

1. Cours 4: Quelques structures algébriques

1.1. Loi de composition interne

On appelle loi de composition interne (ou opération binaire) sur un ensemble non vide E , toute application $*$ de $E \times E$ dans E .

L'image $*(x, y)$ est souvent notée $x * y$.

$$\# \left(\begin{array}{l} * \text{ est une loi de composition} \\ \text{interne sur } E \end{array} \right) \Leftrightarrow \left\{ \begin{array}{l} \forall x, y \in E, x * y \in E \\ \forall x, y, x', y' \in E, (x = x' \text{ et } y = y') \Rightarrow x * y = x' * y' \end{array} \right.$$

Exemples:

1) On sait que: $\forall x, y \in \mathbb{N} : x + y \in \mathbb{N}$ et $x \cdot y \in \mathbb{N}$

et $\forall x, y, x', y' \in \mathbb{N}, (x = x' \text{ et } y = y') \Rightarrow (x + y = x' + y' \text{ et } x \cdot y = x' \cdot y')$

Alors, l'addition usuelle "+" et la multiplication usuelle "." sont des lois de composition internes sur \mathbb{N} .

Il est clair que l'addition usuelle "+" et la multiplication usuelle "." sont des lois de composition internes sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C} .

2) La soustraction usuelle "-" est une loi de composition interne sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C} , mais pas sur \mathbb{N} .

3) L'addition usuelle "+" sur l'ensemble $B = \{0, 1\}$ n'est pas une loi de composition interne. En effet:

(x, y)	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$+(x, y)$	0	1	1	$2 \notin B$

La multiplication usuelle "." sur l'ensemble $B = \{0, 1\}$ est une loi de composition interne. En effet:

(x, y)	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$\cdot(x, y)$	0	0	0	1

4) Le produit scalaire $\diamond : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ défini par $\begin{pmatrix} x \\ y \end{pmatrix} \diamond \begin{pmatrix} x' \\ y' \end{pmatrix} = xx' + yy'$ n'est pas une loi de composition interne.

5) La composition \circ est une loi de composition interne sur l'ensemble $A(E, E)$ des applications de E dans E . En effet: Si $f : E \rightarrow E$ et $g : E \rightarrow E$ sont deux applications alors, $f \circ g : E \rightarrow E$ est une application.

6) L'intersection \cap est une loi de composition interne sur l'ensemble $\mathcal{P}(E)$ des parties de E .

Définitions: Soit $*$ une loi de composition interne sur un ensemble non vide E .

Alors:

- 1) La loi $*$ est dite associative, si $\forall x, y, z \in E, (x * y) * z = x * (y * z)$
- 2) La loi $*$ admet un élément neutre si $\exists e \in E, \forall x \in E, (x * e = x) \wedge (e * x = x)$
L'élément e (s'il existe) est appelé élément neutre de $*$.
- 3) Dans le cas où $*$ admet un élément neutre e , on dit que tout élément de E est inversible (ou symétrisable) par rapport à $*$, si $\forall x \in E, \exists x' \in E, (x * x' = e) \wedge (x' * x = e)$
L'élément x' (s'il existe) est appelé inverse (ou symétrique) de x et est noté x^{-1} .
- 4) La loi $*$ est dite commutative, si $\forall x, y \in E, x * y = y * x$

Remarque:

- 1) La disposition des parenthèses est inutile si la loi $*$ est associative et on peut écrire $x * y * z$ au lieu de $(x * y) * z$ et $x * (y * z)$
- 2) Si x^{-1} existe, alors $(x^{-1})^{-1} = x$.

Exemples:

- 1) On sait que
 $\forall x, y, z \in \mathbb{R}, x + (y + z) = (x + y) + z$, donc l'addition usuelle "+" est associative dans \mathbb{R} .
 $\exists e = 0 \in \mathbb{R}, \forall x \in \mathbb{R}, (x + 0 = x) \wedge (0 + x = x)$, donc 0 est l'élément neutre de "+" dans \mathbb{R} .
 $\forall x \in \mathbb{R}, \exists x' = -x \in \mathbb{R}, (x + (-x) = 0) \wedge ((-x) + x = 0)$, donc tout élément de \mathbb{R} est inversible par rapport à "+".
 $\forall x, y \in \mathbb{R}, x + y = y + x$, donc l'addition usuelle "+" est commutative dans \mathbb{R} .
- 2) On sait que
 $\forall x, y, z \in \mathbb{R}, x \cdot (y \cdot z) = (x \cdot y) \cdot z$, donc la multiplication usuelle "." est associative dans \mathbb{R} .
 $\exists e = 1 \in \mathbb{R}, \forall x \in \mathbb{R}, (x \cdot 1 = x) \wedge (1 \cdot x = x)$, donc 1 est l'élément neutre de "." dans \mathbb{R} .
Pour $x = 0$ on ne peut pas trouver $x' \in \mathbb{R}$ tel que $0 \cdot x' = 1$; donc $x = 0$ n'est pas inversible par rapport à la multiplication usuelle "." :
C.à.d: $\exists x = 0 \in \mathbb{R}, \forall x' \in \mathbb{R}, (x \cdot x' \neq 1) \vee (x' \cdot x \neq 1)$, donc les éléments de \mathbb{R} ne sont pas tous inversibles par rapport à ".".
 $\forall x, y \in \mathbb{R}, x \cdot y = y \cdot x$, donc la multiplication usuelle "." est commutative dans \mathbb{R} .

3) Etudions l'opération \top définie sur \mathbb{Z} par $n \top m = -n - m$ pour $n, m \in \mathbb{Z}$.

Soient $n, m, s \in \mathbb{Z}$.

$$(n \top m) \top s = (-n - m) \top s = n + m - s$$

$$n \top (m \top s) = n \top (-m - s) = -n + m + s$$

$$\text{On a par exemple: } (1 \top 2) \top 3 = (-1 - 2) \top 3 = 3 - 3 = 0$$

$$1 \top (2 \top 3) = 1 \top (-2 - 3) = -1 + 5 = 4 \neq (1 \top 2) \top 3; \text{ donc } \top$$

n'est pas associative dans \mathbb{Z} .

Supposons e est l'élément neutre de l'opération \top dans \mathbb{Z} .

$$\text{C.à.d } \forall n \in \mathbb{Z}, n \top e = n \wedge e \top n = n.$$

$$n \top e = n \Leftrightarrow -n - e = n \Leftrightarrow e = -2n$$

donc \top n'admet pas d'élément neutre, car l'élément neutre doit être le même pour tous les $n \in \mathbb{Z}$.

On ne peut pas chercher l'inverse d'un élément, car \top n'admet pas d'élément neutre

$$n \top m = -n - m = -m - n = m \top n, \text{ donc } \top \text{ est commutative dans } \mathbb{Z}.$$

1.2. Structure de groupe

Définition: Soit $*$ une loi de composition interne sur un ensemble non vide G . On dit que $(G, *)$ est un groupe si $*$ est associative, admet un élément neutre e et tout élément de G est inversible par rapport à $*$.

Si en plus, $*$ est commutative, le groupe est dit commutatif ou abélien.

Exemples :

- 1) Les structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs.
- 2) Les structures (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) et (\mathbb{C}, \cdot) ne sont pas des groupes (Car 0 n'a pas d'inverse pour la multiplication usuelle " \cdot ".)
- 3) Les structures (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) et (\mathbb{C}^*, \cdot) sont des groupes commutatifs.
- 4) Les structures $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) ne sont pas des groupes.
- 5) (\mathbb{Z}, \top) telle que $n \top m = -n - m$, n'est pas un groupe.

1.2.1. Sous groupe

Définition: Soit $(G, *)$ un groupe et H une partie de G .

On dit $(H, *)$ est un sous groupe de $(G, *)$ si $(H, *)$ est lui même un groupe pour la loi $*$ restreinte à H .

Proposition: Soit H une partie d'un groupe $(G, *)$ d'élément neutre e . Alors,

$((H, *) \text{ est un sous groupe de } (G, *)) \Leftrightarrow \begin{cases} e \in H \\ \forall x, y \in H : x * y^{-1} \in H \end{cases}$

Preuve: a) Supposons que $(H, *)$ est un sous groupe de $(G, *)$ et montrons que

$\begin{cases} e \in H \\ \forall x, y \in H : x * y^{-1} \in H \end{cases}$

Soit $x, y \in H$,

On a $x, y^{-1} \in H$ (Car tout élément de H admet un inverse par rapport à $*$ dans H)

et $x * y^{-1} \in H$ (Car $*$ est une loi de composition interne dans H)

Donc $\forall x, y \in H : x * y^{-1} \in H$

Mais $H \neq \emptyset$, donc $\exists x_0 \in G : x_0 \in H$, d'où $x_0 * x_0^{-1} \in H$. C.à.d $e \in H$.

b) Supposons que $\begin{cases} e \in H \\ \forall x, y \in H : x * y^{-1} \in H \end{cases}$ et montrons que $(H, *)$ est un sous groupe de $(G, *)$

On a $H \neq \emptyset$ car $e \in H$.

et comme $\forall x \in G : x * e = x = e * x$. En particulier $\forall x \in H : x * e = x = e * x$

C.à.d: e est l'élément neutre de $*$ dans H .

Soit $y \in H$ et $x = e \in H$, alors $x * y^{-1} = e * y^{-1} = y^{-1} \in H$, donc $\forall y \in H : y^{-1} \in H$.

C.à.d: Tout élément de H admet un inverse par rapport à $*$ dans H .

Soit $x, y \in H$, alors $x, y^{-1} \in H$ d'où $x * (y^{-1})^{-1} = x * y \in H$; donc $\forall x, y \in H : x * y \in H$.

C.à.d: $*$ est une loi de composition interne dans H .

Soit $x, y, z \in H$, alors $x, y, z \in G$ d'où $(x * y) * z = x * (y * z)$, donc

$\forall x, y, z \in H : (x * y) * z = x * (y * z)$. C.à.d: $*$ est une loi associative dans H .

Ainsi $(H, *)$ vérifie toutes les conditions d'un groupe, donc c'est bien un sous groupe de $(G, *)$. ■

Exemples :

1) \mathbb{Z} est une partie de \mathbb{Q} et $(\mathbb{Q}, +)$ est un groupe.

On a $\begin{cases} 0 \in \mathbb{Z} \\ \forall x, y \in \mathbb{Z} : x + (-y) \in \mathbb{Z} \end{cases}$, alors $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Q}, +)$.

De même $(\mathbb{Q}, +)$ est un sous groupe de $(\mathbb{R}, +)$ et de $(\mathbb{C}, +)$.

2) Si $(G, *)$ est un groupe d'élément neutre e .

On a $\begin{cases} e \in G \\ \forall x, y \in G : x * y^{-1} \in G \end{cases}$, alors $(G, *)$ est un sous groupe de $(G, *)$.

On a $\begin{cases} e \in \{e\} \\ \forall x, y \in \{e\} : x * y^{-1} \in \{e\} \end{cases}$, alors $(\{e\}, *)$ est un sous groupe de $(G, *)$.
 $\{e\}$ et G sont appelés sous groupes triviaux de $(G, *)$.

3) Le cercle unité $S^1 = \{z \in \mathbb{C} / |z| = 1\}$ est une partie de \mathbb{C}^* et (\mathbb{C}^*, \cdot) est un groupe.

On a $|1| = 1$ donc $1 \in S^1$.

Soit $z, z' \in S^1$, on a $|z \cdot (z')^{-1}| = \frac{|z|}{|z'|} = 1$, donc $z \cdot (z')^{-1} \in S^1$

Donc $\begin{cases} 1 \in S^1 \\ \forall z, z' \in S^1 : z \cdot (z')^{-1} \in S^1 \end{cases}$, alors (S^1, \cdot) est un sous groupe de (\mathbb{C}^*, \cdot) .

4) \mathbb{R}^{*+} est une partie de \mathbb{R}^* et (\mathbb{R}^*, \cdot) est un groupe.

On a $1 \in \mathbb{R}^{*+}$.

Soit $x, x' \in \mathbb{R}^{*+}$, on a $x \cdot (x')^{-1} = \frac{x}{x'} > 0$, donc $x \cdot (x')^{-1} \in \mathbb{R}^{*+}$

Donc $\begin{cases} 1 \in \mathbb{R}^{*+} \\ \forall x, x' \in \mathbb{R}^{*+} : x \cdot (x')^{-1} \in \mathbb{R}^{*+} \end{cases}$, alors (\mathbb{R}^{*+}, \cdot) est un sous groupe de (\mathbb{R}^*, \cdot) .

1.3. Homomorphismes de groupes

Définition: On appelle homomorphisme du groupe $(G, *)$ dans le groupe $(G', *')$, toute application $f : G \rightarrow G'$ telle que:

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

Exemples :

1) Soit l'application $h : \mathbb{R} \rightarrow \mathbb{R}^{*+}$ telle que $h(x) = e^x$ et soit $x, y \in \mathbb{R}$.

On a $h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot h(y)$.

Alors h est un homomorphisme du groupe $(\mathbb{R}, +)$ dans le groupe (\mathbb{R}^{*+}, \cdot)

2) Soit l'application $f : \mathbb{C}^* \rightarrow \mathbb{R}^*$ telle que $f(z) = |z|$ et soit $z, z' \in \mathbb{C}^*$.

On a $f(z \cdot z') = |z \cdot z'| = |z| \cdot |z'| = f(z) \cdot f(z')$.

Alors f est un homomorphisme du groupe (\mathbb{C}^*, \cdot) dans le groupe (\mathbb{R}^*, \cdot)

Théorème: Soit $f : G \rightarrow G'$ un homomorphisme du groupe $(G, *)$ dans le groupe $(G', *')$ d'éléments neutres respectifs e et e' , alors

1) $f(e) = e'$.

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

Preuve:

1) On a $f(e) = f(e) *' e' = f(e) *' [f(x) *' (f(x))^{-1}] = [f(e) *' f(x)] *' (f(x))^{-1}$
 $= f(e * x) *' (f(x))^{-1} = f(x) *' (f(x))^{-1} = e'$

2) Soit $x \in G$

$f(x^{-1}) *' f(x) = f(x^{-1} * x) = f(e) = e'$
et $f(x) *' f(x^{-1}) = f(x * x^{-1}) = f(e) = e'$

Alors $(f(x))^{-1} = f(x^{-1})$.

1.4. Structure d'Anneau

Définition: Soit A un ensemble non vide muni de deux lois de composition interne $*_1$ et $*_2$. On dit que $(A, *_1, *_2)$ est un anneau si

1) $(A, *_1)$ est un groupe commutatif.

2) La loi $*_2$ est associative.

3) $\forall x, y, z \in A : \left\{ \begin{array}{l} x *_2 (y *_1 z) = (x *_2 y) *_1 (x *_2 z) \\ (y *_1 z) *_2 x = (y *_2 x) *_1 (z *_2 x) \end{array} \right.$

(Cette condition est appelée distributivité de la loi $*_2$ par rapport à la loi $*_1$).

Si la loi $*_2$ admet un élément neutre, on l'appelle unité et on dit que l'anneau est unitaire.

Si la loi $*_2$ est commutative, on dit que l'anneau est commutatif.

Exemples:

1) On sait que $(\mathbb{Z}, +)$ est un groupe commutatif, la multiplication usuelle " \cdot " est associative et distributive par rapport à l'addition usuelle " $+$ " dans \mathbb{Z} .

Alors $(\mathbb{Z}, +, \cdot)$ est un anneau.

De plus, la deuxième loi " \cdot " est commutative et admet 1 comme élément neutre, donc $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif et unitaire.

De même, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux unitaires, commutatifs.

Remarque:

Les lois d'un anneau $(A, *_1, *_2)$ sont souvent notées $+_A$ et \cdot_A au lieu de $*_1$ et $*_2$ et pour cette raison on note l'élément neutre de $+_A$ par 0_A et l'inverse de x par rapport à $+_A$ par $-x$

Aussi, on note l'élément neutre de \cdot_A (s'il existe) par 1_A et l'inverse de x par rapport à \cdot_A (s'il existe) par x^{-1} .

1.4.1. Quelques règles de calcul

Proposition: Soit $(A, +_A, \cdot_A)$ un anneau d'élément neutre 0_A . Alors:

- 1) $\forall x \in A : x \cdot_A 0_A = 0_A = 0_A \cdot_A x$
- 2) $\forall x, y \in A : (-x) \cdot_A y = -(x \cdot_A y) = x \cdot_A (-y)$
- 3) $\forall x, y \in A : (-x) \cdot_A (-y) = x \cdot_A y$
- 4) Si l'anneau admet un élément unité 1_A , alors $\forall x \in A : -x = (-1_A) \cdot_A x$.

Preuve

1) Soit $x \in A$

$$\begin{aligned} x \cdot_A 0_A &= x \cdot_A 0_A +_A 0_A \\ &= x \cdot_A 0_A +_A [x \cdot_A 0_A +_A (- (x \cdot_A 0_A))] && \text{Car } -x \cdot_A 0_A \text{ est le symétrique de } x \cdot_A 0_A \\ & && \text{par rapport à } +_A. \\ &= x \cdot_A (0_A +_A 0_A) +_A (- (x \cdot_A 0_A)) && \text{Car } \cdot_A \text{ est distributive par rapport à } +_A \\ &= x \cdot_A 0_A +_A (- (x \cdot_A 0_A)) \\ &= 0_A \end{aligned}$$

De la même façon on montre que $-(x \cdot_A y) = x \cdot_A (-y)$

2) Soit $x, y \in A$

$$\begin{aligned} x \cdot_A y +_A ((-x) \cdot_A y) &= (x +_A (-x)) \cdot_A y && \text{Car } \cdot_A \text{ est distributive par rapport à } +_A \\ &= 0_A \cdot_A y \\ &= 0_A && \text{D'après 1)} \end{aligned}$$

Alors $(-x) \cdot_A y = -(x \cdot_A y)$.

De la même façon on montre que $0_A \cdot_A x = 0_A$

3) Soient $x, y \in A$,

$$\begin{aligned} (-x) \cdot_A (-y) &= -(x \cdot_A (-y)) && \text{D'après 2)} \\ &= -(- (x \cdot_A y)) && \text{D'après 2)} \\ &= x \cdot_A y \end{aligned}$$

1.4.2. Anneau intègre

On dit qu'un anneau $(A, +_A, \cdot_A)$ est intègre, si

$$\forall x, y \in A : (x \cdot_A y = 0_A \Rightarrow (x = 0_A \vee y = 0_A))$$

Exemples:

Les structures $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux intègres.

1.5. Structure de corps

Définition: Soit $(K, +_K, \cdot_K)$ un anneau unitaire. On dit que $(K, +_K, \cdot_K)$ est un corps si

1) $1_K \neq 0_K$

2) Tout élément de $K - \{0_K\}$ est inversible par rapport à la loi \cdot_K .

Le corps est dit commutatif si la loi \cdot_K est commutative.

Remarques:

1) Si $(K, +_K, \cdot_K)$ est un corps, alors (K^*, \cdot_K) est un groupe (où $K^* = K - \{0_K\}$).

2) Tout corps K est un anneau intègre. En effet: Soit $a, b \in K$, On a:

$$\begin{aligned} a \cdot_K b = 0_K &\Rightarrow (a \cdot_K b = 0_K \wedge (a = 0_K \vee a \neq 0_K)) \\ &\Rightarrow ((a \cdot_K b = 0_K \wedge a = 0_K) \vee (a \cdot_K b = 0_K \wedge a \neq 0_K)) \\ &\Rightarrow ((a = 0_K) \vee (a^{-1} \cdot_K a \cdot_K b = a^{-1} \cdot_K 0_K)) \text{ car } a \neq 0_K \text{ assure que } a^{-1} \text{ existe} \\ &\Rightarrow ((a = 0_K) \vee (b = 0_K)) \end{aligned}$$

Exemples :

1) Les structures $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des corps commutatifs.

2) La structure $(\mathbb{Z}, +, \cdot)$ n'est pas un corps, car les seuls éléments inversibles dans \mathbb{Z}^* par rapport à la multiplication usuelle \cdot sont 1 et -1 .