Maths : Algebra

Contents

1 Loi de composition interne :

1.1 Définition

Loi $*$ de composition interne sur X :

$$\begin{array}{rrcl} * : & X^2 & \longrightarrow & X \\ & (x,y) & \longmapsto & x*y \end{array}$$

1.2 Propriétés

Pour une LCI $* \in X^X$:

- Associativité : $\forall (x,y,z) \in X^3,\ x*(y*z) = (x*y)*z$
- Commutativité : $\forall (x,y) \in X^2,\ x*y = y*x$
- Élément neutre : $\exists e \in X \mid \forall x \in X,\ x*e = e*x = x$
- Élément régulier : $\exists a \in X \mid \forall (x,y) \in X^2, \begin{cases} a*x = a*y \Rightarrow x = y & \text{régulier à gauche} \\ x*a = y*a \Rightarrow x = y & \text{régulier à droite} \end{cases}$
- Symétrie : $x \in X$ est symétrisable $\Leftrightarrow$ $\exists x' \in X \mid x*x' = x'*x = e$
- Stabilité : $Y \in \mathcal{P}(X)$ stable par $*$ $\Leftrightarrow$ $\forall (x,y) \in Y^2,\ x*y \in Y$

2 Groupes

2.1 Définition (groupe)

Le couple $(G,*)$ est un groupe si :

- $G \neq \varnothing$
- $\forall (x,y) \in G^2,\ x*y \in G$ ($*$ LCI)
- $\forall (x,y,z) \in G^3,\ x*(y*z) = (x*y)*z$ ($*$ associative)
- $\exists e \in G \mid \forall x \in G,\ x*e = e*x = x$ (élément neutre)
- $\forall x \in G,\ \exists x' \in G \mid x'*x = x*x' = e$ (Tout élément est symétrisable)

On note $x^{-1} = x'$.
Le groupe $(G,*)$ est dit *abélien* si $*$ est commutative.

2.2 Définition (sous-groupe)

H est un sous-groupe de $(G,*)$ si :

- $H \in \mathcal{P}(G) \setminus \{\varnothing\}$
- $\forall (x,y) \in H^2,\ x * y \in H$ (H stable par $*$)
- $\forall x \in H,\ x^{-1} \in H$ (H stable par passage au symétrique)

3 Anneaux

3.1 Définition (anneau)

Le triplet $(A, \oplus, \otimes)$ est un anneau si :

- $(A, \oplus)$ est un groupe abélien
- $\forall (x,y) \in A^2,\ x \otimes y \in A$ ($\otimes$ LCI sur A)
- $\forall (x,y,z) \in A^3,\ x \otimes (y \otimes z) = (x \otimes y) \otimes z$ ($\otimes$ associative)
- $\exists e \in A \mid \forall x \in A,\ x \otimes e = e \otimes x = x$ ($\otimes$ admet un élément neutre)
- $\forall (x,y,z) \in A^3,\ \begin{cases} x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \\ (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x) \end{cases}$ ($\otimes$ distributive sur $\oplus$)

L'élément neutre de $\oplus$ est noté 0.
L'élément neutre de $\otimes$ est noté 1.
Le symétrique de $x \in A$ par $\oplus$ est noté $-x$, et appelé opposé.
Le symétrique de $x \in A$ par $\otimes$, s'il existe, est noté x^{-1}, et appelé inverse.
On définit : $\forall (x,y) \in A^2,\ xy = x \otimes y$.
On définit : $A^* = \{x \in A \mid \exists y \in A \mid xy = 1\}$

L'anneau $(A, +, \times)$ est dit *abélien* si $\times$ est commutative.

3.2 Diviseur de zéro

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

Alors $x \in A$ est un diviseur de zéro si $\begin{cases} x \neq 0 \\ \exists y \in A \setminus \{0\} \mid xy = 0 \text{ ou } yx = 0 \end{cases}$.

3.3 Anneau intègre

Un anneau $(A, +, \times)$ est intègre si $\begin{cases} A \neq \{0\} \\ \forall (x,y) \in A^2,\ xy = yx \\ \forall (x,y) \in A^2,\ xy = 0 \Rightarrow (x = 0 \text{ ou } y = 0) \end{cases}$

3.4 Propriétés

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

- $(A^*, \times)$ est un groupe
- $\forall (x, y) \in A^{*2}, \begin{cases} xy \in A^* \\ (xy)^{-1} = y^{-1}x^{-1} \end{cases}$
- $\forall (a, b) \in A^2 \mid ab = ba, \ \forall n \in \mathbb{N}, \quad \begin{cases} (a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ a^n - b^n = (a-b) \displaystyle\sum_{k=0}^{n-1} a^k b^{n-1-k} \end{cases}$

3.5 Définition (sous-anneau)

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

- B est un sous-groupe de $(A, +)$
- $1 \in B$
- $\forall (x, y) \in B^2, \ xy \in B$

4 Corps

4.1 Définition (corps)

Le triplet $(K, +, \times)$ est un corps si

- $(K, +, \times)$ est un anneau abélien
- $\exists x, y \in K \mid x \neq y$ (K contient au moins deux éléments)
- $K^* = K \setminus \{0\}$ (Tous les éléments sauf 0 sont inversibles)

4.2 Définition (sous-corps)

C est un sous-corps de $(K, +, \times)$ si :

- C est un sous-anneau de $(K, +, \times)$
- $\forall x \in C \setminus \{0\}, \ x^{-1} \in C$ (C stable par passage à l'inverse)

5 Morphismes

5.1 Morphismes de groupes

5.1.1 Définition

Soient $(G, *)$ et $(G', *')$ deux groupes.

- Un morphisme de groupes de G vers G' est une fonction

$$f : G \longrightarrow G' \mid \forall (x,y) \in G,\ f(x * y) = f(x) *' f(y)$$

• Un isomorphisme de groupes est un morphisme de groupes bijectif.

• Un automorphisme de groupes est un isomorphisme de groupes d'un groupe dans lui-même.

5.1.2 Propriétés

Soient $(G,*)$, $(G',*')$ deux groupes, e, e' leurs éléments neutres respectifs, et f un morphisme de groupes de G vers G'.

• $f(e) = e'$

• $\forall x \in G,\ f(x^{-1}) = \Big(f(x)\Big)^{-1}$

• La composition de deux morphismes de groupes est un morphisme de groupes.

5.2 Noyau

5.2.1 Définition

Soient $(G,*)$, $(G',*')$ deux groupes, f un morphisme de groupes de G vers G' et e' l'élément neutre de $(G',*')$.
Le noyau de f est :

$$\mathrm{Ker}(f) = f^{-1}\Big(\{e'\}\Big) = \{x \in G \mid f(x) = e'\}$$

5.2.2 Propriétés

Soient $(G,*)$, $(G',*')$ deux groupes, f un morphisme de groupes de G vers G' et e l'élément neutre de $(G,*)$.
Alors :

$$f \text{ injective } \Leftrightarrow \mathrm{Ker}(f) = \{e\}$$

5.3 Morphismes d'anneaux

Soient $(A,+,\times)$ et $(B,+',\times')$ deux anneaux.

• Un morphisme d'anneaux de $(A,+,\times)$ vers $(B,+',\times')$ est un morphisme de groupes de $(A,+)$ vers $(B,+')$ tel que :

$$\forall (x,y) \in A,\ \begin{cases} f(xy) = f(x)f(y) \\ f(1) = 1 \end{cases}$$

• Un isomorphisme d'anneaux est un morphisme d'anneaux bijectifs.