

Algèbre

Étienne Fouvry

6 février 2016

Première partie

Groupe, anneaux, idéaux, corps.

I.1 Groupe

Définition 1 (Loi de composition interne). *Est appelée loi de composition interne toute application φ :*

$$\begin{aligned}\varphi : X \times X &\rightarrow X \\ (x, y) &\mapsto \varphi(x, y)\end{aligned}$$

On insère souvent un symbole à la place de φ :

$$\varphi(x, y) = x * y \in X$$

L'addition usuelle est une loi de composition interne dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}^k$.

La composition (\circ) est une loi de composition interne sur $\mathcal{F}(E, E)$.

Soit $X = \mathcal{P}(E)$. L'union (\cup), l'intersection (\cap) sont des lois de composition interne.

Le produit scalaire $a.b := \begin{cases} (\mathbb{K}^n)^2 \rightarrow \mathbb{K} \\ (a, b) \mapsto \sum_{i=0}^n a_i b_i \end{cases}$ n'est pas une loi de composition interne.

Définition 2 (Groupe). *Soit G un ensemble muni d'une loi de composition interne $*$.*

*On dit que $(G, *)$ est un groupe si :*

- $*$ admet un élément neutre
- $*$ est associative

— Pour tout élément de G il en existe un inverse pour $*$.

$(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +), (\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times), (\{\pm 1\}, \times)$ sont tous des groupes, mais (\mathbb{Z}^*, \times) n'en est pas un.

0 n'a jamais d'inverse.

$(\mathcal{B}(E) = \{\text{bijections de } E\}, \circ)$ est un groupe.

$(\mathbb{D}, +)$ est un groupe additif. $(\mathbb{D} \setminus \{0\}, \times)$ n'en est pas un.

Définition 3 (Commutativité). $*$ sur X non vide est dite commutative si

$$\forall x, y \in X, x * y = y * x$$

Définition 4 (Groupe abélien). Un groupe $(G, *)$ où $*$ est commutative est dit groupe commutatif ou groupe abélien.

$(\mathcal{GL}(\mathbb{R}^2), \circ)$ est non abélien.

Notation additive Lors qu'un groupe $(E, +)$ est abélien, alors il est usuel de noter son élément neutre 0 et les inverses $-x$.

Définition 5 (Sous-groupe). Soit $(G, *)$ un groupe, $H \subseteq G$, $H \neq \emptyset$.

$(H, *)$ est un sous-groupe de G si $*$ est interne à H et $(H, *)$ est un groupe.

$(\mathbb{Z}, +)$ est un sous-groupe $(\mathbb{C}, +)$.

Caractérisation Soit $(G, *)$ un groupe, $H \subseteq G$, $H \neq \emptyset$. Alors $(H, *)$ est un sous-groupe si $\begin{cases} \forall x, y \in H, x * y \in H \\ \forall x \in H, x^{-1} \in H \end{cases}$ ou $\forall x, y \in H, xy^{-1} \in H$.

Proposition 1 (Unicité de l'élément neutre). Soit $(G, *)$ un groupe. Alors il existe un unique élément neutre e .

Démonstration.

$$\begin{aligned} & \forall x \in G : x * e = e * x = e' * x = x * e' = x \\ & \begin{cases} xe = xe' \\ ex = e'x \end{cases} \iff x^{-1}xe = x^{-1}xe' \iff e = e' \end{aligned}$$

□

Proposition 2 (Unicité de l'inverse). Soit $(G, *)$ un groupe. Alors $\forall x \in G, \exists ! x^{-1} : x * x^{-1} = x^{-1} * x = e$.

Définition 6 (Groupe produit). Soient $(G, *)$, $(G', *)'$ deux groupes.

Alors on définit le groupe produit par : $(G \times G', * \times *' = \square)$

I.1.1 Morphisme de groupes

Définition 7. Soient $(G, *)$, $(G', *')$ deux groupes.

On appelle morphisme de $(G, *)$ dans $(G', *')$ une application $\varphi : G \rightarrow G'$ telle que

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

On a alors $\varphi(1_G) = 1_{G'}$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$.

I.2 Anneaux

Définition 8 (Anneau). Soit A un ensemble non vide muni de deux lois de composition $+$ et $*$.

On dit que $(A, +, *)$ est un anneau si :

- $(A, +)$ est un groupe abélien
- $*$ est associative
- $*$ est distributive par rapport à $+$
- Il existe un élément neutre pour $*$

$(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$ sont des anneaux, $(\mathcal{M}_n, +, \times)$ aussi, mais non commutatif.

Définition 9 (Sous-anneau). Soit $(A, +, *)$ un anneau.

On dit que $(B, +, *)$ est un anneau si :

- $\emptyset \neq B \subseteq A$
- $(B, +)$ est un sous-groupe additif
- B est laissé stable par $*$
- $e_A \in B$

Définition 10 (Corps). Un anneau $(A, +, *)$ est un corps si :

- $\#A > 2$
- $\forall x \in A \setminus \{0_+\}, \exists x^{-1}$ pour $*$

Définition 11 (Intégrité). Un anneau $(A, +, *)$ est intègre si $x * y = 0 \iff x = 0 \vee y = 0$.