Introductions aux structures algébriques

# 1 Lois de composition interne

## 1.1 Définition

Soit $E$ un ensemble non vide, une loi de composition interne sur $E$ est une application de $E^2$ dans $E$.

Exemples :

1. L'addition est une loi de composition interne sur $\mathbb{N}$ (sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$).
2. Le produit est une loi de composition interne sur $\mathbb{N}$ (sur $\mathbb{Q}$, $\mathbb{R}$).
3. La soustraction est une loi de composition interne sur $\mathbb{Z}$ (sur $\mathbb{Q}$, $\mathbb{R}$).
4. Le produit vectoriel est une loi de composition interne sur $\mathbb{R}^3$.

## 1.2 Propriétés

Soit un ensemble $E$ non vide muni de deux lois de composition interne $\star$ et $*$.

### 1.2.1 Associativité

La loi $\star$ est associative, si

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

Exemples :

1. L'addition est une loi de composition interne associative sur $\mathbb{N}$

$$\forall (x,y,z) \in \mathbb{N}^3, \quad (x+y)+z = x+(y+z).$$

2. La soustraction n' est pas une loi de composition interne associative sur $\mathbb{Z}$

$$(2-1)-3 = -2 \neq 4 = 2-(1-3).$$

### 1.2.2 Commutativité

La loi $\star$ est commutative, si

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

On réserve la notation $+$ (notation additive) pour les lois commutatives.

Exemples :

1. L'addition est une loi de composition interne commutative sur $\mathbb{N}$

$$\forall (x,y) \in \mathbb{N}^2, \quad x+y = y+x.$$

2. La soustraction n' est pas une loi de composition interne commutative sur $\mathbb{Z}$

$$2-1 = 1 \neq -1 = 1-2.$$

### 1.2.3 Élément neutre

Un élément $e$ de $E$ est l'élément neutre pour la loi $\star$, si

$$\forall x \in E, \quad x \star e = e \star x = x.$$

Si il existe, il est unique. On le note $e_E$ ou $1_E$.

Exemples :

1. 0 est le neutre pour la loi d'addition sur $\mathbb{N}$.

$$\forall x \in \mathbb{N}, \quad x + 0 = 0 + x = x.$$

2. La soustraction sur $\mathbb{Z}$ n' a pas de neutre.

### 1.2.4 Éléments symétrisables

On suppose que la loi $\star$ admet un élément neutre $e$. Soit $x$ un élément de $E$, $x$ est dit symétrisable dans $E$, si il existe $y \in E$, tel que $x \star y = y \star x = e$. On note $x^{-1}$ le symétrique (ou l'inverse) de $x$.

Exemples :

1. 0 est le seul élément symétrisable pour la loi d'addition sur $\mathbb{N}$.
2. Tous les éléments de $\mathbb{Z}$ sont symétrisables pour la loi d'addition.

### 1.2.5 Distributivité

La loi $\star$ est distributive à gauche (respectivement à droite) par rapport à la loi $*$ si

$$\forall (x, y, z) \in E^3, \quad x \star (y * z) = (x \star y) * (x \star z) \quad \text{(respectivement } (x * y) \star z = (x \star z) * (y \star z)).$$

La loi $\star$ est distributive par rapport à la loi $*$, si elle est distributive à droite et à gauche.

Exemple : La multiplication est distributive par rapport à la loi d'addition sur $\mathbb{N}$.

$$\forall (x, y, z) \in \mathbb{N}^3, \quad (x + y)z = xz + yz = z(x + y) = zx + zy.$$

### 1.2.6 Parties stables

Soient $E$ un munie d'une lois de composition interne $\star$ et $A$ une partie de $E$, on dit que $A$ est stable par loi $\star$, si

$$\forall (x, y) \in A^2, \quad x \star y \in A.$$

# 2 Groupes

## 2.1 Définition

Un ensemble non vide $G$ muni d'une loi de composition interne $\star$, $(G, \star)$ est un groupe si

(i) La loi $\star$ est associative.
(ii) La loi $\star$ admet un élément neutre $e_G$.
(iii) Tous les éléments de $G$ sont symétrisables pour la loi $\star$.

Un groupe est commutatif ou abélien, si la loi est commutative. On utilise la notation additive $+$ pour la loi uniquement pour des groupes commutatifs et le neutre est alors noté 0 ou $0_G$.

**Exemples de groupes :**

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathcal{S}_X, \circ)$ l'ensemble des permutations d'un ensemble.

## 2.2 Sous-groupes

### 2.2.1 Définition

Soient $(G, \star)$ un groupe et $H$ une partie de $G$, $(H, \star)$ un sous-groupe de $(G, \star)$, si $H$ est stable par $\star$ et que $(H, \star)$ possède une structure de groupe.

## 2.3 Caractérisation

Soient $(G, \star)$ un groupe et $H$ une partie de $G$, il y a équivalence entre les 3 propriétés suivantes :

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

(ii) $e_G \in H$
$\forall x, y \in H, \quad x \star y \in H \quad et \quad x^{-1} \in H$

(iii) $e_G \in H$
$\forall x, y \in H, \quad x^{-1} \star y \in H$

**Exemples de sous-groupes :**

$(\mathbb{R}^{+*}, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$.

## 2.4 Morphismes de groupes

### 2.4.1 Définition

Soient $(G, \star)$ et $(G', *)$ deux groupes et $f$ une application de $G$ dans $G'$, $f$ est un morphisme de groupes de $(G, \star)$ dans $(G', *)$ si

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

Si de plus $(G, \star) = (G', *)$, $f$ est un endomorphisme.

Si de plus $f$ est bijective, $f$ est isomorphisme.

Si $f$ est un endomorphisme et un isomorphisme, $f$ est un automorphisme.

### 2.4.2 Propriétés

Soit $f$ un morphisme de groupes de $(G, \star)$ dans $(G', *)$, alors on a :

1. $f(e_G) = e_{G'}$
2. $\forall x \in G, \quad f(x^{-1}) = f(x)^{-1}$
3. Si $H$ est un sous-groupe de $G$, $f(H)$ est un sous-groupe de $G'$.
4. Si $H'$ est un sous-groupe de $G'$, $f^{-1}(H')$ est un sous-groupe de $G$.
5. $f^{-1}(\{e_{G'}\})$ est un sous-groupe de $G$ appelé noyau de $f$ et noté $\mathrm{Ker}\,(f)$.
6. $f(G)$ est un sous-groupe de $G'$ appelé image de $f$ et noté $\mathrm{Im}\,(f)$.
7. $f$ morphisme injectif $\iff \mathrm{Ker}\,(f) = \{e_G\}$.

# 3 Anneaux et corps

## 3.1 Anneaux

Soit un ensemble $A$ non vide muni de deux lois de composition interne $+$ et $*$, $(A, +, *)$ est un anneau si

(i) $(A, +)$ est un groupe abélien. (on note $0_A$ son neutre)

(ii) La loi $*$ est associative et admet un élément neutre $e_A$. (on le note $1_A$)

(iii) La loi $*$ est distributive par rapport à $+$

L'anneau est commutatif, si la loi $*$ est commutative.

Exemples :

1. $(\mathbb{Z}, +, \times)$ est un anneau (idem pour $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$)
2. $\mathcal{M}_n(\mathbb{R})$ l'ensemble des matrices carrés d'ordre $n$ à coefficients dans $\mathbb{R}$ est un anneau (non commutatif dés que $n \geq 2$).

## 3.2 Sous-anneaux

### 3.2.1 Définition

Soient $(A, +, *)$ un anneau et $H$ une partie de $A$, $(H, +, *)$ un sous-anneau de $(A, +, *)$, si $H$ est stable par $+$ et $*$ et si $(H, +, *)$ possède une structure d'anneau.

### 3.2.2 Caractérisation

Soient $(A, +, *)$ un anneau et $H$ une partie de $A$, il y a équivalence entre les 2 propriétés suivantes :

(i) $(H, +, *)$ est un sous-anneau de $(A, +, *)$

(ii) $(H, +)$ est un sous-groupe de $(A, +)$, $1_A \in H$ et $\forall x, y \in H, \quad x * y \in H$.

Exemples :

1. $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. $(\mathbb{Q}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
3. $(\mathbb{R}, +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

## 3.3 Propriétés

**Proposition 1.** *Soit $(A, +, *)$ un anneau.*

*Les éléments de $A$ qui admettent un élément symétrique pour la loi $*$ sont appelés inversibles de l'anneau. L'ensemble des inversibles de $A$ (noté $A^*$) est un groupe pour la loi $*$.*

**Formules :** Si $a, b \in A$ **commutent** (c'est-à-dire $ab = ba$), alors on a pour tout entier $n \geq 0$ :

1. $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
2. $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k$
3. $a^{2n+1} + b^{2n+1} = (a+b) \sum_{k=0}^{2n} (-1)^k a^{2n-k} b^k$

**Définition 1.** *Soient $(A_1, +_1, \times_1)$ et $(A_2, +_2, \times_2)$ deux anneaux et $f$ une application de $A_1$ dans $A_2$, $f$ est un morphisme d'anneaux de $A_1$ dans ($A_2$ si*

$$\forall (x, y) \in G, \quad f(x +_1 y) = f(x) +_2 f(y). \quad \text{et} \quad f(x \times_1 y) = f(x) \times_2 f(y)$$

*Et*

$$f(1_{A_1}) = f(1_{A_2}).$$

## 3.4 Corps

Soit $(A, +, *)$ un anneau, $(A, +, *)$ est un corps si $(A \setminus \{0_A\}, *)$ est un groupe. On dit qu'un corps est commutatif, si l'anneau $A$ est commutatif. Les corps utilisés en cours seront toujours commutatifs.

Exemples :

1. $(\mathbb{Z}, +, \times)$ n'est pas un corps.
2. $(\mathbb{Q}, +, \times)$ est un corps (idem pour $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$).

## 3.5 Sous-corps

Soient $(\mathbb{K}, +, *)$ un corps et $H$ une partie de $\mathbb{K}$, $(H, +, *)$ un sous-corps de $(\mathbb{K}, +, *)$, si $H$ est stable par $+$ et $*$ et si $(H, +, *)$ possède une structure de corps.

Exemples :

1. $(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}^+, +, \times)$.
2. $(\mathbb{R}, +, \times)$ est un sous-corps de $(\mathbb{C}^+, +, \times)$.

### 3.5.1 Caractérisation

Soient $(\mathbb{K}, +, *)$ un corps et $H$ une partie de $\mathbb{K}$, il y a équivalence entre les 2 propriétés suivantes :

(i) $(H, +, *)$ est un sous-corps de $(\mathbb{K}, +, *)$

(ii) $(H, +, *)$ est un sous-anneau de $(\mathbb{K}, +, *)$, $\forall x \in H \setminus \{0_{\mathbb{K}}\}, \quad x^{-1} \in H$.