeurs à sa droite qui lui sont strictement inférieures.

**Exercice :** Déterminez le nombre d'inversions de la permutation : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 4 & 1 & 5 & 6 & 2 & 9 & 7 \end{pmatrix}$

*Solution* ▽
$I(\sigma) = 2+6+2+1+1+1 = 13$. ▲

### 3.b Signature d'une permutation

**Définition :** *Soit $n \in \mathbf{N}^\star$, $\sigma \in \mathfrak{S}_n$. On appelle* ***signature*** *de $\sigma$ le nombre réel $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.*

**Remarque :** $\varepsilon(\sigma) \in \{-1,1\}$. Son signe dépend de la parité de $I(\sigma)$

**Exemples :** dans $\mathfrak{S}_n$

- comme l'identité ne réalise aucune inversion, $\varepsilon(id) = 1$.
- la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & n-1 & n-2 & \cdots & 1 \end{pmatrix}$ vérifie $I(\sigma) = n-1+n-2+\cdots+1 = \dfrac{n(n-1)}{2}$ et par conséquent $\varepsilon(\sigma) = (-1)^{\frac{n(n-1)}{2}}$.

**Proposition 14.29.—** Soit $n \in \mathbf{N}^\star$ et $\tau \in \mathfrak{S}_n$ une transposition. Alors

$$\boxed{\varepsilon(\tau) = -1}$$

**Démonstration** ▽
Soient $n \in \mathbf{N}$, $n \geq 2$, et $(i,j) \in [\![1,n]\!]^2$ tel que $i<j$. Montrons que le nombre d'inversions de la transposition $\tau = (i\ \ j)$ est $2(j-i)-1$

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & j-1 & j & \cdots & n \\ 1 & 2 & \cdots & j & i+1 & \cdots & j-1 & i & \cdots & n \end{pmatrix}$$

Par conséquent $I(\tau) = 0+0+\cdots+(j-i)+\underbrace{1+\cdots+1}_{j-i-1 \text{ fois}}+0+\cdots+0 = 2(j-i)-1$.

Ainsi $\varepsilon(\tau) = (-1)^{2(j-i)-1} = -1$. ▲

### 3.c Propriété fondamentale de la signature

**Lemme 14.30.—** Soit $n \in \mathbf{N}^\star$, pour toute permutation $\sigma \in \mathfrak{S}_n$,

$$\boxed{\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,j\} \in \mathscr{P}_2(\mathbb{F}_n)} \frac{\sigma(j)-\sigma(i)}{j-i}}$$

**Démonstration** ▽
Soit $\sigma \in \mathfrak{S}_n$. La démonstration sera en trois étapes :

- Notons $P = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$. On montre que $P = \prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)} \frac{\sigma(j)-\sigma(i)}{j-i}$.
  Comme nous l'avons vu au **Chapitre 11**, l'ensemble des 2-listes strictement croissantes d'entiers entre 1 et $n$ est en bijection avec l'ensemble des paires d'éléments de $[\![1,n]\!]$. En clair, l'application

$$\begin{array}{rccl}\Phi\ : & \{(i,j)\in[\![1,n]\!]^2 \mid 1\leq i<j\leq n & \to & \mathscr{P}_2(\mathbb{F}_n)\\ & (i,j) & \mapsto & \{i,j\}\end{array}$$

  est bijective. De plus, pour chaque couple $(i,j)$ d'entiers vérifiant $1\leq i<j\leq n$, on a

$$\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(i)-\sigma(j)}{i-j}$$

  Par conséquent, ce facteur ne dépend que de la paire $\{i,j\}$, et non du couple. Par conséquent, on a bien

$$\prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)} \frac{\sigma(j)-\sigma(i)}{j-i}$$

- Calculons la valeur absolue de $P$ :
  La permutation $\sigma:\mathbb{F}_n\to\mathbb{F}_n$ étant bijective, l'application

$$\begin{array}{rccl}\Psi\ : & \mathscr{P}_2(\mathbb{F}_n) & \to & \mathscr{P}_2(\mathbb{F}_n)\\ & \{i,j\} & \mapsto & \{\sigma(i),\sigma(j)\}\end{array}$$

  l'est aussi. Par conséquent, le changement d'indice $k=\sigma(i), \ell=\sigma(j)$ donne :

$$\prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)} \big|\sigma(i)-\sigma(j)\big| = \prod_{\{k,\ell\}\in\mathscr{P}_2(\mathbb{F}_n)} \big|k-\ell\big|$$

  En utilisant la deuxième expression pour $P$, il s'ensuit que $|P|=1$.

- Finalement, intéressons-nous au signe de $P$ :
  Pour ce faire, on utilise la première expression de $P$. On observe alors que pour tout couple $(i,j)$ tel que $1\leq i<j\leq n$, on a
  - si $\sigma$ inverse le couple $(i,j)$, alors $SGN\left(\frac{\sigma(j)-\sigma(i)}{j-i}\right) = -1$,
  - sinon $SGN\left(\frac{\sigma(j)-\sigma(i)}{j-i}\right) = +1$

  Ainsi,

$$SGN\left(\prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}\right) = 1\times SGN\left(\prod_{\substack{1\leq i<j\leq n\\ (i,j)\text{inversé}}} \frac{\sigma(j)-\sigma(i)}{j-i}\right) = (-1)^{I(\sigma)}$$

- .Finalement le produit $P$ étant de valeur absolue 1 et de signe $(-1)^{I(\sigma)}$, il s'ensuit que

$$P = \varepsilon(\sigma)$$

▲

**Théorème 14.31.—** L'application $\varepsilon:\mathfrak{S}_n\to\{-1,1\}$ est un morphisme du groupe $(\mathfrak{S}_n,\circ)$ dans le groupe multiplicatif $\big(\{\pm1\},\times\big)$. Autrement dit,

$$\boxed{\forall(\sigma,\rho)\in\mathfrak{S}_n^2,\quad \varepsilon\big(\sigma\circ\rho\big)=\varepsilon\big(\sigma\big)\times\varepsilon\big(\rho\big)}$$

**Démonstration** ▽
Soit $(\sigma,\rho)\in\mathfrak{S}_n^2$. Alors

$$\begin{aligned}\varepsilon\big(\sigma\circ\rho\big) &= \prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma\circ\rho(j)-\sigma\circ\rho(i)}{j-i}\\ &= \prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma\circ\rho(j)-\sigma\circ\rho(i)}{\rho(j)-\rho(i)}\times\frac{\rho(j)-\rho(i)}{j-i}\\ &= \prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma\circ\rho(j)-\sigma\circ\rho(i)}{\rho(j)-\rho(i)}\times\prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\rho(j)-\rho(i)}{j-i}\\ &= \varepsilon(\rho)\times\prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma\circ\rho(j)-\sigma\circ\rho(i)}{\rho(j)-\rho(i)}\end{aligned}$$

Comme $\rho$ est bijective, l'application $\begin{array}{ccc}\mathscr{P}_2(\mathbb{F}_n) & \to & \mathscr{P}_2(\mathbb{F}_n)\\ \{i,j\} & \mapsto & \{\rho(i),\rho(j)\}\end{array}$ l'est aussi. Par conséquent, le changement d'indice $k=\rho(i),\ell=\rho(j)$ donne

$$\prod_{\{i,j\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma\circ\rho(j)-\sigma\circ\rho(i)}{\rho(j)-\rho(i)}=\prod_{\{k,\ell\}\in\mathscr{P}_2(\mathbb{F}_n)}\frac{\sigma(\ell)-\sigma(k)}{\ell-k}=\varepsilon(\sigma)$$

Il en résulte que $\varepsilon(\sigma\circ\rho)=\varepsilon(\sigma)\times\varepsilon(\rho)$. ▲

**Remarque :** cette propriété se généralise : la signature d'une composée est le produit des signatures.

$$\varepsilon(\sigma_1\circ\cdots\circ\sigma_p)=\varepsilon(\sigma_1)\times\cdots\times\varepsilon(\sigma_p)$$

**Corollaire 14.32.—** Soit $c$ un $p$ cycle de $\mathfrak{S}_n$. Alors $\varepsilon(c)=(-1)^{p-1}$.

**Démonstration** ▽
Si $c=\big(a_1\quad a_2\quad\cdots\quad a_p\big)$, nous savons décomposer $c$ en produit de $p-1$ transpositions :

$$c=\big(a_1\quad a_2\big)\circ\big(a_2\quad a_3\big)\circ\cdots\circ\big(a_{p-1}\quad a_p\big)$$

Comme la signature est un morphisme de groupes, il s'ensuit que

$$\varepsilon(c)=\prod_{i=1}^{p-1}\varepsilon\big(\tau_{a_i,a_{i+1}}\big)=(-1)^{p-1}$$

▲

**En pratique :** pour calculer la signature d'une permutation, vous pouvez

- déterminer son nombre d'inversions
- la décomposer en produit de transpositions
- la décomposer en produit de cycles à supports disjoints

### 3.d Parité d'une permutation

Comme $\varepsilon:\mathfrak{S}_n\to\{-1,1\}$, une permutation a une signature égale à 1 ou à $-1$.

**Définition :** *Soit $n\in\mathbf{N}^\star$. Une permutation $\sigma\in\mathfrak{S}_n$ est dite*

- ***paire*** *si sa signature est 1,*
- ***impaire*** *si sa signature est $-1$.*

**Exemples :** l'identité est une permutation paire, toute transposition est impaire.

**Notation :** *On note $\mathfrak{A}_n$ l'ensemble des permutations paires de $\mathfrak{S}_n$.*

**Exemples :**

- si $n=1$, $\mathfrak{A}_1=\{id\}$

- si $n = 2$, $\mathfrak{A}_2 = \{id\}$
- si $n = 3$, $\mathfrak{A}_2 = \{id, (1\ 2\ 3), (1\ 3\ 2)\}$.

**Proposition 14.33.—** Soit $n \in \mathbf{N}^\star$. $\Big(\mathfrak{A}_n, \circ\Big)$ est un sous-groupe de $\Big(\mathfrak{S}_n, \circ\Big)$.

**Vocabulaire :** $\Big(\mathfrak{A}_n, \circ\Big)$ *est appelé* ***groupe alterné*** *d'orde* $n$.

**Démonstration** ▽
$\mathfrak{A}_n$ est le noyau de la signature. ▲