

Chapitre 10

Structures algébriques

Plan du chapitre

1	Loi de composition interne	1
1.1	Généralités	1
1.2	Élément neutre, élément symétrisable.	3
2	Groupes	3
2.1	Définition et propriétés générales	3
2.2	Notations additive et multiplicative.	5
2.3	Calcul dans un groupe	5
2.4	Sous-groupes	6
2.5	Morphismes de groupes	8
2.6	Noyau et image d'un morphisme.	9
2.7	Groupe produit	12
3	Anneaux	12
3.1	Anneau	12
3.2	Sous-anneau	13

Hypothèse

Dans tout ce chapitre, E est un ensemble.

1 Loi de composition interne

1.1 Généralités

Définition 10.1 (Loi de composition interne)

On appelle loi de composition interne sur E (en abrégé l.c.i.) toute application de $E \times E$ dans E .
Si on note $\top : E \times E \rightarrow E$ une telle application, alors on notera $x\top y$ au lieu de $\top(x, y)$.

Exemple 1. L'addition $+$ et la multiplication \times sont des l.c.i. sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

La soustraction $-$ est une l.c.i. sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, mais pas sur \mathbb{N} .

La division $/$ est une l.c.i. sur \mathbb{Q}^* ou sur \mathbb{R}_+^* mais pas sur \mathbb{Z}^* .

La conjugaison $z \mapsto \bar{z}$ n'est pas une l.c.i. sur \mathbb{C} car son ensemble de départ est \mathbb{C} et non $\mathbb{C} \times \mathbb{C}$.

Exemple 2. Soit X un ensemble. Sur $E := \mathcal{P}(X)$, on peut définir les l.c.i. suivantes :

1. La réunion : $(A, B) \mapsto A \cup B$

2. L'intersection : $(A, B) \mapsto A \cap B$

3. La différence : $(A, B) \mapsto A \setminus B$

Définition 10.2 (Commutativité, associativité)

Une l.c.i. \top sur un ensemble E est dite :

- commutative si $\forall x, y \in E \quad x \top y = y \top x$,
- associative si $\forall x, y, z \in E \quad (x \top y) \top z = x \top (y \top z)$.

Exemple 3. Les l.c.i. $+$ et \times sont commutatives et associatives sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

La l.c.i. $-$ sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est / n'est pas commutative et est / n'est pas associative.

Pour tout ensemble X , la réunion \cup et l'intersection \cap sont commutatives et associatives sur $\mathcal{P}(X)$.

Remarque (Associativité et réécriture d'expressions). Si \top est une l.c.i. associative sur E , alors on peut écrire sans ambiguïté $x \top y \top z$ sans préciser les parenthèses. On peut de même écrire, pour toute famille $(x_i)_{1 \leq i \leq n}$ d'éléments de E ,

$$\bigtop_{1 \leq i \leq n} x_i := x_1 \top x_2 \top \dots \top x_n$$

Les lois $+, \times, \cup, \cap$ étant associatives, on peut donc écrire :

$$\sum_{i=1}^n x_i \quad \prod_{i=1}^n x_i \quad \bigcup_{i=1}^n A_i \quad \bigcap_{i=1}^n A_i$$

et comme en plus ces lois sont commutatives, l'ordre des x_i ou des A_i importe peu, et on peut donc faire des regroupements de termes comme on le souhaite, par exemple :

$$\sum_{i=1}^{10} x_i = \sum_{i=1}^5 x_{2i} + \sum_{i=0}^4 x_{2i+1}$$

Exemple 4. La composition \circ est une l.c.i. sur E^E . \circ est associative on peut donc écrire $f \circ g \circ h$ sans ambiguïté. Si $E \neq \emptyset$, alors on peut trouver $f, g \in E^E$ tels que $f \circ g \neq g \circ f$, donc \circ n'est pas commutative.

Définition 10.3

Deux éléments $x, y \in E$ commutent (pour \top) si $x \top y = y \top x$.

Bien entendu, si \top est commutative, alors tous les éléments de E commutent.

Exemple 5. Soient $f, g \in \mathbb{C}^{\mathbb{C}}$ les fonctions définies par $f(z) = z^2$ et $g(z) = \bar{z}$. Montrer que f, g commutent.

1.2 Élément neutre, élément symétrisable

Définition 10.4 (Élément neutre et élément symétrisable)

On suppose que \top est une l.c.i. sur E . On dit que $e \in E$ est un élément neutre (pour \top) si

$$\forall x \in E \quad x \top e = e \top x = x$$

Si un élément neutre $e \in E$ existe, alors on dit qu'un élément $x \in E$ est symétrisable (pour \top) si

$$\exists x' \in E \quad x \top x' = x' \top x = e$$

Tout élément $x' \in E$ qui vérifie cette propriété est appelé un symétrique de x (pour \top).

Exemple 6.

- 0 est l'élément neutre de $+$ sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ tout élément x est symétrisable pour $+$, avec pour (unique) symétrique $-x$.
- 1 est l'élément neutre de \times sur $\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$. Sur $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, tout élément x est symétrisable pour \times , avec pour (unique) symétrique x^{-1} .
- Sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, la l.c.i. $-$ n'admet pas d'élément neutre.

Exemple 7. Soit X un ensemble. id_X est l'élément neutre de \circ sur X^X .

\emptyset est l'élément neutre de \cup sur $\mathcal{P}(X)$.

X est l'élément neutre de \cap sur $\mathcal{P}(X)$.

2 Groupes

2.1 Définition et propriétés générales

Définition 10.5 (Groupe)

Soit G un ensemble. On dit que (G, \top) est un groupe si :

G1. \top est une l.c.i. sur G .

G2. \top est associative : $\forall a, b, c \in G \quad a \top (b \top c) = (a \top b) \top c$.

G3. G possède un élément neutre (pour \top) :

$$\exists e \in G \quad \forall a \in G \quad a \top e = e \top a = a$$

G4. Tout élément $a \in G$ est symétrisable (pour \top) :

$$\forall a \in G \quad \exists a' \in G \quad a \top a' = a' \top a = e$$

Si de plus, \top est commutative, on dit que (G, \top) est un groupe commutatif (ou encore un groupe abélien).

Par abus de langage, on sous-entend parfois la loi \top et on dit simplement que G est un groupe.

Exemple 8. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs. Mais $(\mathbb{N}, +)$ n'est pas un groupe car

(\mathbb{Q}^*, \times) , (\mathbb{R}^*, \times) et (\mathbb{C}^*, \times) sont des groupes commutatifs. Mais (\mathbb{Z}^*, \times) n'est pas un groupe (même raison que $(\mathbb{N}, +)$ ci-dessus mais avec la loi \times). De plus, (\mathbb{Q}, \times) , (\mathbb{R}, \times) et (\mathbb{C}, \times) ne sont pas des groupes car

Notation (Lois \times et \cdot , notation ab). Souvent, quand on emploie la loi \times , on préfère noter ab plutôt que $a \times b$. De même, on emploie parfois une loi "point" notée " \cdot " et à nouveau on préfère écrire ab plutôt que $a \cdot b$.

Exemple 9. Soit $n \in \mathbb{N}^*$. Montrer que (\mathbb{R}_+^*, \times) est un groupe commutatif.

Proposition 10.6

Soit (G, \top) un groupe. Alors l'élément neutre de G est unique.

De plus, il y a *unicité* du symétrique de tout élément de G : on dira donc **le** symétrique d'un élément de G .

Démonstration.

□

Remarque. Un groupe G est toujours non vide, car G possède un élément neutre.

G peut ne contenir que son élément neutre. Par exemple $\{0\}$ est un groupe pour $+$. Un groupe qui est réduit à son élément neutre est dit trivial.

2.2 Notations additive et multiplicative

Souvent, les lois associatives sont notées de façon additive ($a + b$) ou multiplicative (ab). De plus, la notation additive $a + b$ n'est employée que pour une l.c.i. commutative.

$a, b, c \in E$	Notation additive : loi +	Notation multiplicative : loi \cdot ou \times
Associativité	$a + (b + c) = (a + b) + c$	$a(bc) = (ab)c$
Élément neutre	$a + 0 = 0 + a = a$	$a1 = 1a = a$ $ae = ea = a$
Symétrique de a	<u>Opposé</u> : $-a$ $a + (-a) = (-a) + a = 0$	<u>Inverse</u> : a^{-1} $aa^{-1} = a^{-1}a = e$
Itéré n -ième ($n \in \mathbb{N}^*$)	$na := \underbrace{a + a + \dots + a}_{n \text{ fois}}$	$a^n := \underbrace{aa \dots a}_{n \text{ fois}}$
Itéré 0-ième	$0a := 0$	$a^0 := e$
Itéré $(-n)$ -ième (si a symétrisable)	$(-n)a := n(-a) = \underbrace{(-a) + (-a) + \dots + (-a)}_{n \text{ fois}}$	$a^{-n} := (a^{-1})^n = \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{n \text{ fois}}$
$\forall n, m \in \mathbb{Z}$	$na + ma = (n + m)a$	$a^n a^m = a^{n+m}$
$\forall n, m \in \mathbb{Z}$	$n(ma) = (nm)a$	$(a^n)^m = a^{nm}$

Remarque. Une fonction $f : E \rightarrow E$ est symétrisable pour \circ si et seulement s'il existe $g : E \rightarrow E$ telle que

$$f \circ g = g \circ f = \text{id}_E$$

c'est-à-dire si et seulement si f admet une application réciproque et dans ce cas $f^{-1} = g$. La notation f^{-1} pour une application réciproque est empruntée à la notation multiplicative ci-dessus.

Il arrive même que certains sujets notent " fg " pour la composée $f \circ g$ afin de mieux correspondre à la notation multiplicative ! Dans ce cas, on prendra garde au fait que f^n désigne la fonction $f \circ f \circ \dots \circ f$ et non $x \mapsto f(x)^n$.

2.3 Calcul dans un groupe

Dans cette partie, on utilisera la notation multiplicative pour noter le symétrique d'un élément (a^{-1}).

Proposition 10.7

Soit (G, \top) un groupe et $x, y \in G$. Alors,

$$(x^{-1})^{-1} = x \quad \text{et} \quad (x \top y)^{-1} = y^{-1} \top x^{-1} \quad \text{et}$$

Démonstration.

□

Proposition 10.8

Soit (G, \cdot) un groupe (notation multiplicative) et $a, b \in G$. Alors,

- Pour tous $x, y \in G$, $ax = ay \implies x = y$. (on multiplie à gauche par a^{-1})
- Pour tous $x, y \in G$, $xa = ya \implies x = y$. (on multiplie à droite par a^{-1})
- l'équation $ax = b$ d'inconnue $x \in G$ possède pour unique solution $x = a^{-1}b$.
- l'équation $xa = b$ d'inconnue $x \in G$ possède pour unique solution $x = ba^{-1}$.

Attention : il se peut qu'une loi soit non commutative et donc a priori $a^{-1}b \neq ba^{-1}$ (notamment pour les matrices).

2.4 Sous-groupes**Définition 10.9**

Soit E un ensemble muni d'une l.c.i. \top . Une partie $F \subset E$ est dite stable (par \top) si : $\forall x, y \in F \quad x \top y \in F$.

Dans ce cas, la l.c.i. \top définie sur $E \times E$ peut être restreinte à $F \times F$: on obtient alors une l.c.i. sur F :

$$\begin{aligned} \top' : F \times F &\rightarrow F \\ (x, y) &\mapsto x \top y \end{aligned}$$

qui est appelée la loi induite (par \top) sur F . Très souvent, on la note encore \top bien qu'il y ait ambiguïté.

Définition 10.10

Soit (G, \top) un groupe et $H \subset G$. On dit que H est un sous-groupe de G si H est une partie stable par \top et que, si on note \top' la loi induite sur H , alors (H, \top') est un groupe.

Autrement dit, pour que H soit un sous-groupe de G , il faut vérifier que H muni de \top' vérifie les propriétés **G1.** à **G4.**, à savoir : \top' doit être une l.c.i. sur H , \top' doit être associative, H doit avoir un élément neutre pour \top' , et tout élément de H doit avoir un symétrique pour \top' .

Cela fait beaucoup à vérifier. En pratique, on utilise systématiquement les caractérisations qui suivent :

Proposition 10.11

Soit (G, \cdot) un groupe (notation multiplicative). Une partie $H \subset G$ est un sous-groupe si et seulement si :

1. $H \neq \emptyset$
2. H est stable par la l.c.i. \cdot : $\forall x, y \in H \quad xy \in H$
3. H est stable par passage au symétrique : $\forall x \in H \quad x^{-1} \in H$

Si on utilise pour la loi de G la notation additive (loi $+$), les assertions 2 et 3 se réécrivent :

1. $\forall x, y \in H \quad x + y \in H$
2. $\forall x \in H \quad -x \in H$

Exemple 10. \mathbb{Z} et \mathbb{Q} sont des sous-groupes de $(\mathbb{R}, +)$.

\mathbb{N} n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car $1 \in \mathbb{N}$ mais $-1 \notin \mathbb{N}$.

\mathbb{Q}^* est un sous-groupes de (\mathbb{R}^*, \times) , mais par \mathbb{Z}^* (assertion 3 non vérifiée : $x = 2 \in \mathbb{Z}$ mais $2^{-1} \notin \mathbb{Z}$).

\mathbb{R}_+^* est un sous-groupe de (\mathbb{R}^*, \times) .

On peut condenser les assertions 2 et 3 de la propriété ci-dessus en une seule :

Proposition 10.12

Soit (G, \cdot) un groupe (notation multiplicative). Une partie $H \subset G$ est un sous-groupe si et seulement si :

1. $H \neq \emptyset$
2. $\forall x, y \in H \quad xy^{-1} \in H$ (en notation additive : $\forall x, y \in H \quad x - y \in H$).

Exemple 11. Soit G un groupe d'élément neutre e . Alors $\{e\}$ et G sont des sous-groupes de G .

Proposition 10.13

Soit G un groupe d'élément neutre e . Si H est un sous-groupe de G , alors nécessairement $e \in H$.

De plus, $\{e\}$ est un sous-groupe de G , dit sous-groupe trivial.

Démonstration. Si H est un sous-groupe de E , alors $H \neq \emptyset$, donc il existe $x \in H$. Alors (en prenant $y = x$ dans l'assertion 2), on a $e = xx^{-1} \in H$.

Montrons la deuxième assertion. Il est clair que $\{e\} \neq \emptyset$. Soit $x, y \in \{e\}$. Alors $x = y = e$ si bien que $xy^{-1} = ee^{-1} = e \in \{e\}$. Ainsi, $\{e\}$ est un sous-groupe de G . \square

Remarque. C'est en général le moyen le plus rapide de justifier que $H \neq \emptyset$: il suffit de vérifier que $e \in H$.

Exemple 12. Montrer que \mathbb{U} est un sous-groupe de (\mathbb{C}^*, \times) .

2.5 Morphismes de groupes

Définition 10.14 (Morphisme de groupes)

Soit (G, \top) et (G', \perp) deux groupes, et $f : G \rightarrow G'$ une application. On dit que f est un morphisme (de groupes) si

$$\forall x, y \in G \quad f(x \top y) = f(x) \perp f(y)$$

On peut également dire que f est un morphisme de (G, \top) dans (G', \perp) : ceci permet de préciser quelles sont les l.c.i. de G et de G' pour lesquelles f est un morphisme de groupes. Il arrive parfois qu'on omette les lois \top et \perp et qu'on écrive : “ f est un morphisme de G dans G' ”.

Définition 10.15

Soit (G, \top) et (G', \perp) deux groupes.

- Si $f : G \rightarrow G'$ est un morphisme de groupes et f est bijective, on dit que f est un isomorphisme (de groupes).
- Si f est un morphisme de (G, \top) dans (G, \top) , on dit que f est un endomorphisme (de G).
- Si f est un isomorphisme et un endomorphisme (de G), on dit que f est un automorphisme (de G).

Exemple 13. Montrer que les fonctions suivantes sont des morphismes de groupes. Sont-ce des isomorphismes ? Des endomorphismes ? Des automorphismes ?

$$f : (\mathbb{Z}, +) \rightarrow (\mathbb{R}_+^*, \times) \\ n \mapsto 2^n$$

$$g : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +) \\ x \mapsto \ln x$$

$$h : (\mathbb{C}, +) \rightarrow (\mathbb{C}, +) \\ z \mapsto \bar{z}$$

Proposition 10.16

Soit G, G' deux groupes d'éléments neutres respectifs e, e' . Soit $f : G \rightarrow G'$ un morphisme de groupes. Avec la notation multiplicative :

1. $f(e) = e'$
2. $\forall x \in G \quad f(x^{-1}) = f(x)^{-1}$
3. $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = f(x)^n$

Démonstration. On ne prouve que les deux premières assertions, la troisième étant une récurrence immédiate.

□

Exemple 14. L'application $\ln : (\mathbb{R}_+^*, \times) \rightarrow (\mathbb{R}, +)$ est un morphisme de groupes donc

- 1.
- 2.
- 3.

2.6 Noyau et image d'un morphisme

Proposition 10.17

Soit G, G' deux groupes et $f : G \rightarrow G'$ un morphisme de groupes. Alors

- Si H est un sous-groupe de G , alors $f(H)$ est un sous-groupe de G' .
- Si H' est un sous-groupe de G' , alors $f^{-1}(H')$ est un sous-groupe de G .

Pour rappel :

$$f(H) := \{f(x) \mid x \in H\} \subset G'$$
$$f^{-1}(H') := \{x \in G \mid f(x) \in H'\} \subset G$$

Démonstration.

□

Définition 10.18 (Noyau)

Soit G, G' deux groupes d'éléments neutres respectifs e, e' . Soit $f : G \rightarrow G'$ un morphisme de groupes. On appelle noyau de f , noté $\text{Ker} f$, l'ensemble

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

Proposition 10.19

Avec les mêmes notations que la définition :

1. $\text{Ker} f$ est un sous-groupe de G .
2. $\text{Ker} f = \{e\}$ si et seulement si f est injective.

Démonstration. Montrons la première assertion : $\{e'\}$ est un sous-groupe de G' , donc $f^{-1}(\{e'\}) = \text{Ker } f$ est un sous-groupe de G par la proposition 10.17.

Montrons la seconde assertion. Sens réciproque : supposons f injective. Comme $f(e) = e'$, il est clair que $e \in \text{Ker } f$. Montrons l'autre inclusion, à savoir $\text{Ker } f \subset \{e\}$. Soit $x \in \text{Ker } f$. Alors $f(x) = e' = f(e)$ et comme f est injective, $x = e$. Ainsi, $x \in \{e\}$ et on a bien l'inclusion recherchée. D'où $\text{Ker } f = \{e\}$.

Sens direct : supposons $\text{Ker } f = \{e\}$ et montrons que f est injective. Soit $x, y \in G$ tels que $f(x) = f(y)$. Alors :

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

et comme f est un morphisme, $f(xy^{-1}) = e'$. Ainsi, $xy^{-1} \in \text{Ker } f = \{e\}$. Donc, $xy^{-1} = e$, ou encore $x = y$. Donc (par arbitraire sur x, y), f est injective. \square

Exemple 15. L'application

$$\begin{aligned} f : (\mathbb{R}, +) &\rightarrow (\mathbb{C}^*, \times) \\ x &\mapsto e^{ix} \end{aligned}$$

est un morphisme de groupes, dont le noyau est

Définition 10.20 (Image)

Soit G, G' deux groupes d'éléments neutres respectifs e, e' . Soit $f : G \rightarrow G'$ un morphisme de groupes. On appelle image de f , noté $\text{Im } f$, l'ensemble

$$\text{Im } f := \{f(x) \mid x \in G\} = f(G)$$

Proposition 10.21

Avec les mêmes notations que la définition :

1. $\text{Im } f$ est un sous-groupe de G' .
2. $\text{Im } f = G'$ si et seulement si f est surjectif.

Démonstration. Montrons la première assertion : $f(G)$ est un sous-groupe de G' , donc $f(G)$ est un sous-groupe de G' par la proposition 10.17.

La seconde assertion est tautologique : $\text{Im } f = f(G)$ et on a vu au chapitre 4 que $f(G) = G'$ si et seulement si f est surjective. \square

Exemple 16. Le morphisme de groupes

$$\begin{aligned} f : (\mathbb{R}, +) &\rightarrow (\mathbb{C}^*, \times) \\ x &\mapsto e^{ix} \end{aligned}$$

a pour image

2.7 Groupe produit

Proposition 10.22 (Groupe produit)

Soit (G, \top) et (H, \perp) deux groupes. On peut définir une l.c.i. $*$ sur $G \times H$, dite loi produit :

$$\forall (x, y), (x', y') \in (G \times H)^2 \quad (x, y) * (x', y') = (x \top x', y \perp y')$$

Dans ce cas, $(G \times H, *)$ est un groupe, dit groupe produit de G et H .

Son élément neutre est (e_G, e_H) , où e_G, e_H sont les éléments neutre de G, H respectivement.

Si $(x, y) \in G \times H$, alors, en notation multiplicative : $(x, y)^{-1} = (x^{-1}, y^{-1})$.

Enfin, si G, H sont abéliens, alors $G \times H$ l'est aussi.

Attention, il n'y a pas de notation dédiée pour la loi produit : on peut la noter $*$, \times , ou encore \otimes ...

Démonstration. Il est clair que $*$ est une l.c.i. sur $G \times H$. On peut vérifier (mais c'est fastidieux) que $*$ est associative. Montrons que $G \times H$ vérifie **G3.** et **G4.**

□

Exemple 17. $(\mathbb{R}, +)$ et (\mathbb{R}^*, \times) sont des groupes donc on peut munir $\mathbb{R} \times \mathbb{R}^*$ de la loi produit

$$(x, y) \otimes (x', y') := (x + x', yy')$$

Dans ce cas, l'élément neutre est $(0, 1)$ et le symétrique d'un élément (x, y) est $(-x, y^{-1})$.

3 Anneaux

3.1 Anneau

Définition 10.23 (Monoïde, hors programme)

Soit M un ensemble. On dit que (M, \top) est un monoïde si :

M1. \top est une l.c.i. sur M .

M2. \top est associative : $\forall a, b, c \in M \quad a \top (b \top c) = (a \top b) \top c$.

M3. M possède un élément neutre (pour \top) : $\exists e \in M \quad \forall a \in G \quad a \top e = e \top a = a$.

Autrement dit, un monoïde vérifie les mêmes propriétés qu'un groupe sauf qu'un élément n'a pas besoin d'être symétrisable.

Exemple 18. (\mathbb{Z}, \times) , (\mathbb{Q}, \times) , (\mathbb{R}, \times) et (\mathbb{C}, \times) sont des monoïdes.

Si X est un ensemble, $(\mathcal{P}(X), \cap)$ et $(\mathcal{P}(X), \cup)$ sont des monoïdes, d'éléments neutres respectifs ... et ...

Définition 10.24 (Anneau)

Soit A un ensemble. On dit que $(A, +, \times)$ est un anneau si :

A1. $(A, +)$ est un groupe abélien.

A2. (A, \times) est un monoïde. (donc \times est une l.c.i. associative sur A , et A possède un élément neutre pour \times)

A3. \times est distributive par rapport à $+$, c'est-à-dire :

$$\forall a, b, c \in A \quad a(b + c) = ab + ac \quad \text{et} \quad (b + c)a = ba + ca$$

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

Notation. L'élément neutre pour $+$ est noté 0_A et appelé élément nul.

L'élément neutre pour \times est noté 1_A et appelé élément unité.

Attention ! Dans un anneau A , un élément $x \in A$ n'est pas nécessairement inversible (i.e. symétrisable par rapport à \times). L'expression x^{-1} n'a donc pas toujours de sens. Par contre, l'opposé de x , à savoir $-x$, existe toujours car $(A, +)$ est un groupe.

Exemple 19. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.

L'ensemble des suites réelles $(\mathbb{R}^{\mathbb{N}}, +, \times)$ est un anneau commutatif. Son élément nul est la suite de terme général $u_n = 0$, son élément unité est la suite de terme général $u_n = 1$.

L'ensemble des fonctions réelles de la variable réelle $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau commutatif. Son élément nul est la fonction $x \mapsto 0$, son élément unité est la fonction $x \mapsto 1$.

Remarque. Très souvent, les anneaux qu'on étudiera auront pour l.c.i. les lois $+$ et \times usuelles. Mais la notion d'anneau se généralise à des l.c.i. quelconques \top et \perp : (A, \top, \perp) est un anneau si (A, \top) est un groupe abélien, (A, \perp) est un monoïde et \perp est distributive sur \top , càd

$$\forall a, b, c \in A \quad a \perp (b \top c) = (a \perp b) \top (a \perp c) \quad \text{et} \quad (b \top c) \perp a = (b \perp a) \top (c \perp a)$$

3.2 Sous-anneau

On rappelle que la notion de sous-ensemble stable par l.c.i. et de loi induite a été vue à la définition 10.9.

Définition 10.25

Soit $(A, +, \times)$ un anneau. Une partie $B \subset A$ est dite un sous-anneau de A si B est stable par les l.c.i. $+$ et \times , et que $(B, +', \times')$ est un anneau, où $+', \times'$ sont les lois induites par $+, \times$ sur B .

Pour vérifier que $(B, +', \times')$ est un anneau, il faudrait donc vérifier les propriétés **A1.** à **A3.**. En pratique, on utilise la caractérisation suivante :

Proposition 10.26

Soit $(A, +, \times)$ un anneau. Une partie $B \subset A$ est un sous-anneau de A si et seulement si :

1. $1_A \in B$
2. $\forall x, y \in B \quad x - y \in B$ (les lois induites par $+$ et \times sur B sont encore notées $+$ et \times)
3. $\forall x, y \in B \quad xy \in B$

Démonstration. On vérifie que les assertions **A1.** à **A3.** sont vraies pour B .

- Il faut enfin montrer que, sur B , \times est distributive sur $+$, c'est-à-dire :

$$\forall x, y, z \in B \quad x(y+z) = xy + xz \quad \text{et} \quad (y+z)x = yx + zx$$

mais cela est évident car $x, y, z \in A$ et que A est un anneau. □

Exemple 20. \mathbb{Z} est un sous-anneau de $(\mathbb{R}, +, \times)$. \mathbb{D} est un sous-anneau de $(\mathbb{Q}, +, \times)$.

L'ensemble des suites convergentes est un sous-anneau de $(\mathbb{R}^{\mathbb{N}}, +, \times)$.

L'ensemble des fonctions polynômiales est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$.