

## Structures algébriques d'anneau et de corps

## 1 Structure d'anneau

### 1 Définition

#### Définition 1

Soit  $A$  un ensemble,  $+$ ,  $\times$  deux lois de composition internes sur  $A$ . On dit que  $(A, +, \times)$  est un **anneau** lorsque

- $(A, +)$  est un groupe abélien. L'élément neutre est noté  $0_A$ .
- $\times$  est associative et distributive sur  $+$ .
- $\times$  admet un élément neutre appelé unité de  $A$ , noté  $1_A$ .

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

#### Propriété 1

$(\mathbb{Z}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{C}, +, \times)$ ,  $(\mathbb{R}^D, +, \times)$ ,  $(\mathbb{C}^D, +, \times)$  (avec  $D \neq \emptyset$ ) sont des anneaux commutatifs.

### 2 Diviseurs de zéro et intégrité

#### Définition 2 : Diviseur de zéro

Soit  $(A, +, \times)$  un anneau. Un élément  $a \in A$  est appelé **diviseur de zéro** si

- $a \neq 0_A$ .
- On peut trouver  $b \in A$  tel que  $b \neq 0_A$  et  $a \times b = 0_A$ .

#### Définition 3 : Anneau intègre

Un anneau  $(A, +, \times)$  est dit **intègre** si

- $A$  est commutatif,
- $A \neq \{0_A\}$  c'est-à-dire  $1_A \neq 0_A$ ,
- $A$  n'admet aucun diviseur de zéro, c'est-à-dire

$$\forall a, b \in A, a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A.$$

### 3 Règles de calcul dans un anneau

#### Propriété 2

Soit  $(A, +, \times)$  un anneau.

(i)  $0_A$  est **absorbant** :

$$\forall a \in A, a \times 0_A = 0_A \times a = 0_A.$$

(ii)  $\forall a, b \in A, (-a) \times b = a \times (-b) = -(a \times b)$ .

(iii) Si  $n, p \in \mathbb{Z}$  et  $a, b \in A$ ,

- $n(a \pm b) = na \pm nb$ ,
- $n(pa) = (np)b$ ,
- $n(ab) = (na)b = a(nb)$ ,
- $na = (n1_A)a = a(n1_A)$ .

#### Propriété 3

Soit  $(A, +, \times)$  un anneau. Si  $a, b \in A$  tels que  $a \times b = b \times a$  et  $n \in \mathbb{N}$ ; alors

- **Formule du binôme de Newton** :

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

- **Factorisation de  $a^n - b^n$**  :

$$\begin{aligned} a^n - b^n &= (a - b) (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}) \\ &= (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}. \end{aligned}$$

### 4 Groupe des inversibles

#### Définition 4

Soit  $(A, +, \times)$  un anneau.

$a \in A$  est dit **inversible** si et seulement s'il est symétrisable pour  $\times$ .

Son symétrique est appelé **inverse** de  $a$ , noté  $a^{-1}$ .

On note  $U_A$  ou  $U(A)$  ou  $A^\times$  l'ensemble des inversibles de  $A$ .

#### Propriété 4 : Groupe des inversibles

Si  $(A, +, \times)$ , alors  $(U_A, \times)$  est un groupe appelé **groupe des inversibles** de  $A$ .

### 5 Sous-anneau

#### Définition 5 : Sous-anneau

Soit  $(A, +, \times)$  un anneau. On dit que  $(B, +, \times)$  est un **sous-anneau** de  $(A, +, \times)$  lorsque  $B \subset A$ ,  $1_A \in B$  et  $(B, +|_{B^2}, \times|_{B^2})$  est un anneau.



**Propriété 5 : Caractérisation des sous-anneaux**

$(B, +, \times)$  est un sous-anneau de  $(A, +, \times)$  si et seulement si

$$\left\{ \begin{array}{l} B \subset A \\ (B, +) \text{ est un sous-groupe de } (A, +) \\ B \text{ est stable par } \times : \forall x, y \in B, x \times y \in B \\ 1_A \in B \end{array} \right.$$

ou, de manière équivalente,

$$\left\{ \begin{array}{l} B \subset A ; 1_A \in B \\ \forall x, y \in B, x + y \in B, -x \in B \text{ et } x \times y \in B \\ \text{ou } \forall x, y \in B, x - y \in B \text{ et } x \times y \in B \end{array} \right.$$

**6 Morphisme d'anneau**

**Définition 6 : Morphisme d'anneaux**

Soient  $(A, +, \times)$  et  $(A', \oplus, \otimes)$  deux anneaux.  $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$  est un **morphisme d'anneaux** si et seulement si

- (i)  $\forall (a, b) \in A^2, f(a + b) = f(a) \oplus f(b)$   
(ie  $f : (A, +) \rightarrow (A', \oplus)$  morphisme de groupes)
- (ii)  $\forall (a, b) \in A^2, f(a \times b) = f(a) \otimes f(b)$
- (iii)  $f(1_A) = 1_{A'}$

On parle aussi, d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux avec des définitions identiques.

**Propriété 6**

Si  $f : (A, +, \times) \rightarrow (A', \oplus, \otimes)$  est un morphisme d'anneaux et si  $a$  est inversible dans  $A$ , alors  $f(a)$  l'est dans  $A'$  et  $f(a^{-1}) = (f(a))^{-1}$ .

**II Structure de corps**

**1 Définition**

**Définition 7**

Soit  $\mathbb{K}$  un ensemble,  $+, \times$  deux lois de composition internes sur  $\mathbb{K}$ . On dit que  $(\mathbb{K}, +, \times)$  est un **corps** lorsque

- $(\mathbb{K}, +, \times)$  est un anneaux.
- $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$  est non vide et tous ses éléments sont inversibles (c'est-à-dire  $\mathbb{K} \neq \{0_{\mathbb{K}}\}$  et  $U_{\mathbb{K}} = \mathbb{K}^\times = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ .)
- $\times$  est commutative.

ou, de manière équivalente,

- $(\mathbb{K}, +)$  est un groupe abélien,
- $(\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times)$  est un groupe abélien,
- $\times$  est distributive sur  $+$ .

**Propriété 7**

Tout corps n'admet aucun diviseur de zéro. En particulier, tout corps est intègre. La réciproque est fausse.

**2 Sous-corps**

**Définition 8 : Sous-corps**

Soit  $(\mathbb{K}, +, \times)$  un corps. On dit que  $(\mathbb{L}, +, \times)$  est un sous-corps de  $(\mathbb{K}, +, \times)$  lorsque  $\mathbb{L} \subset \mathbb{K}$  et  $(\mathbb{L}, +|_{\mathbb{L}^2}, \times|_{\mathbb{L}^2})$  est un corps.

**Propriété 8 : Caractérisation des sous-corps**

$(\mathbb{L}, +, \times)$  est un sous-corps de  $(\mathbb{K}, +, \times)$  si et seulement si

$$\left\{ \begin{array}{l} \mathbb{L} \subset \mathbb{K} \\ (\mathbb{L}, +) \text{ est un sous-groupe de } (\mathbb{K}, +) \\ (\mathbb{L} \setminus \{0_{\mathbb{K}}\}, \times) \text{ est un sous-groupe de } (\mathbb{K} \setminus \{0_{\mathbb{K}}\}, \times) \end{array} \right.$$

ou, de manière équivalente,

$$\left\{ \begin{array}{l} \mathbb{L} \subset \mathbb{K} \\ \mathbb{L} \setminus \{0_{\mathbb{K}}\} \neq \emptyset \quad (1_{\mathbb{K}} \in \mathbb{L}) \\ \forall x, y \in \mathbb{L}, x - y \in \mathbb{L} \\ \forall x, y \in \mathbb{L} \setminus \{0_{\mathbb{K}}\}, xy^{-1} \in \mathbb{L} \end{array} \right.$$

**3 Morphismes de corps**

**Définition 9 : Morphisme de corps**

Soient  $(\mathbb{K}, +, \times)$  et  $(\mathbb{K}', \oplus, \otimes)$  deux corps.  $f : (\mathbb{K}, +, \times) \rightarrow (\mathbb{K}', \oplus, \otimes)$  est un **morphisme de corps** si et seulement s'il s'agit d'un morphisme d'anneaux, c'est-à-dire

- (i)  $\forall (x, y) \in \mathbb{K}^2, f(x + y) = f(x) \oplus f(y)$   
(ie  $f : (\mathbb{K}, +) \rightarrow (\mathbb{K}', \oplus)$  morphisme de groupes)
- (ii)  $\forall (x, y) \in \mathbb{K}^2, f(x \times y) = f(x) \otimes f(y)$
- (iii)  $f(1_{\mathbb{K}}) = 1_{\mathbb{K}'}$