# Reconnaitre un groupe, un anneau ou un corps par les axiomes


## Quand on ne sait pas !

- On appelle groupe tout couple $(G, \star)$ où $G$ est un ensemble et $\star$ est une loi de composition interne telle que
  — La loi est associative
  — Il existe un élément $e$ appelé élément neutre de $G$ tel que pour tout $x$ de $G$,
  $$x \star e = e \star x = x$$
  — Pour tout élément $x$, il existe un élément $y$ tel que $x \star y = y \star x = e$.
  L'élément $y$ est le symétrique de $x$

  Si de plus, la loi $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif ou un groupe abélien.
- On appelle anneau tout triplet $(A, +, \times)$ où $A$ est un ensemble et $+$ et $\times$ des lois de composition internes telles que
  — $(A, +)$ soit un groupe abélien dont le neutre se note $0_A$ et s'appelle l'élément nul.
  — La loi $\times$ est associative
  — Il existe un élément $1_A$ tel que pour tout $x \in A$, $1_A \times x = x \times 1_A = x$
  — La multiplication est distributive par rapport à l'addition, c'est-à-dire :
  $$\forall (x, y, z) \in A^3, x \times (y + z) = (x \times y) + (x \times z) \text{ et } (y + z) \times x = (y \times x) + (z \times x)$$

  Si $(A, +, \times)$ est un anneau et que la loi $\times$ est commutative, on dit que c'est un anneau commutatif.
- On appelle corps tout anneau commutatif $(A, +, \times)$ tel que tout élément non nul $x$ de $A$ admette un inverse, c'est-à-dire, un élément $y$ tel que $x \times y = 1_A$.

## Que faire ?

- Quand on veut démontrer que $(G, \star)$ (ou $(A, +, \times)$) est un groupe (ou un anneau), la meilleure méthode est de démontrer que c'est un sous-groupe (ou un sous-anneau) d'un groupe (ou anneau) connu. Cela sera abordé dans la fiche 3.

- Pour montrer, en revenant aux axiomes que $(G, \star)$ est un groupe, il faut vérifier que la loi est associative (ce qui est souvent assez formel), trouver l'élément neutre de la loi et, pour tout élément $x$ exhiber son symétrique.

  **EXEMPLE 1** Rappelons un exemple du cours. On veut montrer que si $X$ est un ensemble, l'ensemble $S_X$ des bijections de $X$ dans $X$ est un groupe pour la composition.

  — On vérifie que la loi $\circ$ est une loi interne de $S_X$. En effet si $f$ et $g$ sont des bijections de $X$ dans $X$ alors $f \circ g$ aussi.

  — La loi $\circ$ est associative. En effet si $f, g$ et $h$ appartiennent à $S_X$,

  $$f \circ (g \circ h) = (f \circ g) \circ h$$

  — La fonction identité de $X$ notée $\iota : X \to X$ est un élément neutre pour $\circ$ car, pour tout $x \in X$,

  $$(f \circ \iota)(x) = f(\iota(x)) = f(x) \text{ et } (\iota \circ f)(x) = \iota(f(x)) = f(x)$$

  — Toute fonction $f$ de $S_X$ admet un symétrique puisque, comme $f$ est bijective, il existe une fonction $g$, elle même bijective vérifiant $f \circ g = g \circ f = \iota$. Il suffit de prendre pour $g$ la bijection réciproque de $f$.

  On a bien montré que $(S_X, \circ)$ était un groupe. Notons que ce n'est pas un groupe abélien sauf si $X$ a strictement moins de 3 éléments.

## Conseils

Dans le cas des groupes, il ne faut pas se mélanger entre les notations additives et les notations multiplicatives. Plus précisément :

- quand on note un groupe additivement (le plus souvent dans le cas des groupe abéliens), l'élément neutre est noté $0$ et le symétrique de $x$, que l'on appelle l'opposé se note $-x$. C'est le cas par exemple du groupe $(\mathbb{Z}, +)$.
- quand on note un groupe multiplicativement, l'élément neutre est noté $1$ et le symétrique de $x$, que l'on appelle l'inverse se note $x^{-1}$. C'est le cas par exemple du groupe $(\mathrm{GL}_n(\mathbb{K}), \times)$.

## Exemple traité

On considère l'opération $\top$ sur $X = \mathbb{R} \setminus \{-1\}$ définie par

$$\forall (x, y) \in X^2, x \top y = x + y + xy$$

**1** Montrer que pour tout $(x, y)$ dans $X^2$, $x \top y = (1 + x)(1 + y) - 1$.

**2** Montrer que $(\mathbb{R}, \top)$ est un groupe.

### SOLUTION

**1** Soit $x, y$ dans $X$, $(1+x)(1+y) = 1+x+y+xy = 1+x\top y$. La relation voulue s'en déduit.

**2** Montrons les axiomes des groupes.

- On commence par remarquer que la loi $\top$ est une loi interne à $X$. En effet si $x$ et $y$ appartiennent à $X$ alors $(1+x) \neq 0$ et $(1+y) \neq 0$ donc $(1+x)(1+y) \neq 0$ et de ce fait, $x\top y \neq -1$.
- Montrons que la loi $\top$ est associative. Soit $x, y$ et $z$ dans $X$, en utilisant le calcul précédent,

$$\begin{array}{rcl} (x\top y)\top z & = & (1+x\top y)(1+z)-1 \\ & = & (1+x)(1+y)(1+z)-1 \\ & = & (1+x)(1+y\top z)-1 \\ & = & x\top(y\top z) \end{array}$$

  La loi est bien associative
- On remarque que $0$ est un élément neutre pour $\top$ car pour tout $x \in X$,

$$x\top 0 = 0\top x = x$$

- Pour $x \in X$, on cherche $y \in X$ tel que $x\top y = 0$. On est ramené à résoudre (en $y$) l'équation $x+y+xy = 0$. Elle est équivalente à $(1+x)y = -x$. Comme $x$ est supposé dans $X$, $1+x \neq 0$ et ainsi l'unique solution est $y = -\frac{x}{1+x}$ qui appartient bien à $X$ car $x \neq 1+x$. On vérifie de plus que, en posant $y = -\frac{x}{1+x}$, $y\top x = 0$. Finalement $y = -\frac{x}{1+x}$ est le symétrique de $x$ pour la loi $\top$.

On a bien montré tous les axiomes du groupe donc $(X, \top)$ est un groupe (qui est abélien).

## Exercices

**EXERCICE 1.1** Soit $A$ un ensemble, on considère $P = \mathcal{P}(A)$ l'ensemble des parties de l'ensemble $A$. Pour toutes parties $X$ et $Y$ de $A$, on appelle différence symétrique de $X$ et $Y$ et on note $X\Delta Y$ l'ensemble $(X \cup Y) \setminus (X \cap Y)$.
Si $X$ est une partie de $A$, on note $1_X$ la fonction caractéristique de $X$ :

$$\begin{array}{rrcc} 1_X : & A & \mapsto & \{0,1\} \\ & x & \mapsto & \left\{\begin{array}{ll} 1 & \text{si } x \in X \\ 0 & \text{sinon} \end{array}\right. \end{array}$$

On pourra utiliser le fait que pour deux parties $X$ et $Y$ de $A$, $X = Y$ si et seulement si $1_X = 1_Y$.

**1** Soit $X$ et $Y$ dans $P$. Montrer que $1_{X\Delta Y} = 1_X + 1_Y - 2 \times 1_X 1_Y$.
**2** En déduire que $(P, \Delta)$ est un groupe abélien.
**3** Soit $X$ et $Y$ dans $P$. Montrer que $1_{X\cap Y} = 1_X 1_Y$.
**4** En déduire que $(P, \Delta, \cap)$ est un anneau commutatif.
**5** Montrer que si $A$ n'a pas qu'un seul élément alors $(P, \Delta, \cap)$ n'est pas un corps.

## Pour vous aider à démarrer

**EXERCICE 1.1**

**1** On pourra, pour un élément $x$ de $A$, séparer selon que $x \in A \cap B$, $x \in A \setminus B, \ldots$

**2** Utiliser la question précédente pour montrer l'associativité de $\Delta$.

**3** Faire le calcul.

**4** Utiliser les applications caractéristiques pour montrer la distributivité.

**5** Il suffit de montrer que si $X \neq A$ et $X \neq \varnothing$ alors il n'existe pas $Y$ tel que $X \cap Y$ soit le neutre pour $\cap$.

## Solutions des exercices

**EXERCICE 1.1**

**1** Soit $x \in A$.

- Si $x \in X \cap Y$ (c'est-à-dire que $x$ est dans $X$ et dans $Y$), $1_X(x) = 1_Y(x) = 1$ et donc
$$(1_X + 1_Y - 2 \times 1_X 1_Y)(x) = 1 + 1 - 2 = 0 = 1_{X\Delta Y}(x)$$
En effet, $x$ n'appartient pas à $X\Delta Y$.
- Si $x \in X \setminus Y$ (c'est-à-dire que $x$ est dans $X$ et pas dans $Y$), $1_X(x) = 1$ et $1_Y(x) = 0$ et donc
$$(1_X + 1_Y - 2 \times 1_X 1_Y)(x) = 1 + 0 - 0 = 1 = 1_{X\Delta Y}(x)$$
En effet, $x$ appartient à $X\Delta Y$.
- On traite de même les cas où $x \in Y \setminus X$ et les cas où $x$ n'est ni dans $X$ ni dans $Y$.

**2** Montrons les axiomes des groupes.

- Il est clair que $\Delta$ est une loi interne sur $P$.
- Montrons l'associativité. Soit $(X, Y, Z) \in P^3$.
On veut montrer que $(X\Delta Y)\Delta Z = X\Delta(Y\Delta Z)$. Pour cela, il suffit de montrer que $1_{(X\Delta Y)\Delta Z} = 1_{X\Delta(Y\Delta Z)}$. Or, d'après la question précédente :
$$\begin{aligned}
1_{(X\Delta Y)\Delta Z} &= 1_{X\Delta Y} + 1_Z - 2 \times 1_{X\Delta Y} 1_Z \\
&= 1_X + 1_Y - 2 \times 1_X 1_Y + 1_Z - 2(1_X + 1_X - 2 \times 1_X 1_Y) 1_Z \\
&= 1_X + 1_Y + 1_Z - 2(1_X 1_Y + 1_Y 1_Z + 1_X 1_Z) + 4 \times 1_X 1_Y 1_Z
\end{aligned}$$

Il suffit alors de calculer $1_{X\Delta(Y\Delta Z)}$ et de vérifier que l'on trouve la même expression.

- Comme l'union et l'intersection sont commutatives, la différence symétrique aussi.
- Vérifions que $\varnothing$ est un élément neutre pour $\Delta$. Soit $X \in P$,

$$X\Delta\varnothing = (X \cup \varnothing) \setminus (X \cap \varnothing) = X \setminus \varnothing = X$$

De même, $\varnothing\Delta X = X$ donc $\varnothing$ est bien un élément neutre pour $\Delta$.

- Soit $X \in P$. On cherche son symétrique $Y$ tel que $X\Delta Y = \varnothing$. On remarque que

$$X\Delta X = (X \cup X) \setminus (X \cap X) = X \setminus X = \varnothing$$

On vient donc de voir que le symétrique de $X$ est $X$ lui même.

On a bien montré que $(P, \Delta)$ est un groupe abélien.

**3** Soit $X$ et $Y$ dans $P$ et $x \in A$,

$$x \in X \cap Y \iff x \in X \text{ et } x \in Y \iff 1_X(x) = 1_Y(x) = 1 \iff (1_X 1_Y)(x) = 1$$

Cela prouve que $1_{X\cap Y} = 1_X 1_Y$.

**4** On a déjà vu que $(P, \Delta)$ était un groupe abélien. Montrons les axiomes qui restent.

- On sait que la relation $\cap$ est associative et commutative (on peut aussi le démontrer en utilisant la question précédente).
- La partie $A$ elle même est un élément neutre pour $\cap$ car pour tout $X \in P$,

$$X \cap A = A \cap X = X.$$

- Soit $X, Y$ et $Z$ dans $P$, on veut montrer que $X\Delta(Y \cap Z) = (X\Delta Y) \cap (X\Delta Z)$. Pour cela, on va passer par les applications caractéristiques.

$$\begin{aligned} 1_{X\cap(Y\Delta Z)} &= 1_X 1_{Y\Delta Z} \\ &= 1_X(1_Y + 1_Z - 2 \times 1_Y 1_Z) \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X 1_Y 1_Z \end{aligned}$$

D'autre part

$$\begin{aligned} 1_{(X\cap Y)\Delta(X\cap Z)} &= 1_{X\cap Y} + 1_{X\cap Z} - 2 \times 1_{X\cap Y} 1_{X\cap Z} \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X^2 1_Y 1_Z \\ &= 1_X 1_Y + 1_X 1_Z - 2 \times 1_X 1_Y 1_Z \end{aligned}$$

La dernière égalité venant du fait que $1_X$ étant à valeur dans $\{0, 1\}$, $1_X^2 = 1_X$.

Finalement $(P, \Delta, \cap)$ est bien un anneau commutatif.

**5** Soit $X$ qui n'est ni $A$, ni vide (qui existe bien car $A$ n'a pas qu'un seul élément). Pour tout $Y \in P$, $(X \cap Y) \subset X \subsetneq A$. On en déduit que $(X \cap Y) \neq A$ et donc que $X$ n'est pas inversible dans l'anneau $(P, \Delta, \cap)$. On a exhibé un élément non nul qui n'est pas inversible donc l'anneau considéré n'est pas un corps.

# 2 Montrer qu'une application est un morphisme de groupe ou un morphisme d'anneaux

## Quand on ne sait pas !

- Soit $(G, \star)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un morphisme de groupes si pour tout $(g_1, g_2) \in G^2$, $f(g_1 \star g_2) = f(g_1) \top f(g_2)$.
- Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. Une application $f : A \to A'$ est un morphisme d'anneaux si
  - $\forall (x_1, x_2) \in A^2, f(x_1 + x_2) = f(x_1) + f(x_2)$
  - $\forall (x_1, x_2) \in A^2, f(x_1 \times x_2) = f(x_1) \times f(x_2)$
  - $f(1_A) = f(1_B)$ où $1_A$ est l'élément neutre pour la multiplication de $A$ et $1_B$ l'élément neutre pour celle de $B$.

Un morphisme de groupes (ou d'anneaux) est donc une application qui est compatible avec les opérations des ensembles de départ et d'arrivée.

## Que faire ?

Dans la très grande majorité des cas, aussi bien dans le cas des groupes que dans le cas des anneaux, il suffit juste de vérifier les axiomes de la définition.

**EXEMPLE 1** Soit $n \geq 2$. On considère le groupe $S_n$ des permutations de $n$ éléments. Soit $\sigma$ une permutation de $S_n$, on considère $\varphi : S_n \to S_n$ définie par $\varphi : \tau \mapsto \sigma\tau\sigma^{-1}$. On veut montrer que $\varphi$ est un morphisme de groupes.
Pour tout $(\tau_1, \tau_2) \in S_n^2$,

$$\varphi(\tau_1)\varphi(\tau_2) = \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1} = \sigma\tau_1\tau_2\sigma^{-1} = \varphi(\tau_1\tau_2)$$

On a bien montré que $\varphi$ est un morphisme de groupes.

**EXEMPLE 2** Soit $\mathbb{K}$ un corps et $\mathbb{K}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{K}$.
Soit $\alpha \in \mathbb{K}$, on considère l'application $\varepsilon$ d'évaluation en $\alpha$.

$$\varepsilon : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K} \\ P & \mapsto & P(\alpha) \end{array}$$

On veut vérifier que $\varepsilon_\alpha$ est un morphisme d'anneaux.

- Soit $(P_1, P_2) \in (\mathbb{K}[X])^2$,

$$\varepsilon(P_1 + P_2) = (P_1 + P_2)(\alpha) = P_1(\alpha) + P_2(\alpha) = \varepsilon(P_1) + \varepsilon(P_2)$$

- Soit $(P_1, P_2) \in (\mathbb{K}[X])^2$,

$$\varepsilon(P_1 \times P_2) = (P_1 \times P_2)(\alpha) = P_1(\alpha) \times P_2(\alpha) = \varepsilon(P_1) \times \varepsilon(P_2)$$

- L'unité de $\mathbb{K}[X]$ est le polynôme constant égal à $1_\mathbb{K}$ que l'on va noter $\mathbf{1}$. On a alors,

$$\varepsilon(\mathbf{1}) = \mathbf{1}(\alpha) = 1_\mathbb{K}$$

On a bien montré que $\varepsilon$ était un morphisme d'anneaux.

## Conseils

Il faut faire attention aux opérations des ensembles de départ et d'arrivée. Par exemple le logarithme néperien est un morphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$ car pour tout $x, y$ réels strictement positifs, $\ln(x \times y) = \ln(x) + \ln(y)$.

## Exercices

**EXERCICE 2.1**

On considère les applications $\varphi$ et $\psi$ définies de $\mathbb{Z}$ dans $\mathcal{M}_2(\mathbb{C})$ par

$$\varphi : n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ et } \psi : n \mapsto \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}.$$

**1** **a.** Montrer que pour tout entier relatif $n$, $\varphi(n)$ est inversible.

**b.** Montrer que $\varphi$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathrm{GL}_2(\mathbb{C}), \times)$.

**2** L'application $\psi$ est-elle un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans $(\mathcal{M}_2(\mathbb{C}), +, \times)$ ?

## Pour vous aider à démarrer

**EXERCICE 2.1**

**1** **a.** On pourra, par exemple, calculer le déterminant de $\varphi(n)$ pour $n \in \mathbb{Z}$.

**b.** Vérifier les axiomes d'un morphisme de groupes.

**2** Bien penser à essayer de vérifier tous les axiomes d'un morphisme d'anneaux.

**EXERCICE 2.1**

**1** **a.** Soit $n \in \mathbb{Z}$. On a

$$\det(\varphi(n)) = \begin{vmatrix} 1 & n \\ 0 & 1 \end{vmatrix} = 1 \neq 0$$

On en déduit que $\varphi(n)$ est inversible.

**b.** Soit $n, m$ deux entiers relatifs,

$$\varphi(n) \times \varphi(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} = \varphi(n+m)$$

Cela montre que $\varphi$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(\mathcal{M}_2(\mathbb{C}), \times)$.

**2** Un calcul simple montre que $\psi$ vérifie les deux premiers axiomes des morphismes d'anneaux ; en effet pour $n, m$ deux entiers relatifs

$$\psi(n) + \psi(m) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n+m & 0 \\ 0 & 0 \end{pmatrix} = \psi(n+m)$$

et

$$\psi(n) \times \psi(m) = \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} m & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} nm & 0 \\ 0 & 0 \end{pmatrix} = \psi(nm)$$

Cependant, ce n'est pas un morphisme d'anneaux car $\psi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq I_2$. Donc l'image par $\psi$ du neutre pour la multiplication de $\mathbb{Z}$ n'est pas le neutre pour celle de $\mathcal{M}_2(\mathbb{C})$.