

# GROUPES, ANNEAUX, CORPS

## Table des matières

<b>1</b>	<b>Notion de loi de composition interne</b>	<b>1</b>
1.1	Définition et exemples . . . . .	1
1.2	Propriétés remarquables d’une loi de composition interne . . . . .	2
1.2.1	Associativité . . . . .	2
1.2.2	Élément neutre . . . . .	3
1.2.3	Élément inversible . . . . .	3
1.2.4	Commutativité . . . . .	4
<b>2</b>	<b>Structure de groupe</b>	<b>5</b>
2.1	Définition et exemples . . . . .	5
2.2	Puissances dans un groupe . . . . .	6
2.3	Groupe produit . . . . .	6
2.4	Notion de sous-groupe . . . . .	7
<b>3</b>	<b>Morphismes de groupes</b>	<b>9</b>
3.1	Définition et premières propriétés . . . . .	9
3.2	Noyau d’un morphisme de groupes . . . . .	10
3.3	Image d’un morphisme de groupes . . . . .	11
<b>4</b>	<b>Anneaux et corps</b>	<b>12</b>
4.1	Structure d’anneau . . . . .	12
4.2	Sous-anneau . . . . .	13
4.3	Identités remarquables . . . . .	14
4.4	Structure de corps . . . . .	14
4.5	Morphisme d’anneaux . . . . .	15

## I – Notion de loi de composition interne

Dans toute cette partie,  $E$  désigne un ensemble non vide quelconque.

### 1) Définition et exemples

**Définition** On appelle *loi de composition interne* (en abrégé LCI) sur  $E$  toute application :

$$\star : E \times E \longrightarrow E$$

On dit alors que le couple  $(E, \star)$  est un *magma*.

**Notation :** si  $(x, y) \in E^2$ , l’image  $\star((x, y))$  sera notée  $x \star y$ .

**Exemple** Les applications suivantes sont des lois de composition interne.

★ dans  $\mathbb{N}$  :

$$+ : \begin{cases} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (m, n) & \longmapsto & m + n \end{cases} \quad (\text{addition des entiers naturels})$$

★ la soustraction dans  $\mathbb{Z}$

★ dans  $\mathbb{R}^{\mathbb{R}}$  :

$$\circ : \begin{cases} \mathbb{R}^{\mathbb{R}} \times \mathbb{R}^{\mathbb{R}} & \longrightarrow & \mathbb{R}^{\mathbb{R}} \\ (f, g) & \longmapsto & f \circ g \end{cases} \quad (\text{composition des applications})$$

★ dans  $\mathcal{P}(E)$ , la réunion ou l'intersection

★ La soustraction dans  $\mathbb{N}$  n'est pas une loi de composition interne.

★ La division dans  $\mathbb{R}^*$  est une loi de composition interne.

## 2) Propriétés remarquables d'une loi de composition interne

Une loi de composition interne sur  $E$  doit vérifier les propriétés suivantes pour que le magma  $(E, \star)$  soit suffisamment *intéressant*.

On suppose ici que  $(E, \star)$  est un magma.

### (a) Associativité

**Définition (associativité)** On dit que  $\star$  est *associative* dans  $E$  si :

$$\forall x, y, z \in E, \quad (x \star y) \star z = x \star (y \star z)$$

Le produit  $(x \star y) \star z$  sera alors noté plus simplement  $x \star y \star z$ .

**Exemple** ★ Dans  $\mathbb{Z}$ , les addition  $+$  et multiplication  $\times$  sont des LCI associatives. On peut en effet écrire que :

$$\forall m, n, p \in \mathbb{Z}, \quad (m + n) + p = m + (n + p) \quad \text{et} \quad (mn)p = m(np)$$

★ Dans  $\mathbb{R}^{\mathbb{R}}$ , la LCI  $\circ$  est associative :

$$\forall f, g, h \in \mathbb{R}^{\mathbb{R}}, \quad (f \circ g) \circ h = f \circ (g \circ h)$$

★ Dans  $\mathcal{P}(E)$ , on sait que l'intersection et la réunion sont associatives.

★ Dans  $\mathbb{Z}$ , la différence des entiers «  $-$  » est une loi de composition interne qui n'est pas associative. Par exemple, 1, 2 et 3 sont des entiers relatifs et :

$$(1 - 2) - 3 = -4 \quad \text{tandis que} \quad 1 - (2 - 3) = 2$$

★ De même, la division (qui est une LCI dans  $\mathbb{R}^*$ ) n'est pas associative.

(b) Élément neutre

**Définition (élément neutre)** Soit  $e \in E$ . On dit que  $e$  est un élément neutre pour la loi  $\star$  si :

$$\forall x \in E, \quad x \star e = e \star x = x$$

**Exemple**  $\star$  Dans les sous-ensembles de  $\mathbb{C}$  usuels  $(\mathbb{N}, \mathbb{R}, \mathbb{Z}, \mathbb{Q}, \dots)$ , 1 est un élément neutre pour la multiplication et 0 est le neutre pour l'addition.

- $\star$  Dans  $\mathbb{R}^{\mathbb{R}}$ , l'application  $\text{Id}_{\mathbb{R}}$  est un élément neutre pour la composition.
- $\star$  Dans  $\mathcal{P}(E)$ , l'ensemble vide  $\emptyset$  est un élément neutre pour la réunion, tandis que  $E$  est un élément neutre pour l'intersection.

En effet :

$$\forall \mathcal{P}(E), \quad A \cup \emptyset = \emptyset \cup A = A \quad \text{et} \quad A \cap E = E \cap A = A$$

- $\star$  Dans  $\mathbb{Z}$ , la soustraction n'admet pas d'élément neutre.

Par l'absurde, supposons qu'il existe  $e \in \mathbb{Z}$  tel que :

$$\forall n \in \mathbb{N}, \quad n - e = n \quad \text{et} \quad e - n = n$$

Alors la première égalité ci-dessus (appliquée à  $n$  quelconque dans  $\mathbb{N}$ ) nous donne l'égalité  $e = 0$ . La second égalité appliquée avec  $n = 1 \in \mathbb{Z}$  nous donne l'égalité  $-1 = 1$ , ce qui est absurde.

**Proposition (unicité du neutre)** Si un magma  $(E, \star)$  admet un élément neutre, alors il est unique.

**Démonstration** Soient  $e, e' \in E$  des éléments neutres de  $(E, \star)$ . Montrons que  $e = e'$ .

- $\star$  Comme  $e$  est élément neutre pour  $\star$ , on a  $e \star e' = e'$ .
- $\star$  Comme  $e'$  est élément neutre pour  $\star$ , on a  $e \star e' = e$ .

Donc  $e = e'$ . ■

(c) Élément inversible

**Définition (élément inversible)** On suppose que  $(E, \star)$  admet  $e \in E$  pour élément neutre. Un élément  $x$  de  $E$  est dit *inversible* si :

$$\exists y \in E, \quad x \star y = y \star x = e$$

**Exemple**  $\star$  Dans  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  ou  $\mathbb{C}$  munis de l'addition, tout élément  $x$  est inversible, son inverse étant  $-x$ .

- $\star$  Tout élément  $x$  de  $(\mathbb{R}^*, \times)$  est inversible d'inverse  $\frac{1}{x}$ .
- $\star$  Dans  $\mathbb{N}$  muni de l'addition, le seul élément inversible est 0 (d'inverse 0).
- $\star$  Dans  $\mathbb{R}^{\mathbb{R}}$  muni de la composition, les éléments inversibles sont les applications bijectives.
- $\star$  Dans  $\mathcal{P}(E)$  muni de la réunion, le seul élément inversible est  $\emptyset$ .

On procède par analyse-synthèse.

- $\bullet$  **Analyse** : soit  $A \in \mathcal{P}(E)$ . Supposons que  $A$  soit inversible dans  $(\mathcal{P}(E), \cup)$ . Alors il existe  $B \in \mathcal{B}(E)$  tel que  $A \cup B = \emptyset$ . Comme  $A \subset A \cup B$ , on a  $A \subset \emptyset$ . Or on a aussi l'inclusion  $\emptyset \subset A$  donc, par double inclusion, on conclut que  $A = \emptyset$ .
- $\bullet$  **Synthèse** : l'élément  $\emptyset$  est inversible dans  $(\mathcal{P}(E), \cup)$  car  $\emptyset \cup \emptyset = \emptyset$ .

- $\star$  Dans  $\mathcal{P}(E)$  muni de l'intersection, le seul élément inversible est  $E$ .

**Proposition (propriétés de l'inverse)** Soit  $(E, \star)$  un magma associatif d'élément neutre  $e$ .

★ Il y a unicité de l'inverse lorsqu'il existe.

Si  $x \in E$  est inversible, on notera  $x^{-1}$  son inverse.

★ Si  $x \in E$  est inversible pour  $\star$ , alors  $x^{-1}$  est inversible d'inverse :

$$(x^{-1})^{-1} = x$$

★ Soit  $x \in E$  un élément inversible. Alors  $x$  est un élément *régulier*, ce qui signifie que :

$$\forall y, z \in E, \quad x \star y = x \star z \implies y = z$$

et :

$$\forall y, z \in E, \quad y \star x = z \star x \implies y = z$$

★ Si  $x$  et  $y$  sont deux éléments inversibles dans  $E$ , alors  $x \star y$  est un élément inversible d'inverse :

$$(x \star y)^{-1} = y^{-1} \star x^{-1}$$

**Démonstration** ★ Soit  $x \in E$  un élément inversible. Supposons que  $y, z \in E$  soient tels que :

$$x \star y = y \star x = e \quad \text{et} \quad x \star z = z \star x = e$$

Montrons que  $y = z$ . Par associativité de  $\star$ , on a :

$$y = e \star x = (z \star x) \star y = z \star (x \star y) = z \star e = z,$$

d'où l'unicité de l'inverse en cas d'existence.

★ Si  $x$  est inversible d'inverse  $x^{-1}$ , alors :

$$x \star x^{-1} = x^{-1} \star x = e$$

Par définition de l'inversibilité,  $x^{-1}$  est inversible et on a  $(x^{-1})^{-1} = x$  (par unicité de l'inverse).

★ Soient  $y, z \in E$  tel que  $x \star y = x \star z$ . Comme  $x$  est inversible, on a :

$$x^{-1} \star (x \star y) = x^{-1} \star (x \star z)$$

et donc, par associativité de  $\star$  :

$$(x^{-1} \star x) \star y = (x^{-1} \star x) \star z \quad \text{c'est-à-dire} \quad e \star y = e \star z$$

Comme  $e$  est élément neutre pour  $\star$ , on obtient  $y = z$ . La deuxième propriété se démontre de la même manière.

★ Soient  $x$  et  $y$  deux éléments inversibles de  $E$ . On a :

$$\begin{aligned} (y^{-1} \star x^{-1}) \star (x \star y) &= y^{-1} \star (x^{-1} \star x) \star y && \text{(par associativité de } \star) \\ &= y^{-1} \star e \star y \\ &= y^{-1} \star y \\ &= e \end{aligned}$$

ce qui démontre que  $x \star y$  est inversible d'inverse  $y^{-1} \star x^{-1}$ . ■

**Remarque :** si la loi du groupe est additive, on notera l'inverse «  $-x$  » (au lieu de «  $x^{-1}$  »). Par exemple, dans  $(\mathbb{Z}, +)$ , l'entier 2 est inversible et son inverse est  $-2$ .

### (d) Commutativité

**Définition** La LCI  $\star$  est dite commutative dans  $E$  si :

$$\forall x, y \in E, \quad x \star y = y \star x$$

- Exemple**
1. La multiplication et l'addition dans  $\mathbb{C}$  ( $\mathbb{R}$ ,  $\mathbb{Q}$ ,  $\mathbb{Z}$ ,  $\mathbb{N}$ ) sont commutatives.
  2. L'intersection et la réunion sont commutatives dans  $\mathcal{P}(E)$ .
  3. Dans  $\mathbb{R}^{\mathbb{R}}$ , on sait que la composition n'est pas commutative.

**Remarque :** lorsque  $\star$  est commutative, certaines des propriétés précédentes de  $\star$  peuvent être simplifiées :

- ★  $e \in E$  est élément neutre si :  $\forall x \in E, x \star e = x$  ;
- ★ un élément  $x$  de  $E$  est inversible s'il existe  $y \in E$  tel que  $x \star y = e$ .

## II – Structure de groupe

Soit  $G$  un ensemble non vide.

### 1) Définition et exemples

**Définition (groupe)** Soit  $(G, \star)$  un magma. On dit que  $(G, \star)$  est un *groupe* si :

- $(G_1)$  la loi  $\star$  est associative ;
- $(G_2)$  la loi  $\star$  admet un élément neutre (noté  $e$ ) ;
- $(G_3)$  tous les éléments de  $G$  sont inversibles pour  $\star$ .

Si de plus la loi  $\star$  est commutative, on parle de groupe *commutatif* (ou de groupe *abélien*).

### Quelques exemples usuels

- ★ Si  $(E, \star)$  est un magma admettant un élément neutre  $e$ , alors  $(\{e\}, \star)$  est un groupe, appelé *groupe trivial*.
- ★ Les ensembles  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  sont des groupes abéliens dits *additifs* (c'est-à-dire sont des groupes lorsqu'ils sont munis de l'addition).
- ★ Le couple  $(\mathbb{N}, +)$  n'est pas un groupe ( $(G_3)$  n'étant pas vérifiée).
- ★  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{R}_+^*, \times)$ ,  $(\mathbb{C}^*, \times)$ ,  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{Q}_+^*, \times)$  sont des groupes abéliens dits *multiplicatifs*.
- ★ **Rappels :**

— l'ensemble des nombres complexes de module 1 est :

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$$

— pour tout  $n \in \mathbb{N}^*$ , l'ensemble des racines  $n^{\text{e}}$  de l'unité est :

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{ e^{i \frac{2k\pi}{n}} \mid k \in \llbracket 0, n-1 \rrbracket \right\} \subset \mathbb{U}$$

Alors  $\mathbb{U}$  est un groupe abélien, de même que  $\mathbb{U}_n$  pour tout  $n \in \mathbb{N}^*$  (ces derniers étant de cardinaux finis).

- ★ Si  $E$  est un ensemble non vide, l'ensemble des bijections de  $E$  dans  $E$ , noté  $S_E$ , est un groupe muni de la composition (que l'on appelle *groupe symétrique de  $E$* ). L'élément neutre est  $\text{Id}_E$ .

## 2) Puissances dans un groupe

Lorsque la loi  $\star$  est clairement identifiée (notamment quand on travaille dans un groupe multiplicatif ou additif), on peut s'affranchir de la notation «  $x \star y$  » en écrivant simplement «  $xy$  ». C'est ce qu'on fait usuellement dans le groupe  $(\mathbb{R}^*, \times)$  par exemple.

**Définition (itérés ou puissances d'un élément d'un groupe)** Soit  $G$  un groupe d'élément neutre  $e$  et soit  $x \in G$ . Pour tout entier relatif  $n$ , on définit la puissance  $n^e$  de  $x$  par récurrence de la manière suivante :

- ★  $x^0 = e$ ;
- ★ si  $n \in \mathbb{N}$ ,  $x^{n+1} = x^n x$ ;
- ★ si  $n < 0$ , alors on pose  $x^n = (x^{-1})^{-n}$ .

**Exemple** 1. Dans le groupe  $(\mathbb{C}^*, \times)$ , les puissances d'un élément correspond à la propriété d'exponentiation usuelle.

2. Dans le groupe additif  $(\mathbb{C}, +)$ , les puissances de  $x \in \mathbb{C}$  correspondent en fait à :

- $\forall n \in \mathbb{N}^*$ ,  $nx = x + \dots + x$  ( $n$  fois) ;
- $\forall n \in \mathbb{Z} \setminus \mathbb{N}$ ,  $nx = -(-n)x$

Autrement dit, les puissances *additives* correspondent aux multiples.

3. Dans  $S_E$ , la puissance  $n^e$  (avec  $n \in \mathbb{N}^*$ ) de  $\sigma \in S_E$  est définie par :

$$\sigma^n = \sigma \circ \dots \circ \sigma \quad (n \text{ fois})$$

Par exemple,  $f : x \mapsto 2x$  est un élément de  $S_{\mathbb{R}}$  et :

$$\forall n \in \mathbb{Z}, \quad f^n : x \mapsto 2^n x$$

**Proposition** Soit  $G$  un groupe.

★ Soit  $x \in G$ . Alors :

$$\forall m, n \in \mathbb{Z}, \quad x^{m+n} = x^n x^m = x^m x^n$$

★ Soient  $x$  et  $y$  deux éléments de  $G$  qui commutent (c'est-à-dire tels que  $xy = yx$ ). Alors :

$$\forall m, n \in \mathbb{Z}, \quad x^n y^m = y^m x^n$$

et :

$$\forall n \in \mathbb{Z}, \quad (xy)^n = x^n y^n = y^n x^n$$

**Démonstration** Il suffit de procéder par récurrence en distinguant les cas d'exposants positifs et négatifs. ■

**Remarque :** en notation additive, on obtient par exemple pour la première propriété :

$$\forall x \in G, \forall (m, n) \in \mathbb{Z}^2, \quad (m + n)x = mx + nx$$

## 3) Groupe produit

Soient  $n \in \mathbb{N}^*$  et  $(G_1, \star_1), \dots, (G_n, \star_n)$  des groupes. On définit une loi de composition interne  $\star$  sur le produit  $G = G_1 \times \dots \times G_n$  en posant, pour tous  $(g_1, \dots, g_n), (h_1, \dots, h_n) \in G$  :

$$(g_1, \dots, g_n) \star (h_1, \dots, h_n) = (g_1 \star_1 h_1, \dots, g_n \star_n h_n)$$

**Proposition** Le magma  $(G, \star)$  est un groupe d'élément neutre  $(e_{G_1}, \dots, e_{G_n})$ . Il est abélien si tous les groupes sous-jacents le sont. On l'appelle le groupe produit de  $G_1, \dots, G_n$ .

**Démonstration** On se place dans le cas  $n = 2$ , le cas général étant similaire.

- ★ Tout d'abord, il est clair que  $\star$  est une loi de composition interne dans  $G$ .
- ★ L'associativité de  $\star_1$  et  $\star_2$  implique l'associativité de  $\star$  dans  $G$ .
- ★ En notant  $e_1$  et  $e_2$  les éléments neutres de  $G_1$  et  $G_2$  respectivement, il est facile de vérifier que  $e = (e_1, e_2) \in G$  est élément neutre dans  $G$ .
- ★ Enfin, pour tout  $g = (g_1, g_2) \in G$ , il est facile de voir que  $g$  est inversible dans  $G$  d'inverse  $g^{-1} = (g_1^{-1}, g_2^{-1}) \in G$ . ■

**Exemple** ★ On sait que  $(\mathbb{R}, +)$  est un groupe abélien donc, pour tout  $n \in \mathbb{N}^*$ , le couple  $(\mathbb{R}^n, +)$  est un groupe où l'addition  $+$  est ici défini par :

$$\forall (x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n, \quad (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

L'élément neutre est  $(0, \dots, 0)$ .

- ★ On sait que  $(\mathbb{R}, +)$  et  $(\mathbb{U}, \times)$  sont des groupes. Donc  $\mathbb{R} \times \mathbb{U}$  est un groupe dont la loi  $\star$  est définie par :

$$\forall (x, u), (y, v) \in \mathbb{R} \times \mathbb{U}, \quad (x, u) \star (y, v) = (x + y, uv)$$

L'élément neutre est  $(0, 1)$ .

#### 4) Notion de sous-groupe

**Définition** Soient  $(G, \star)$  un groupe et  $H$  un sous-ensemble non vide de  $G$ . On dit que  $H$  est un sous-groupe de  $G$  (pour la loi  $\star$ ) si :

- $(SG)_1 \quad \forall h, k \in H, h \star k \in H$  (on dit que  $H$  est stable pour la loi  $\star$ );
- $(SG)_2 \quad \forall h \in H, h^{-1} \in H$  (on dit que  $H$  est stable par passage à l'inverse).

**Exemple** ★  $(\mathbb{R}, +)$  est un sous-groupe de  $(\mathbb{C}, +)$ ;

- ★ pour tout  $n \in \mathbb{N}^*$ ,  $(\mathbb{U}_n, \times)$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ .

**Démonstration** Soit  $n \in \mathbb{N}^*$ . Tout d'abord,  $\mathbb{U}_n$  est non vide (puisqu'il contient 1) et est inclus dans  $\mathbb{C}^*$  (le nombre complexe 0 n'étant pas une racine de l'unité).

- ★ Soient  $z, w \in \mathbb{U}_n$ . Alors :

$$(zw)^n = z^n w^n = 1 \times 1 = 1$$

car  $z, w \in \mathbb{U}_n$ . Donc  $zw \in \mathbb{U}_n$ .

- ★ Soit  $z \in \mathbb{U}_n$ . Alors  $z \neq 0$  et :

$$\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = \frac{1}{1} = 1$$

donc  $\frac{1}{z} \in \mathbb{U}_n$ .

Finalement,  $(\mathbb{U}_n, \times)$  est un sous-groupe de  $(\mathbb{C}^*, \times)$ . ■

**Proposition** Soit  $H$  est une partie non vide de  $G$ , alors :

$$H \text{ est un sous-groupe de } G \iff \forall h, k \in H, h \star k^{-1} \in H$$

**Démonstration** On raisonne par double implication.

- ★ Supposons que  $H$  soit un sous-groupe de  $G$ . Soient  $h, k \in H$ . Alors  $k^{-1} \in H$  (propriété  $(SG_2)$ ) puis  $h \star k^{-1} \in H$  (propriété  $(SG_1)$ ).
- ★ Réciproquement, supposons que pour tout  $h, k \in H$ , on ait  $h \star k^{-1} \in H$ . Montrons alors que  $H$  est un sous-groupe de  $G$ .
  - Comme  $H$  est non vide, on peut considérer un élément  $h$  dans  $G$ . D'après la propriété vérifiée par  $H$ , on a  $e = h \star h^{-1} \in H$ .
  - Pour tout  $h \in H$ , on a (puisque l'on sait maintenant que  $e \in H$ )  $h^{-1} = e \star h^{-1} \in H$ .
  - Pour tous  $h, k \in H$ , on a  $k^{-1} \in H$  donc (d'après la propriété vérifiée par  $H$ ) :

$$h \star k = h \star (k^{-1})^{-1} \in H$$

On vient de montrer que  $H$  vérifie les propriétés  $(SG_1)$  et  $(SG_2)$  donc  $H$  est un sous-groupe de  $G$ . ■

L'intérêt de cette définition réside dans la proposition suivante.

**Proposition** Soient  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Alors  $(H, \star)$  est un groupe.

**Démonstration** ★ D'après  $(SG)_1$ ,  $(H, \star)$  est un magma.

- ★ Comme  $H \neq \emptyset$ , on peut considérer un élément  $h$  de  $H$ . Alors  $h^{-1} \in H$  d'après  $(SG)_2$  et donc  $e_G = h \star h^{-1} \in H$  d'après  $(SG)_1$ .
- ★ La loi  $\star$  étant associative dans  $G$ , elle l'est aussi dans tout sous-ensemble de  $G$ , donc en particulier dans  $H$ .
- ★ Tous les éléments de  $H$  sont inversibles pour  $\star$  (puisque  $(G, \star)$  est un groupe et les inverses appartiennent à  $H$  d'après  $(SG)_2$ ).

Donc  $(H, \star)$  est un groupe. ■

Ainsi, pour montrer qu'un ensemble muni d'une loi est un groupe, il suffit de montrer qu'il s'agit d'un sous-groupe d'un groupe connu.

**Exemple** Pour tout  $n \in \mathbb{Z}$ , l'ensemble  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  est un groupe en tant que sous-groupe de  $(\mathbb{Z}, +)$ .

**Proposition** Soit  $(G, \star)$  un groupe et  $H, K$  deux sous-groupes de  $G$ . Alors  $H \cap K$  est un sous-groupe de  $G$ .

**Démonstration** On utilise la proposition précédente. Notons  $e$  l'élément neutre de  $G$ .

- ★ Comme  $H$  et  $K$  sont des sous-groupes de  $G$ , on a  $e \in H \cap K$ . En particulier,  $H \cap K \neq \emptyset$ .
- ★ Soient  $x, y \in H \cap K$ . En particulier,  $x, y \in H$  et  $H$  est un sous-groupe de  $G$  donc  $x \star y^{-1} \in H$ . De la même manière,  $x \star y^{-1} \in K$ . On a donc  $x \star y^{-1} \in H \cap K$ .

Finalement,  $H \cap K$  est un sous-groupe de  $G$ . ■

**Remarque :** la propriété est fautive pour la réunion. Par exemple,  $2\mathbb{Z}$  et  $3\mathbb{Z}$  sont des sous-groupes de  $\mathbb{Z}$  mais  $2\mathbb{Z} \cup 3\mathbb{Z}$  n'en est pas un. En effet, 2 et 3 appartiennent à cet ensemble mais  $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$  (puisque 5 n'est ni un multiple de 2, ni un multiple de 3).

### III – Morphismes de groupes

Dans cette partie,  $(G, \star)$  et  $(H, \Delta)$  désignent deux groupes (de neutres notés  $e_G$  et  $e_H$ ) et  $f : G \longrightarrow H$  est une application.

Commençons par un exemple. Considérons l'application  $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ . On sait que :

- ★  $(\mathbb{R}, +)$  est un groupe ;
- ★  $(\mathbb{R}_+^*, \times)$  est un groupe ;
- ★  $\forall x, y \in \mathbb{R}, \exp(x + y) = \exp(x) \times \exp(y)$

Ainsi, la fonction  $\exp$  préserve la structure des deux groupes  $(\mathbb{R}, +)$  et  $(\mathbb{R}_+^*, \times)$ . On parle de *morphisme de groupes*.

#### 1) Définition et premières propriétés

**Définition (morphisme de groupes)** On dit que  $f$  est un *morphisme* de groupes de  $G$  vers  $H$  si :

$$\forall x, y \in G, \quad f(x \star y) = f(x) \Delta f(y)$$

On dit que  $f$  est un *isomorphisme de groupes* si  $f$  est bijectif.

**Exemple** Les applications suivantes sont des morphismes de groupes :

- ★  $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$  (isomorphisme) ;
- ★  $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$  ;
- ★  $\varphi : \begin{cases} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{cases}$
- ★  $f_n : \begin{cases} (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}, +) \\ k & \longmapsto & nk \end{cases}$  (où  $n \in \mathbb{Z}^*$ )
- ★  $\theta : \begin{cases} G & \longrightarrow & H \\ g & \longmapsto & e_H \end{cases}$  est un morphisme de groupes (dit trivial)

**Dans la suite de cette section,  $f : G \longrightarrow H$  est un morphisme de groupes.**

**Proposition** On a :

- (i)  $f(e_G) = e_H$  ;
- (ii) pour tout  $x \in G$ , on a  $f(x^{-1}) = f(x)^{-1}$  ;
- (iii) pour tout  $(n, x) \in \mathbb{Z} \times G$ , on a  $f(x^n) = f(x)^n$ .

**Démonstration** (i) On sait que  $e_G \star e_G = e_G$  donc (comme  $f$  est un morphisme de groupes) :

$$f(e_G) = f(e_G \star e_G) = f(e_G) \Delta f(e_G)$$

En simplifiant par  $f(e_G)$  dans le groupe  $H$ , on a bien  $f(e_G) = e_H$ .

(ii) Soit  $x \in G$ . Comme  $f$  est un morphisme de groupes, on a :

$$f(x^{-1}) \Delta f(x) = f(x^{-1} \star x) = f(e_G) = e_H$$

De la même manière,  $f(x) \Delta f(x^{-1}) = e_H$ . Donc, par unicité de l'inverse,  $f(x^{-1}) = f(x)^{-1}$ .

(iii) Soit  $x \in \mathbb{N}$ . On démontre par récurrence que, pour tout entier naturel  $n$ , on a  $f(x^n) = f(x)^n$ . Ensuite, si  $n \in \mathbb{Z} \setminus \mathbb{N}$ , on a :

$$\begin{aligned} f(x^n) &= f((x^{-n})^{-1}) = f(x^{-n})^{-1} && \text{(d'après (ii))} \\ &= (f(x)^{-n})^{-1} && \text{(d'après la récurrence précédente car } -n \geq 0) \\ &= f(x)^n \end{aligned}$$

**Proposition (image, image réciproque)** (i) Si  $G'$  est un sous-groupe de  $G$ , alors  $f(G')$  est un sous-groupe de  $H$ .  
(ii) Si  $H'$  est un sous-groupe de  $H$ , alors  $f^{-1}(H')$  est un sous-groupe de  $G$ .

**Démonstration** (i) Posons  $\tilde{H} = f(G')$ . On sait que  $e_H = f(e_G)$  (puisque  $f$  est un morphisme de groupes). Comme  $e_G \in G'$ , on a bien  $e_H \in \tilde{H}$ . Soit maintenant  $(h, k) \in \tilde{H}^2$ . Par définition de  $\tilde{H}$ , il existe  $(a, b) \in G'^2$  tel que  $h = f(a)$  et  $k = f(b)$ . On a alors (par propriétés de morphismes) :

$$h\Delta k^{-1} = f(a)\Delta f(b)^{-1} = f(a)\Delta f(b^{-1}) = f(a \star b^{-1})$$

Comme  $G'$  est un groupe, on sait que  $a \star b^{-1} \in G'$  et donc  $h\Delta k^{-1} \in \tilde{H}$ . Finalement,  $\tilde{H} = f(G')$  est un sous-groupe de  $H$ .

(ii) Posons :

$$\tilde{G} = f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$$

Tout d'abord,  $e_G$  appartient à  $\tilde{G}$ . En effet, on a  $f(e_G) = e_H$  (puisque  $f$  est un morphisme de groupes) et on sait que  $e_H \in H'$  car  $H'$  est un sous-groupe de  $H$ . Soit maintenant  $(g, h) \in \tilde{G}^2$  et montrons que  $g \star h^{-1} \in \tilde{G}$ . Pour cela, montrons que  $f(g \star h^{-1}) \in H'$ . On a (en utilisant les propriétés de morphismes de  $f$ ) :

$$f(g \star h^{-1}) = f(g)\Delta f(h^{-1}) = f(g)\Delta f(h)^{-1} \in H'$$

car  $H'$  est un sous-groupe de  $H$  et car  $(g, h) \in \tilde{G}^2$ . Finalement,  $\tilde{G} = f^{-1}(H')$  est un sous-groupe de  $G$ . ■

**Exemple** Considérons le morphisme de groupes :

$$f : \begin{cases} (\mathbb{Z}, +) & \longmapsto & (\mathbb{Z}, +) \\ n & \longmapsto & 2n \end{cases}$$

D'après la proposition précédente,  $2\mathbb{Z} = f(\mathbb{Z})$  est un sous-groupe (pour  $+$ ) de  $\mathbb{Z}$  (ce que l'on savait déjà).

## 2) Noyau d'un morphisme de groupes

Le noyau est lié à l'injectivité.

**Définition (noyau)** On appelle *noyau de  $f$* , noté  $\text{Ker}(f)$ , le sous-ensemble de  $G$  suivant :

$$\text{Ker}(f) = \{g \in G \mid f(g) = e_H\}$$

Le noyau de  $f$  est donc l'ensemble des antécédents par  $f$  de  $e_H$ , c'est-à-dire  $\text{Ker}(f) = f^{-1}(\{e_H\})$ . Par conséquent :

**Proposition** Le noyau  $\text{Ker}(f)$  de  $f$  est un sous-groupe de  $G$ .

**Démonstration** C'est une application directe de la proposition précédente avec le groupe trivial  $(\{e_H\}, \Delta)$ . ■

L'importance majeure de l'étude du noyau réside dans le résultat suivant :

**Théorème** Le morphisme de groupes  $f : G \rightarrow H$  est injectif si et seulement si  $\text{Ker}(f) = \{e_G\}$ .

**Démonstration** On raisonne par double implication.

- ★ On suppose que  $\text{Ker}(f) = \{e_G\}$ . Montrons que  $f$  est injectif. Soit  $(x, y) \in G^2$  tel que  $f(x) = f(y)$ . Alors  $f(xy^{-1}) = e_H$  et donc  $xy^{-1} \in \text{Ker}(f)$ , d'où l'on déduit que  $x = y$ . Donc  $f$  est injectif.
- ★ Supposons que  $f$  est injectif. Soit  $x \in G$ . Alors :

$$\begin{aligned} x \in \text{Ker}(f) &\iff f(x) = e_H \iff f(x) = f(e_G) && \text{(car } f \text{ est un morphisme de groupes)} \\ &\iff x = e_G \end{aligned}$$

car  $f$  est injectif. Ainsi,  $\text{Ker}(f) = \{e_G\}$ .

On obtient bien l'équivalence annoncée. ■

**Exemple** ★ Pour tout  $n \in \mathbb{Z}^*$ , on a  $\text{Ker}(f_n) = \{0\}$  donc  $f_n$  est injectif.

- ★ On a  $\text{Ker}(\varphi) = 2\pi\mathbb{Z} \neq \{0\}$  donc  $\varphi$  n'est pas injectif.

### 3) Image d'un morphisme de groupes

L'image est liée à la surjectivité.

**Définition (image)** Soit  $f : G \rightarrow H$  un morphisme de groupes. On appelle *image de  $f$* , notée  $\text{Im}(f)$ , le sous-ensemble de  $H$  suivant :

$$\begin{aligned} \text{Im}(f) &= \{h \in H \mid \exists g \in G, h = f(g)\} \\ &= \{f(g) \mid g \in G\} \end{aligned}$$

Comme  $\text{Im}(f) = f(G)$ , la proposition 9 nous permet d'obtenir le premier point du résultat suivant.

**Proposition** ★ L'image  $\text{Im}(f)$  de  $f$  est un sous-groupe de  $H$ .

- ★ Le morphisme  $f$  est surjectif si et seulement si  $\text{Im}(f) = H$ .

**Démonstration** Le deuxième point est évident. ■

**Exemple** On reprend l'exemple précédent.

1. On a  $\text{Im}(f_n) = n\mathbb{Z} = \mathbb{Z}$  si et seulement si  $n \in \{-1, 1\}$ . Donc  $f_n$  est surjectif si et seulement si  $n \in \{-1, 1\}$ .
2. On a  $\text{Im}(\varphi) = \mathbb{U}$  donc  $\varphi$  est surjectif.

## IV – Anneaux et corps

### 1) Structure d'anneau

**Définition (anneau)** Soit  $A$  un ensemble non vide muni de deux LCI notées  $+$  et  $\times$ . On dit que  $(A, +, \times)$  est un *anneau* si :

(A<sub>1</sub>)  $(A, +)$  est un groupe abélien (de neutre noté  $0_A$ );

(A<sub>2</sub>)  $\times$  est associative *i.e.* si :

$$\forall a, b, c \in A, \quad (a \times b) \times c = a \times (b \times c)$$

(A<sub>3</sub>)  $\times$  est distributive par rapport à  $+$  *i.e.* si :

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

(A<sub>4</sub>) la loi  $\times$  admet un élément neutre noté  $1_A$ , *i.e.* :

$$\forall a \in A, \quad a \times 1_A = 1_A \times a = a$$

Si la loi  $\times$  est de plus commutative, on dit que l'anneau est commutatif.

**Notation :** en général, le neutre pour  $+$  est noté  $0$  (ou  $0_A$ ) et le neutre pour  $\times$  est noté  $1$  (ou  $1_A$ ).

**Remarque :** si  $(A, +, \times)$  est un anneau, alors :

$$\forall x \in A, \quad 0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x$$

car  $0_A$  est élément neutre pour  $+$  puis par distributivité de  $\times$  par rapport à  $+$ . Comme  $0 \times x$  est inversible pour  $+$ , on a  $0_A \times x = 0_A$ .

**Exemple** ★ Les ensembles  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$  sont des anneaux pour l'addition et la multiplication usuelles.

★ Si  $E$  est un ensemble et si  $A$  est un anneau, alors  $A^E$  est un anneau.

★ Le seul anneau dans lequel  $0_A = 1_A$  est l'anneau nul  $\{0_A\}$  (il s'agit bien d'un anneau). En effet, si  $0_A = 1_A$ , alors :

$$\forall x \in A, \quad 0_A \times x = 0_A = 1_A \times x = x$$

**Définition (éléments inversibles d'un anneaux)** Soit  $(A, +, \times)$  un anneau.

★ Un élément  $a$  de  $A$  est dit inversible si il l'est pour la loi  $\times$  *i.e.* si :

$$\exists b \in A, \quad a \times b = b \times a = 1_A$$

★ On note  $A^\times$  l'ensemble des éléments inversibles de  $A$ .

 **Exercice** Soit  $(A, +, \times)$  un anneau. Montrer que  $A^\times$ , muni de la multiplication, est un groupe.

**Exemple** 1.  $\mathbb{Z}^\times = \{-1, 1\}$ ;  
2.  $\mathbb{C}^\times = \mathbb{C}^*$ ,  $\mathbb{Q}^\times = \mathbb{Q}^*$ ,  $\mathbb{R}^\times = \mathbb{R}^*$

- 3.  $\mathcal{M}_n(\mathbb{K})^\times = \text{GL}_n(\mathbb{K})$
- 4. anneau nul :  $\{0_A\}^\times = \{0_A\}$  (dans un tel anneau,  $1_A = 0_A$ ).

**Définition (anneau intègre)** Soit  $(A, +, \times)$  un anneau. On dit que  $A$  est *intègre* si  $A$  est non nul (c'est-à-dire  $A \neq \{0_A\}$ ) et si :

$$\forall a, b \in A, \quad a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A$$

**Remarques :**

- ★ En pratique, travailler dans un anneau intègre permet de résoudre des équations produit-nul.
- ★ Si  $A$  est un anneau intègre, alors :

$$\forall a, x, y \in A, \quad ax = ay \implies a = 0 \text{ ou } x = y$$

**Exemple** ★ Les anneaux,  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{K}[X]$  sont intègres.

- ★ L'anneau  $\mathcal{M}_n(\mathbb{K})$  ne l'est pas si  $n \geq 2$ . En effet, on sait que le produit de deux matrices non nulles peut être nul. Par exemple :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

- ★  $(\mathbb{R}^{\mathbb{R}}, +, \times)$  est un anneau non intègre.

## 2) Sous-anneau

**Définition (sous-anneau)** Soient  $(A, +, \times)$  un anneau et  $B$  une partie non vide de  $A$ . On dit que  $B$  est un sous-anneau de  $A$  (pour les lois  $+$  et  $\times$ ) si :

$$B \text{ est un sous-anneau de } A \iff \begin{cases} 1 \in B \\ \forall x, y \in B, x - y \in B \\ \forall x, y \in B, x \times y \in B \end{cases}$$

L'intérêt de la notion est la même que pour les sous-groupes.

**Proposition** Si  $B$  est un sous-anneau de  $(A, +, \times)$ , alors  $(B, +, \times)$  est un anneau.

**Démonstration** analogue à celle pour les sous-groupes ■

**Exemple** ★  $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Q}$ , qui est lui-même un sous-anneau de  $\mathbb{R}$ , qui est lui-même un sous-anneau de  $\mathbb{C}$ ;

- ★  $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$  (anneau des entiers de Gauss) est un sous-anneau de  $\mathbb{C}$  (donc est un anneau).

**Justification.** On a tout d'abord  $\mathbb{Z}[i] \subset \mathbb{C}$ . Ensuite,  $\mathbb{Z}[i]$  contient 1 car  $1 = 1 + 0 \times i$  (et 1 et 0 sont des entiers). Enfin, pour tout  $(x, y) \in \mathbb{Z}[i]^2$ , il existe  $(a, b, a', b') \in \mathbb{Z}^4$  tel que  $x = a + ib$  et  $y = a' + ib'$  et donc  $x - x' \in \mathbb{Z}[i]$  et  $xx' \in \mathbb{Z}[i]$  (calculs immédiats).

- ★ L'ensemble  $\mathcal{C}(\mathbb{R}, \mathbb{R})$  des fonctions continues sur  $\mathbb{R}$  à valeurs réelles est un sous-anneau de  $\mathbb{R}^{\mathbb{R}}$  (donc est un anneau).

### 3) Identités remarquables

Soit  $(A, +, \times)$  un anneau. On définit les puissances positives entières d'un élément  $a \in A$  de la même manière que dans un groupe. On peut définir  $a^n$  pour  $n \in \mathbb{Z} \setminus \mathbb{N}$  si  $a$  est inversible (sous-entendu pour  $\times$ ). De plus, si  $a, b \in A$  sont tels que  $ab = ba$ , alors :

$$\forall m, n \in \mathbb{N}, \quad a^m b^n = b^n a^m \quad \text{et} \quad (ab)^n = a^n b^n = b^n a^n$$

On a les deux identités suivantes :

**Proposition (binôme de Newton et identité de Bernoulli)** Soit  $(A, +, \times)$  un anneau.

★ **Formule du binôme de Newton** : pour tout  $(a, b) \in A^2$  tel que  $ab = ba$  et pour tout entier naturel  $n$ , on a

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

★ **Identité de Bernoulli** : pour tout  $(a, b) \in A^2$  tel que  $ab = ba$  et pour tout entier naturel  $n$  non nul, on a

$$a^n - b^n = \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

**Démonstration** ★ déjà fait

★ On a :

$$\begin{aligned} (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= a \sum_{k=0}^{n-1} a^k b^{n-1-k} - b \sum_{k=0}^{n-1} a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \quad (\text{car } ab = ba) \\ &= \sum_{k=1}^n a^k b^{n-k} - \sum_{k=0}^n a^k b^{n-k} \\ &= b^n - a^n \end{aligned}$$

d'après la relation de Chasles. ■

**Remarque** : en choisissant  $a = 1_A$  (et  $b = a$ ), on obtient (puisque  $1_A$  et  $a$  commutent) :

$$\forall n \in \mathbb{N}^*, \quad a^n - 1_A = (a - 1_A) \sum_{k=0}^{n-1} a^k$$

### 4) Structure de corps

**Définition (corps)** Un anneau  $(A, +, \times)$  est appelé *corps* si :

(C<sub>1</sub>)  $A$  est commutatif (pour la loi  $\times$ );

(C<sub>2</sub>)  $A \neq \{0_A\}$ ;

(C<sub>3</sub>) tous ses éléments non nuls sont inversibles pour la loi  $\times$ .

**Exemple** Les anneaux  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$  sont des corps,  $\mathbb{Z}$  et  $\mathbb{R}^{\mathbb{R}}$  n'en sont pas.

**Remarques :**

- ★ Si  $A$  est un corps, alors  $A^\times = A \setminus \{0_A\}$ .
- ★ Dans un corps, on peut additionner, soustraire, multiplier et diviser (sauf par  $0_A$ ). En particulier, tout corps est un anneau intègre. En effet, si  $a, b \in A$  est tel que  $ab = 0_A$  et si  $a \neq 0$ , alors  $a$  est inversible dans  $A$  (puisque  $A$  est un corps) et on a  $b = 0$  après division par  $a$ .

**5) Morphisme d'anneaux**

On introduit, comme pour les groupes, la notion de morphisme d'anneaux.

**Définition (morphisme d'anneaux)** Soient  $(A, +_A, \times_A)$  et  $(B, +_B, \times_B)$  deux anneaux. Une application  $\varphi : A \rightarrow B$  est un morphisme d'anneaux si :

$$(M_1) \text{ pour tous } a, b \in A, \text{ on a } \varphi(a +_A b) = \varphi(a) +_B \varphi(b);$$

$$(M_2) \text{ pour tous } a, b \in A, \text{ on a } \varphi(a \times_A b) = \varphi(a) \times_B \varphi(b);$$

$$(M_3) \varphi(1_A) = 1_B.$$

On dit que  $\varphi$  est un isomorphisme d'anneaux si  $\varphi$  est de plus bijectif.

**Remarques :**

- ★ Si  $\varphi$  est un morphisme d'anneaux, alors  $\varphi$  est en particulier un morphisme de groupes de  $(A, +_A)$  vers  $(B, +_B)$ .
- ★ En particulier, on a  $\varphi(0_A) = \varphi(0_B)$  et, pour tout  $a \in A$ , on a  $\varphi(-a) = -\varphi(a)$  (voir les propriétés des morphismes de groupes) et, pour tout  $n \in \mathbb{Z}$ , on a aussi  $\varphi(na) = n\varphi(a)$ .

**Exemple** Pour tout  $x \in \mathbb{R}$ , l'application  $\varphi_x : \begin{cases} \mathbb{R}^\mathbb{R} & \rightarrow & \mathbb{R} \\ f & \mapsto & f(x) \end{cases}$  est un morphisme d'anneaux.

On introduit les notions de noyau et d'image de morphismes d'anneaux qui permettent d'étudier respectivement les caractères injectif et surjectif du morphisme.

**Définition (image, noyau)** Soit  $f : A \rightarrow B$  un morphisme d'anneaux.

- ★ On appelle noyau de  $f$ , noté  $\text{Ker}(f)$ , le sous-ensemble de  $A$  suivant :

$$\text{Ker}(f) = \{a \in A \mid f(a) = 0_A\}$$

- ★ On appelle image de  $f$ , notée  $\text{Im}(f)$ , le sous-ensemble de  $B$  suivant :

$$\text{Im}(f) = \{b \in B \mid \exists a \in A, b = f(a)\}$$

À nouveau :

$$f \text{ est injectif} \iff \text{Ker}(f) = \{0_A\}$$

et :

$$f \text{ est surjectif} \iff \text{Im}(f) = B$$