Groupes, anneaux et corps

Marc CHEVALIER
DI ENS
sur une idée originale de Jérôme FERET

2018-2019

1 Groupes

Définition 1

Un groupe est une paire $(G, \times)$ telle que G soit un ensemble, et $\times$ soit une loi interne associative sur G qui admet un élément neutre, et telle que tout élément de x soit inversible.

Proposition 1

Un groupe est non vide.

Démonstration. En effet, il possède un élément neutre. □

Définition 2

Un groupe $(G, +)$ est dit abélien (ou commutatif), si la loi $+$ est commutative.

Notation 1

Lorsque $(G, +)$ est un groupe abélien, l'élément neutre est souvent noté 0_G et l'inverse d'un élément x est noté $-x$.

Exemple 1

Un ensemble à un élément, x, est un groupe abélien pour la loi $+$ définie par $x + x := x$.

Démonstration.

1. $+$ est associative.
2. $+$ est commutative.
3. x est un élément neutre car pour tout $y \in \{x\}$, on a : $y = x$, puis $y + x = x$ (par définition de $+$), d'où $y + x = x$.
4. x est inversible et son inverse est x, car $x + x = x$ (et x est l'élément neutre).

□

Exemple 2

Aucune des paires $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, ou $(\mathbb{R}, \cdot)$ n'est un groupe.

Exemple 3

Les paires $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sont des groupes abéliens.

Exemple 4

Soit $n \in \mathbb{N}^*$ un entier strictement positif. Soit $(\mathbb{Z}/n\mathbb{Z}, +)$ l'ensemble des entiers entre 0 et $n-1$ muni de l'addition modulo n, est un groupe. L'élément neutre est 0. De plus, pour tout entier $i \in \mathbb{N}$ tel que $0 \leq i < n$, l'inverse de i est $n - i$.

Exemple 5

Si A est un ensemble avec un ou deux éléments. La paire $(Bij(A), \circ)$, où $Bij(A)$ est l'ensemble des bijections de A dans A, est un groupe abélien.

Exemple 6

Si A est un ensemble avec au moins trois éléments. La paire $(Bij(A), \circ)$, où $Bij(A)$ est l'ensemble des bijections de A dans A est un groupe non abélien.

Démonstration. **(On prouve à la fois les énoncés de l'exemple 1 et de l'exemple 1)**
Soit A un ensemble non vide.

1. La composée de deux bijections est une bijection. Donc $\circ$ est bien une loi interne sur $Bij(A)$.

2. La loi $\circ$ est associative, car pour toute $f, g, h \in Big(A)$, $[f \circ g] \circ h$ et $f \circ [g \circ h]$ sont deux fonctions de A dans A, et, de plus, pour tout $x \in A$.

$$[[f \circ g] \circ h](x) = f(g(h(x)))$$
$$[[f \circ g] \circ h](x) = [f \circ [g \circ h]](x).$$

   Ainsi $[f \circ g] \circ h = f \circ [g \circ h]$.
3. La fonction identité Id_A est un élément neutre.
4. Soit f une bijection de A dans A.
   La fonction g de A dans A qui à $y \in A$ associe l'unique antécédent de y par x est une bijection et $g \circ f = Id_A$ et $f \circ g = Id_A$, donc f est inversible et son inverse est g.
5. Supposons que A soit un singleton.
   Alors l'ensemble $Bij(A)$ ne contient que la fonction identité. C'est donc un groupe abélien (Exemple 1).
6. Supposons que A soit un ensemble à deux éléments distincts.
   On les note a et b.
   Il y a deux bijections, la fonction identité Id_A et la fonction σ définie par $\sigma(a) := b$ et $\sigma(b) := a$.
   Soient f et g deux bijections sur A.
   (a) si $f = g$, on a : $f \circ g = g \circ f$.
   (b) sinon, on peut supposer que $f = Id_A$ et $g = \sigma$,
   puis
   $$f \circ g = Id_A \circ \sigma$$
   $$f \circ g = \sigma$$
   $$f \circ g = \sigma \circ Id_A$$
   $$f \circ g = g \circ f$$
7. Supposons que A soit un ensemble avec au moins trois éléments.
   Notons a,b,c trois éléments distincts de A.
   Nous notons :

$$f : \begin{cases} A \to A \\ a \mapsto b \\ b \mapsto a \\ x \mapsto x \quad \text{si } x \notin \{a, b\} \end{cases} \qquad g : \begin{cases} A \to A \\ a \mapsto c \\ c \mapsto a \\ x \mapsto x \quad \text{si } x \notin \{a, b\} \end{cases}$$

f et g sont bien des bijections de A dans A.
De plus,

$$\begin{aligned}[f \circ g](a) &= f(g(a)) \\ [f \circ g](a) &= f(c) \\ [f \circ g](a) &= c.\end{aligned}$$

Et :

$$\begin{aligned}[g \circ f](a) &= g(f(a)) \\ [g \circ f](a) &= g(b) \\ [g \circ f](a) &= b.\end{aligned}$$

Or, $c \neq b$.
D'où, $f \circ g \neq g \circ f$.
Puis $\circ$ n'est pas commutative sur $Bij(A)$.

□

Proposition 2

Si $(G, \times)$ est un groupe d'élément neutre ε_G et tel que pour tout $x \in G$, $x \times x = \varepsilon_G$, alors $(G, \times)$ est abélien.

Démonstration. Si $(G, \times)$ est un groupe d'élément neutre ε_G et tel que pour tout $x \in G$, $x \times x = \varepsilon_G$.

1. Soit $x \in G$.
   On a $\underline{x} \times x = \varepsilon_G$ et $x \times \underline{x} = \varepsilon_G$. Donc $x^{-1} = x$.
2. Soient x et y deux éléments de G.

   — Par le point précédent, $(x \times y)^{-1} = x \times y$.

   — De plus, $(x \times y)^{-1} = y^{-1} \times x^{-1}$.
   Or par le point précédent, $x^{-1} = x$ et $y^{-1} = y$.
   Ainsi, $(x \times y)^{-1} = y \times x$.

D'où, $x \times y = y \times x$.

□

2 Anneaux

Définition 3

Un groupe est un triplet $(A, +, \times)$ tel que :
- $(A, +)$ est un groupe abélien,
- $\forall (a, b, c) \in A^3$,
  - $(a \times b) \times c = a \times (b \times c)$ ($\times$ est associative),
  - $a \times (b + c) = a \times b + a \times c$ ($\times$ est distributive à gauche par rapport à $+$),
  - $(b + c) \times a = b \times a + c \times a$ ($\times$ est distributive à droite par rapport à $+$),
- Il existe un élément $e_\times \in A$ qui est l'élément neutre (à gauche et à droite) de la loi $\times$ (aussi appelée élément unité). C'est à dire : $\forall a \in A, a \times e_\times = e_\times \times a = a$

L'élément unité est généralement noté 1_A ou 1 s'il n'y a pas d'ambiguïté, par analogique avec la loi de multiplication usuelle sur les réels. Pareillement, l'élément neutre pour $(A, +)$ est souvent noté 0_A ou 0 et est appelé élément nul.

Cependant, $(A, \times)$ n'est pas un groupe : il n'y a pas toujours d'inverse. On parle de monoïde.

Définition 4

Un anneau $(A, +, \times)$ est dit abélien (ou commutatif), si la loi $\times$ est commutative.

Attention ! Dans un anneau, $+$ est toujours commutative.

Exemple 7

Les triplets suivants sont des anneaux :
- $(\mathbb{Z}, +, \times)$
- L'ensemble à un seul élément $\{0\}$ muni des opérations $0 + 0 = 0$ et $0 \times 0 = 0$ est un anneau commutatif, appelé anneau nul, ou anneau trivial.
- L'ensemble des nombres de $[\![0, n-1]\!]$ avec les opérations $+$ et $\times$ modulo $n \in \mathbb{N}^*$. On note cet anneau $\mathbb{Z}/n\mathbb{Z}$.

3 Corps

Définition 5

Un coprs est un triplet $(K, +, \times)$ tel que :
- $(K, +, \times)$ est un anneau,
- $\forall x \in K \setminus \{0_K\}, \exists y \in K : x \times y = y \times x = 1_K$ (la loi $\times$ admet un inverse)

Les corps sont souvent notés $\mathbb{K}$.

L'inverse d'un élément x pour la loi $+$ est souvent notée $-x$ et pour la loi $\times$, x^{-1} ou $\frac{1}{x}$.

Dans la suite, on se donne un corps $(K, +, \times)$.

Proposition 3

$$\forall x \in K, 0 \times x = x \times 0 = 0$$

On dit que 0 est absorbant pour la loi $\times$.

Démonstration. Soit $x \in K$. On a

$$\begin{aligned} 0 \times x &= (0+0) \times x \text{ car } 0 \text{ est neutre pour } + \\ &= 0 \times x + 0 \times x \text{ par distributivité} \end{aligned}$$

On peut ajouter $-0 \times x$ de chaque côté. On a alors :

$$\begin{aligned} 0 \times x - 0 \times x &= 0 \times x + 0 \times x - 0 \times x \\ 0 &= 0 \times x \end{aligned}$$

Même démonstration pour $x \times 0$. □

Exemple 8

Les triplets suivants sont des corps :
- $(\mathbb{Q}, +, \times)$
- $(\mathbb{R}, +, \times)$
- $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Mais ne sont pas des corps :
- $(\mathbb{Z}, +, \times)$. En Effet, 2 n'a pas d'inverse pour $\times$ dans $\mathbb{Z}$.
- $\mathbb{Z}/n\mathbb{Z}$ n'est un corps si et seulement si n est composé (non premier).