

---

<b>1</b>	<b>Loi de composition interne sur un ensemble.</b>	<b>2</b>
1.1	Définitions et propriétés. . . . .	2
1.2	Éléments symétrisables. . . . .	4
1.3	Itérés. . . . .	5
1.4	Notations multiplicatives et additives. . . . .	6
<b>2</b>	<b>Structure de groupe.</b>	<b>6</b>
2.1	Définition et exemples. . . . .	6
2.2	Sous-groupes. . . . .	8
2.3	Morphismes de groupes. . . . .	10
<b>3</b>	<b>Structure d'anneau.</b>	<b>11</b>
3.1	Définitions et règles de calcul. . . . .	11
3.2	Groupe des inversibles dans un anneau. . . . .	13
3.3	Nilpotents dans un anneau. . . . .	14
3.4	Sous-anneaux, morphismes d'anneaux. . . . .	14
3.5	Anneaux intègres. . . . .	15
<b>4</b>	<b>Structure de corps.</b>	<b>16</b>
4.1	Définitions et exemples. . . . .	16
4.2	Notation fractionnaire dans un corps. . . . .	16
4.3	Corps des fractions d'un anneau intègre. . . . .	16
	<b>Exercices</b>	<b>17</b>

---

# 1 Loi de composition interne sur un ensemble.

## 1.1 Définitions et propriétés.

### Définition 1.

On appelle **loi de composition interne** sur un ensemble  $E$  (on écrira l.c.i.) une application

$$\star : \begin{cases} E \times E & \rightarrow E \\ (x, y) & \mapsto x \star y \end{cases}.$$

On notera que l'image de  $(x, y)$  par  $\star$  est notée  $x \star y$  plutôt que  $\star(x, y)$ .

Soit  $E$  un ensemble et  $\star$  une loi de composition interne sur  $E$ .

- La loi  $\star$  est dite **associative** si

$$\forall (x, y, z) \in E^3 \quad (x \star y) \star z = x \star (y \star z).$$

- De deux éléments  $x$  et  $y$  de  $E$ , on dit qu'ils **commutent** pour  $\star$  lorsque  $x \star y = y \star x$ .  
On dit que la loi  $\star$  est **commutative** si deux éléments de  $E$  quelconques commutent, c'est-à-dire si

$$\forall (x, y) \in E^2 \quad x \star y = y \star x.$$

- On appelle **élément neutre** pour la loi  $\star$  tout élément  $e \in E$  tel que

$$\forall x \in E \quad x \star e = x \quad \text{et} \quad e \star x = x.$$

Pourquoi *loi de composition interne*? Grâce à  $\star$ , à partir d'un couple  $(x, y)$  d'éléments de  $E$ , on obtient le composé  $x \star y$  qui est un élément de  $E$  : la composition s'est faite à l'intérieur de  $E$ .

### Définition 2 (un peu de vocabulaire qui n'est pas dans le programme).

Un couple  $(E, \star)$ , où  $E$  est un ensemble et  $\star$  une l.c.i. sur  $E$  est appelé un **magma**.

On dit que ce magma est associatif si  $\star$  est associative, commutatif si  $\star$  est commutative, et **unifère** s'il existe dans  $E$  un élément neutre pour  $\star$ .

Si  $(E, \star)$  est un magma associatif et  $x, y, z$  trois éléments de  $E$ , la définition de l'associativité donne que l'écriture  $x \star y \star z$  n'est pas ambiguë. De la même manière, si  $t$  est un quatrième élément de  $E$ , on a les égalités

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

de sorte qu'on pourra écrire  $x \star y \star z \star t$  sans ambiguïté.

### Proposition 3.

Dans un magma unifère, il y a unicité de l'élément neutre.

**Définition 4.**

Soit  $(E, \star)$  un magma. Une partie  $A$  de  $E$  est dite **stable** par  $\star$  si

$$\forall (x, y) \in A^2 \quad x \star y \in A.$$

**Définition 5.**

Soit  $(E, \star)$  un magma et  $A$  une partie de  $E$  stable par  $\star$ . La restriction de  $\star$  à  $A^2$  :

$$\star : \begin{cases} A \times A & \rightarrow A \\ (x, y) & \mapsto x \star y \end{cases}$$

est une loi de composition interne sur  $A$  : on l'appelle **loi induite** par  $\star$  sur  $A$ .

**Exemple 6** (Ensembles de nombres).

- L'addition  $+$  est une loi de composition interne sur chacun des ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ . Elle est associative, commutative et admet  $0$  pour élément neutre. Les parties  $[0, +\infty[$  et  $] -\infty, 0[$  de  $\mathbb{R}$  sont stables par  $+$ .
- La multiplication  $\times$  est une l.c.i sur chacun des ensembles  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ . Elle est associative, commutative et admet  $1$  pour élément neutre. Les parties  $[0, +\infty[$  et  $\mathbb{R}^*$  de  $\mathbb{R}$  sont stables par  $\times$ .
- La soustraction  $-$  est une loi de composition interne sur  $\mathbb{Z}$  qui n'est ni associative, ni commutative et n'admet pas d'élément neutre.  $\mathbb{N}$  est une partie de  $\mathbb{Z}$  qui n'est pas stable par  $-$ .

**Exemple 7** (Ensemble des parties).

Soit  $E$  un ensemble. L'intersection  $\cap$  et la réunion  $\cup$  définissent des l.c.i. sur  $\mathcal{P}(E)$ .

- Le magma  $(\mathcal{P}(E), \cap)$  est associatif, commutatif et unifère, avec  $E$  pour élément neutre.
- Le magma  $(\mathcal{P}(E), \cup)$  est associatif, commutatif et unifère, avec  $\emptyset$  pour élément neutre.

**Exemple 8** (Ensemble de fonctions et composition).

Soit  $E$  un ensemble. La composition  $\circ$  est une loi de composition interne sur  $E^E$ , l'ensemble des fonctions définies sur  $E$  et à valeurs dans  $E$ .

Le magma  $(E^E, \circ)$  est associatif et unifère : il admet  $\text{Id}_E$  pour élément neutre.

Si  $E$  admet au moins deux éléments,  $\circ$  n'est pas commutative.

L'ensemble des fonctions injectives est une partie de  $E^E$  stable par  $\circ$ .

C'est aussi le cas pour l'ensemble des fonctions surjectives et pour celui des fonctions bijectives.

**Définition 9** (Distributivité d'une loi par rapport à une autre).

Soit  $E$  un ensemble muni de deux lois de composition internes  $\oplus$  et  $\otimes$ .  
On dit que  $\otimes$  est **distributive par rapport à  $\oplus$**  si

$$\forall (x, y, z) \in E^3 \quad : \quad \begin{cases} x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \\ (y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x). \end{cases}$$

(Si la loi  $\otimes$  n'est pas commutative, il est primordial de vérifier les deux égalités.)

**Exemple 10.**

- Dans  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ , la multiplication  $\times$  est distributive par rapport à l'addition  $+$ .
- Dans  $\mathcal{P}(E)$ ,  $\cap$  est distributive par rapport à  $\cup$ .
- Dans  $\mathcal{P}(E)$ ,  $\cup$  est distributive par rapport à  $\cap$ .

**1.2 Éléments symétrisables.****Définition 11.**

Soit  $(E, \star)$  un magma unifère d'élément neutre  $e$ , et  $x$  un élément de  $E$ .  
On dit que  $x$  est **symétrisable** (ou **inversible**) s'il existe un élément  $x'$  dans  $E$  tel que

$$x \star x' = e \quad \text{et} \quad x' \star x = e.$$

**Proposition-Définition 12.**

Soit  $(E, \star)$  un magma associatif et unifère d'élément neutre  $e$ .  
Si  $x$  est un élément de  $E$  symétrisable, il existe un unique  $x'$  dans  $E$  tel que  $x \star x' = x' \star x = e$ .  
On appelle cet élément le **symétrique** de  $x$  (ou son inverse), et on le note  $x^{-1}$ .

**Exemples 13.**

- Les inversibles du magma  $(\mathbb{Z}, \times)$  sont  $-1$  et  $1$ .
- Les inversibles du magma  $(\mathbb{R}, \times)$  sont les réels non nuls ; on a admis en effet que pour tout  $x \in \mathbb{R}^*$ , il existe un réel  $x^{-1}$  tel que  $x \times x^{-1} = x^{-1} \times x = 1$ .

**Exemple 14.**

Les inversibles du magma  $(E^E, \circ)$  sont les bijections  $f : E \rightarrow E$ .  
Si  $f : E \rightarrow E$  est une bijection, son inverse  $f^{-1}$  est sa réciproque.

**Proposition 15.**

Soit  $(E, \star)$  un magma associatif et unifère, et  $x$  et  $y$  deux éléments de  $E$ .

1. Si  $x$  est symétrisable,  $x^{-1}$  l'est aussi et  $(x^{-1})^{-1} = x$ .
2. Si  $x$  et  $y$  sont symétrisables,  $x \star y$  l'est aussi et

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

**1.3 Itérés.**

On fixe pour tout ce paragraphe un magma  $(E, \star)$  associatif et unifère, dont l'élément neutre est noté  $e$ .

**Définition 16** (Itérés d'un élément).

Soit  $x \in E$ .

1. Pour  $n \in \mathbb{N}$ , on définit  $x^n$  par récurrence sur  $n \in \mathbb{N}$ .
  - On pose  $x^0 = e$ .
  - Pour tout  $n \in \mathbb{N} : x^{n+1} = x^n \star x$ .
2. Si  $x$  est inversible et  $n \in \mathbb{N}^*$ , on pose

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

**Remarque.** Si  $n \in \mathbb{N}^*$ ,  $x^n$  est donc égal à  $x^n = \underbrace{x \star \dots \star x}_{n \text{ facteurs}}$ , écriture non ambiguë par associativité.

**Proposition 17** (Propriétés des itérés).

$$\forall x \in E \quad \forall (m, n) \in \mathbb{N}^2 \quad x^m \star x^n = x^{m+n} \quad \text{et} \quad (x^m)^n = x^{mn}.$$

Si  $x$  est inversible, les identités ci-dessus sont vraies pour  $(m, n) \in \mathbb{Z}^2$ . En particulier,


Si  $x$  est inversible, pour  $n \in \mathbb{N}$ ,  $x^n$  est inversible d'inverse  $x^{-n}$ .

**Proposition 18** (Itérés d'éléments qui *commutent*).

Soient  $x$  et  $y$  deux éléments de  $E$  qui commutent (c'est-à-dire que  $x \star y = y \star x$ ). Alors

$$\forall (m, n) \in \mathbb{N}^2 \quad x^m \star y^n = y^n \star x^m,$$

$$\forall n \in \mathbb{N} \quad (x \star y)^n = x^n \star y^n.$$

 Les identités ci-dessus sont FAUSSES en général lorsque  $x$  et  $y$  ne commutent pas.

## 1.4 Notations multiplicatives et additives.

Utiliser la **notation multiplicative**, lorsqu'on travaille avec un magma  $(E, \star)$  consiste à ne pas écrire  $\star$  lorsqu'on calcule l'image d'un couple  $(x, y) \in E^2$ . Concrètement, on note alors  $xy$  à la place de  $x \star y$ .

Lorsqu'on travaille avec un magma associatif, commutatif et unifère, on pourra utiliser la notation  $+$  pour la loi de composition interne. Le vocabulaire et les notations introduits plus haut sont alors adaptés à cette **notation additive**, comme explicité dans le tableau ci-dessous.

notation l.c.i	$\star$	$\cdot$	$+$
image de $(x, y)$	$x \star y$	$xy$	$x + y$
notation neutre	$e$	$e$	$0$
on dit	symétrisable	invertible	symétrisable
on dit	symétrique	inverse	opposé
notation symétrique	$x^{-1}$	$x^{-1}$	$-x$
notation itéré	$x^n$	$x^n$	$nx$

## 2 Structure de groupe.

### 2.1 Définition et exemples.

#### Définition 19.

On appelle **groupe** un magma associatif et unifère dans lequel tout élément est symétrisable.

Plus précisément, un groupe est la donnée d'un couple  $(G, \star)$ , où  $G$  est un ensemble et  $\star$  une loi de composition interne sur  $G$  tels que

1.  $\star$  est associative :  $\forall (x, y, z) \in G^3 \quad (x \star y) \star z = x \star (y \star z)$ .
2. il existe dans  $G$  un élément  $e$  neutre pour la loi  $\star$  :  $\forall x \in G \quad x \star e = e \star x = x$ .
3. tout élément de  $G$  est symétrisable :  $\forall x \in G \quad \exists x' \in G \quad x \star x' = x' \star x = e$ .

Si de surcroît  $\star$  est commutative, alors le groupe  $(G, \star)$  est dit **abélien** (ou commutatif).

**Remarques.** Soit  $(G, \star)$  un groupe.

1. S'il n'y a pas d'ambiguïté sur la loi de composition interne  $\star$  dont on parle, on pourra écrire avec un léger abus que «  $G$  est un groupe ».
2. Un groupe n'est jamais vide car il contient au moins son élément neutre.

#### Proposition 20 (Ensembles de nombres).

1.  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$  et  $(\mathbb{C}, +)$  sont des groupes abéliens.
2.  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{R}^*, \times)$  et  $(\mathbb{C}^*, \times)$  sont des groupes abéliens.

**Exemple 21** (Ce ne sont pas des groupes).

1.  $(\mathbb{N}, +)$  n'est pas un groupe car 1 n'est pas symétrisable : il n'a pas d'opposé dans  $\mathbb{N}$ .
2.  $(\mathbb{Z}^*, \times)$  n'est pas un groupe car 2 n'est pas inversible dans  $\mathbb{Z}^*$ .
3.  $(\mathbb{C}, \times)$  n'est pas un groupe car 0 n'a pas d'inverse dans  $\mathbb{C}$ .

**Exemple 22** (Vérifier les axiomes de groupe sur une loi artificielle).

On pose  $G = \mathbb{R}^* \times \mathbb{R}$ . Pour  $(a, b) \in G$  et  $(a', b') \in G$  on définit

$$(a, b) \star (a', b') = (aa', ab' + b).$$

Montrer que  $(G, \star)$  est un groupe

**Définition 23.**

Soit  $E$  un ensemble non vide. On appelle **permutation** de  $E$  une bijection  $\sigma : E \rightarrow E$ .  
On note  $S_E$  l'ensemble des permutations de  $E$ .

**Proposition-Définition 24.**

$(S_E, \circ)$  est un groupe, appelé **groupe des permutations** de  $E$ , ou encore *groupe symétrique* de  $E$ .  
Dès que  $E$  contient au moins 3 éléments, le groupe  $S_E$  n'est pas abélien.

**Proposition 25** (Produit de deux groupes).

Soient  $(G, \star)$  et  $(G', \top)$  deux groupes. On note  $e$  le neutre de  $G$  et  $e'$  celui de  $G'$ .  
Pour  $(x, x')$  et  $(y, y')$  deux éléments de  $G \times G'$ , on pose

$$(x, x') \heartsuit (y, y') := (x \star y, x' \top y').$$

Muni de la l.c.i.  $\heartsuit$ , le produit cartésien  $G \times G'$  est un groupe, d'élément neutre  $(e, e')$ .

**Proposition 26** (Produit de  $n$  groupes).

Soient  $G_1, \dots, G_n$   $n$  groupes (les l.c.i. étant sous-jacentes et notées multiplicativement).  
Pour  $(x_1, \dots, x_n)$  et  $(y_1, \dots, y_n)$  deux éléments de  $G_1 \times \dots \times G_n$ , on pose

$$(x_1, \dots, x_n) \heartsuit (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n).$$

Muni de la l.c.i.  $\heartsuit$ , le produit cartésien  $G_1 \times \dots \times G_n$  est un groupe.

Son neutre est le  $n$ -uplet  $(e_1, \dots, e_n)$  où pour tout  $k \in \llbracket 1, n \rrbracket$ ,  $e_k$  est le neutre du groupe  $G_k$ .

**Application** : définition du groupe additif  $(\mathbb{R}^n, +)$ , dont le neutre est le  $n$ -uplet  $(0, \dots, 0)$ .

## 2.2 Sous-groupes.

### Définition 27.

Soit  $(G, \star)$  un groupe et  $H$  une partie de  $G$ .

On dit que  $H$  est un **sous-groupe** de  $G$  si  $H$  est stable par  $\star$  et si  $(H, \star)$  est un groupe.

**Remarque.** Ci-dessus, lorsqu'on écrit  $(H, \star)$ , il faut comprendre que  $\star$  est la *loi induite* sur  $H$  par la loi  $\star$  définie sur  $G$ . Cette loi induite est bien définie car  $H$  est supposé stable par  $\star$ .

**Exemples.** Si  $(G, \star)$  est un groupe, de neutre  $e$ , alors  $\{e\}$  et  $G$  sont des sous-groupes de  $G$ . On pourra parler à leur sujet de *sous-groupes triviaux*.

### Proposition 28 (Élément neutre et inverses dans un sous-groupe).

Soit  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ .

1. L'élément neutre du groupe  $H$  n'est autre que celui de  $G$ .
2. Soit  $x \in H$ . L'inverse de  $x$  dans le groupe  $(H, \star)$  et celui dans le groupe  $(G, \star)$  sont égaux.

### Théorème 29 (Caractérisation des sous-groupes).

Soit  $(G, \star)$  un groupe dont l'élément neutre est noté  $e$ , et  $H$  une partie de  $G$ .

Les trois assertions suivantes sont équivalentes.

1.  $H$  est un sous-groupe de  $(G, \star)$ .
2. 
$$\begin{cases} \bullet e \in H \\ \bullet \forall (x, y) \in H^2 \quad x \star y^{-1} \in H. \end{cases}$$
3. 
$$\begin{cases} \bullet e \in H \\ \bullet \forall (x, y) \in H^2 \quad x \star y \in H \\ \bullet \forall x \in H \quad x^{-1} \in H. \end{cases}$$

**Remarque.** Récrivons une des équivalences ci-dessus dans le contexte où on utilise la notation additive. Soit  $(G, +)$  un groupe dont l'élément neutre est noté  $0$  et  $H$  une partie de  $G$ . On a

$$H \text{ est un sous-groupe de } (G, +) \iff \begin{cases} 0 \in H \\ \forall (x, y) \in H^2 \quad x - y \in H. \end{cases}$$

### Lemme 30 (Les sous-groupes sont stables par itération).

Soit  $H$  un sous-groupe d'un groupe  $G$  et  $x$  un élément de  $H$ . Alors,

$$\forall p \in \mathbb{Z} \quad x^p \in H.$$



**Proposition 31** (Ensembles de nombres).

1.  $(\mathbb{Q}, +)$  est un sous-groupe de  $(\mathbb{R}, +)$ , qui est lui-même un sous-groupe de  $(\mathbb{C}, +)$ .
2.  $\mathbb{R}_+^*$  est un sous-groupe de  $(\mathbb{R}^*, \times)$ .
3.  $\mathbb{U}$  et  $\mathbb{U}_n$  sont des sous-groupes de  $(\mathbb{C}^*, \times)$ .

**Exemple 32** (Centre d'un groupe).

Soit  $(G, \star)$  un groupe. On note

$$Z(G) = \{x \in G \mid \forall a \in G \quad x \star a = a \star x\}.$$

Montrer que  $Z(G)$  est un sous-groupe de  $G$ .

**Proposition 33** (Une intersection de sous-groupes est un sous-groupe).

Soient  $H$  et  $H'$  deux sous-groupes d'un groupe  $(G, \star)$ .

Leur intersection  $H \cap H'$  est un sous-groupe de  $G$ .

Plus généralement, si  $(H_i)_{i \in I}$  est une famille de sous-groupes d'un même groupe  $G$ , alors  $\bigcap_{i \in I} H_i$  est un sous-groupe de  $G$ .

**Exemple 34** (Une union de sous-groupes n'est pas (toujours) un sous-groupe).

Montrer que  $\mathbb{U}_2 \cup \mathbb{U}_3$  n'est pas un sous-groupe de  $(\mathbb{C}^*, \times)$  puis que  $\bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$  en est un.

**Proposition 35** (Sous-groupes de  $(\mathbb{Z}, +)$  (programme spé)).

Pour  $n \in \mathbb{N}$ , on note

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

Les sous-groupes de  $(\mathbb{Z}, +)$  sont exactement les  $n\mathbb{Z}$ , avec  $n \in \mathbb{N}$ .

Plus précisément,

1. Pour tout  $n \in \mathbb{N}$ ,  $n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .
2. Si  $H$  est un sous-groupe de  $(\mathbb{Z}, +)$  alors  $\exists! n \in \mathbb{N} \quad H = n\mathbb{Z}$ .

**Remarque.** On a croisé des sous-groupes de  $\mathbb{Z}$  dans le cours d'arithmétique. Si  $a$  et  $b$  sont deux entiers relatifs, on a

$$a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z} \quad \text{et} \quad a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z},$$

où on note  $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid (u, v) \in \mathbb{Z}^2\}$  l'ensemble des combinaisons de Bézout de  $a$  et  $b$ .

## 2.3 Morphismes de groupes.

### Définition 36.

Soient  $(G, \star)$  et  $(G', \top)$  deux groupes.

On appelle **morphisme de groupe** de  $G$  dans  $G'$  toute application  $f : G \rightarrow G'$  telle que

$$\forall (x, y) \in G^2 \quad f(x \star y) = f(x) \top f(y).$$

Si de surcroît  $f$  est bijective, on dit qu'une telle application  $f$  est un **isomorphisme** de groupes.

Un morphisme d'un groupe  $G$  vers lui même est appelé **endomorphisme** de  $G$ .

Si un tel endomorphisme est bijectif, on parle d'**automorphisme** de  $G$ .

### Définition 37.

On dit que deux groupes sont **isomorphes** s'il existe un isomorphisme du premier vers le deuxième.

### Exemple 38.

- L'exponentielle réelle est un isomorphisme de groupes de  $(\mathbb{R}, +)$  dans  $(]0, +\infty[, \times)$ .
- L'exponentielle complexe est un morphisme de groupes de  $(\mathbb{C}, +)$  dans  $(\mathbb{C}^*, \times)$ .
- $t \mapsto e^{it}$  est un morphisme de groupes de  $(\mathbb{R}, +)$  dans  $(\mathbb{U}, \times)$ .
- Le logarithme népérien est un isomorphisme de groupes de  $(]0, +\infty[, \times)$  dans  $(\mathbb{R}, +)$ .

### Exemple 39.

Justifier que les groupes  $(\mathbb{R}^2, +)$  et  $(\mathbb{C}, +)$  sont isomorphes.

### Proposition 40.

Soient  $G$  et  $G'$  deux groupes de neutres respectifs  $e$  et  $e'$ , et  $f : G \rightarrow G'$  un morphisme de groupes.

1.  $f(e) = e'$ .
2.  $\forall x \in G \quad f(x^{-1}) = (f(x))^{-1}$ .
3.  $\forall x \in G \quad \forall p \in \mathbb{Z} \quad f(x^p) = (f(x))^p$ .
4. Si  $H$  est un sous-groupe de  $G$  alors  $f(H)$  est un sous-groupe de  $G'$ .
5. Si  $H'$  est un sous-groupe de  $G'$ , alors  $f^{-1}(H')$  est un sous-groupe de  $G$ .
6. Si  $f$  est un isomorphisme de  $G$  vers  $G'$ , alors  $f^{-1}$  est un isomorphisme de  $G'$  vers  $G$ .

1. En notation additive, le point 2 s'écrit  $\forall x \in G \quad f(-x) = -f(x)$ .
2. En notation additive, le point 3 s'écrit  $\forall x \in G \quad \forall p \in \mathbb{Z} \quad f(px) = pf(x)$ .

**Définition 41.**

Soient  $G$  et  $G'$  deux groupes de neutres respectifs  $e$  et  $e'$ , et  $f : G \rightarrow G'$  un morphisme de groupes.

1. On appelle **noyau** de  $f$  et on note  $\text{Ker } f$  l'ensemble

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}.$$

2. On appelle **image** de  $f$  et on note  $\text{Im } f$  l'ensemble

$$\text{Im } f = \{y \in G' \mid \exists x \in G : y = f(x)\}.$$

**Proposition 42.**

Soient  $G$  et  $G'$  deux groupes de neutres respectifs  $e$  et  $e'$ , et  $f : G \rightarrow G'$  un morphisme de groupes.

1.  $\text{Ker } f$  est un sous-groupe de  $G$  et

$$f \text{ est injective} \iff \text{Ker } f = \{e\}.$$

2.  $\text{Im } f$  est un sous-groupe de  $G'$  et

$$f \text{ est surjective} \iff \text{Im } f = G'.$$

### 3 Structure d'anneau.

#### 3.1 Définitions et règles de calcul.

**Définition 43.**

On appelle **anneau** tout triplet  $(A, +, \times)$ , où  $A$  est un ensemble et  $+$  et  $\times$  des l.c.i. tels que

- $(A, +)$  est un groupe abélien, de neutre  $0_A$ .
- $(A, \times)$  est un magma associatif et unifère, de neutre  $1_A$ ,
- $\times$  est distributive par rapport à  $+$ .

Les lois  $+$  et  $\times$  sont appelées respectivement **addition** et **multiplication** de l'anneau  $A$ .

Si de surcroît  $\times$  est commutative, on dit que l'anneau  $A$  est commutatif.

**Remarques.** Soit  $(A, +, \times)$  un anneau.

1. Par définition des éléments neutres,  $\forall a \in A \quad a + 0_A = 0_A + a = a$  et  $1_A \times a = a \times 1_A = a$ .
2.  $(A, +)$  étant un groupe, tout élément  $a$  de  $A$  est symétrisable pour  $+$ , c'est-à-dire admet un opposé  $-a$  tel que  $a + (-a) = 0_A = (-a) + a$ .
3. En revanche, tout élément de  $A$  n'est pas nécessairement symétrisable (inversible) dans  $(A, \times)$  et c'est d'ailleurs ce qui empêche  $(A, \times)$  d'être un groupe.
4. Généralement,  $A$  possède plus de deux éléments, sauf si  $0_A = 1_A$  ( $A$  est alors réduit à  $\{0_A\}$ ).

**Exemples 44** (Ensembles de nombres).

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

**Exemple 45** (Anneau de fonctions).

On rappelle que, pour  $X$  une partie de  $\mathbb{R}$ ,  $\mathcal{F}(X, \mathbb{R})$ , ensemble des fonctions définies sur  $X$  et à valeurs réelles a été muni d'une addition et d'une multiplication  $+$  et  $\times$  de la manière suivante :

$$\forall f, g \in \mathcal{F}(X, \mathbb{R}) \quad f + g : \begin{cases} X & \rightarrow \mathbb{R} \\ x & \mapsto f(x) + g(x) \end{cases} \quad \text{et} \quad f \times g : \begin{cases} X & \rightarrow \mathbb{R} \\ x & \mapsto f(x)g(x) \end{cases} .$$

Le triplet  $(\mathcal{F}(X, \mathbb{R}), +, \times)$  est un anneau commutatif.

L'élément neutre pour  $+$  est la fonction nulle sur  $X$ .

L'élément neutre pour  $\times$  est la fonction constante sur  $X$  égale à 1.

En particulier  $(\mathbb{R}^{\mathbb{N}}, +, \times)$  est un anneau commutatif : celui des suites réelles.

**Exemples 46** (Pas des anneaux).

- $(2\mathbb{Z}, +, \times)$  n'est pas un anneau car...
- $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$  n'est pas un anneau car...

**Règles de calcul.** Soit  $(A, +, \times)$  un anneau.

On rappelle les faits ci-dessous concernant les itérés d'un élément pour l'addition et la multiplication.

1.  $(A, +)$  étant un groupe, le  $n$ ème itéré d'un élément  $a$ , noté  $na$ , est défini par

$$na = \underbrace{a + \dots + a}_{n \text{ termes}} \quad \text{si } n \geq 1 \quad \quad na = \underbrace{(-a) + \dots + (-a)}_{(-n) \text{ termes}} \quad \text{si } n \leq -1 \quad \quad \text{et} \quad 0a = 0_A.$$

On a aussi, pour tous  $(a, b) \in A^2$  et  $(p, q) \in \mathbb{Z}^2$ ,

$$pa + qa = (p + q)a, \quad p(qa) = (pq)a \quad \quad pa + pb = p(a + b),$$

la dernière égalité étant vraie par commutativité de  $+$ .

2.  $(A, \times)$  étant un magma associatif, le  $n$ ème itéré d'un élément  $x$ , noté  $a^n$ , est défini par

$$a^n = \underbrace{a \times \dots \times a}_{n \text{ facteurs}} \quad \text{si } n \geq 1 \quad \quad \text{et} \quad a^0 = 1_A.$$

On a aussi, pour tous  $(a, b) \in A^2$  et  $(m, n) \in \mathbb{N}^2$ ,

$$a^m \times a^n = a^{m+n}, \quad (a^m)^n = a^{mn},$$

**⚠** mais attention ! l'égalité  $(ab)^n = a^n b^n$  est FAUSSE en général si  $\times$  n'est pas commutative.

3. Si  $a$  est un élément inversible dans  $A$ , on peut alors définir la puissance  $n$ ème de  $a$  pour  $n$  strictement négatif par  $a^n = (a^{-1})^{-n}$ . Les identités de (2) sont alors vraies pour  $(m, n) \in \mathbb{Z}^2$ .

**Proposition 47.**

Soit  $(A, +, \times)$  un anneau. En utilisant la notation multiplicative pour la loi  $\times$ ,

1.  $\forall a \in A \quad 0_A \times a = a \times 0_A = 0_A$ .
2.  $\forall (a, b) \in A^2 \quad a(-b) = (-a)b = -(ab)$ .
3.  $\forall (a, b) \in A^2 \quad (-a)(-b) = ab$ .
4.  $\forall (a, b) \in A^2 \quad \forall n \in \mathbb{Z} \quad a(nb) = (na)b = n(ab)$ .

**Proposition 48** (Identités remarquables : si ça commute, d'accord).

Soit  $(A, +, \times)$  un anneau et  $(a, b) \in A^2$ .

1. Si  $ab = ba$ , alors  $\forall n \in \mathbb{N} \quad (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ .
2. Si  $ab = ba$ , alors  $\forall n \in \mathbb{N}^* \quad a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$ .

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

**3.2 Groupe des inversibles dans un anneau.****Définition 49.**

Dans un anneau  $(A, +, \times)$ , les **inversibles** sont les éléments de  $A$  inversibles pour la loi  $\times$ .

L'ensemble des éléments de  $A$  qui sont inversibles sera noté  $U(A)$ , ou encore  $A^\times$ .

**Exemples 50.**

- $U(\mathbb{Z}) = \{-1, 1\}$ .
- $U(\mathbb{R}) = \mathbb{R}^*$ .
- Pour  $X$  une partie de  $\mathbb{R}$ ,  $U(\mathcal{F}(X, \mathbb{R}))$  est l'ensemble des fonctions *ne s'annulant pas* sur  $X$ .

**Proposition 51.**

Si  $(A, +, \times)$  est un anneau,  $(U(A), \times)$  est un groupe. On l'appelle **groupe des inversibles**.  
On a notamment

$$\forall (a, b) \in (U(A))^2 \quad ab \text{ est inversible} \quad \text{et} \quad (ab)^{-1} = b^{-1}a^{-1},$$

### 3.3 Nilpotents dans un anneau.

#### Définition 52.

Dans un anneau  $(A, +, \times)$  on dit d'un élément  $a \in A$  qu'il est **nilpotent** s'il possède une puissance nulle, c'est-à-dire

$$\exists p \in \mathbb{N}^* \quad a^p = 0_A.$$

#### Exemple 53.

Soit  $(A, +, \times)$  un anneau et  $(a, b) \in A^2$ .

1. Montrer que si  $a$  est nilpotent et si  $b$  commute avec  $a$ , alors  $ab$  est nilpotent.
2. Montrer que si  $ab$  est nilpotent, alors  $ba$  est nilpotent.

#### Exemple 54.

Soit  $(A, +, \times)$  un anneau non réduit à  $\{0_A\}$  et  $a \in A$  un élément nilpotent.

1. Montrer que  $a$  n'est pas inversible.
2. Montrer  $1_A - a$  est inversible et exprimer son inverse.

### 3.4 Sous-anneaux, morphismes d'anneaux.

#### Proposition-Définition 55.

Soit  $(A, +, \times)$  un anneau et  $B$  une partie de  $A$ . On dit que  $B$  est un **sous-anneau** de  $A$  si

- $\forall (a, b) \in B^2 \quad a - b \in B$ ,
- $\forall (a, b) \in B^2 \quad ab \in B$ ,
- $1_A \in B$ .

Muni des lois induites par  $+$  et  $\times$ ,  $B$  est un anneau.

#### Exemples 56.

- $A$  est un sous-anneau de  $A$ . Si  $0_A \neq 1_A$ , alors  $\{0_A\}$  n'est pas un sous-anneau de  $A$
- Montrer que  $\mathbb{Z}$  est le seul sous-anneau de  $\mathbb{Z}$ .

#### Exemple 57 (Anneau de Gauss).

Soit l'ensemble

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}.$$

Montrer que  $(\mathbb{Z}[i], +, \times)$  est un anneau commutatif et déterminer ses éléments inversibles.

**Définition 58.**

Soient  $(A, +, \times)$  et  $(A', +, \times)$  deux anneaux.

On appelle **morphisme d'anneaux** de  $A$  dans  $A'$  toute application  $f : A \rightarrow A'$  telle que

- $\forall (a, b) \in A^2 \quad f(a + b) = f(a) + f(b),$
- $\forall (a, b) \in A^2 \quad f(ab) = f(a)f(b),$
- $f(1_A) = 1_{A'}.$

Si de surcroît  $f$  est bijective, on dit qu'une telle application  $f$  est un **isomorphisme** d'anneaux.

**Exemple 59.**

La conjugaison

$$\text{conj} : \begin{cases} \mathbb{C} & \rightarrow \mathbb{C} \\ z & \mapsto \bar{z} \end{cases}$$

est un isomorphisme de l'anneau  $(\mathbb{C}, +, \times)$  dans lui-même.

**3.5 Anneaux intègres.****Définition 60.**

Soit  $(A, +, \times)$  un anneau. On dit d'un élément  $a$  de  $A$  qu'il est un **diviseur de zéro** si  $a \neq 0_A$  et s'il existe un élément  $b$  dans  $A \setminus \{0_A\}$  tel que  $ab = ba = 0_A$ .

**Exemples 61.**

- Dans l'anneau  $(\mathbb{Z}, +, \times)$ , il n'y a pas de diviseurs de zéro.
- Dans l'anneau  $(\mathbb{R}^{\mathbb{R}}, +, \times)$ , il existe des diviseurs de zéro. En exhiber un.

**Définition 62.**

On appelle anneau **intègre** tout anneau commutatif sans diviseurs de 0. Dans un tel anneau,

$$\forall (a, b) \in A^2 \quad (ab = 0_A) \implies (a = 0_A \text{ ou } b = 0_A).$$

**Exemples 63.**

$\mathbb{Z}$  est un anneau intègre.

Dans les chapitres suivants, nous définirons deux anneaux importants :

- l'anneau des polynômes,  $\mathbb{K}[X]$ , qui sera un anneau intègre,
- pour  $n \geq 2$ , l'anneau de matrices  $M_n(\mathbb{K})$ , qui ne sera *pas* intègre.

## 4 Structure de corps.

### 4.1 Définitions et exemples.

#### Définition 64.

On appelle **corps** tout anneau commutatif  $(K, +, \times)$ , non réduit à  $\{0_K\}$ , dans lequel tout élément non nul est inversible.

Par définition, si  $K$  est un corps,  $U(K) = K \setminus \{0_K\}$ . Ce groupe commutatif pourra être noté  $K^*$ .

**Exemples.**  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$  et  $(\mathbb{C}, +, \times)$  sont des corps.

#### Proposition 65.

Tout corps est un anneau intègre. La réciproque est fausse.

#### Exemple 66.

Soit

$$\mathbb{Q}[\sqrt{2}] = \left\{ x \in \mathbb{R} \mid \exists (a, b) \in \mathbb{Q}^2, x = a + b\sqrt{2} \right\}.$$

Montrer que  $\mathbb{Q}[\sqrt{2}]$  est un corps.

### 4.2 Notation fractionnaire dans un corps.

Soit  $(K, +, \times)$  un corps.

Soient  $a \in K$  et  $b \in K^*$ .  $b$  est inversible donc  $b^{-1}$  existe.  $K$  étant commutatif, on a  $ab^{-1} = b^{-1}a$ .

$$\text{L'élément } ab^{-1} \text{ est noté } \frac{a}{b}.$$

Pour  $(a, c) \in K^2$  et  $(b, d) \in (K^*)^2$ , on peut vérifier que

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \quad \frac{a}{b} = \frac{c}{d} \iff ad = bc \quad \frac{1}{a} = a^{-1}.$$

### 4.3 Corps des fractions d'un anneau intègre.

#### Théorème 67.

Pour tout anneau intègre  $A$ , il existe un unique corps commutatif  $K$  contenant  $A$  et vérifiant

$$\forall x \in K \quad \exists a \in A \exists b \in A \setminus \{0_A\} \quad x = \frac{a}{b}.$$

Le corps  $K$  est appelé **corps des fractions** de l'anneau  $A$ .

**Exemple.** Le corps des fractions de  $\mathbb{Z}$  n'est autre que  $\mathbb{Q}$ .



## Exercices

On rappelle que les exemples du cours (et ils sont nombreux dans celui-ci) sont autant d'exercices classiques (et corrigés) : n'hésitez pas à les refaire !

### Groupes, sous-groupes, morphismes de groupes.

**19.1** [◆◆◆] Soit  $(G, \star)$   $p \in \mathbb{N}^*$  et  $a_1, \dots, a_p$  des éléments de  $G$ . Quel est le symétrique de

$$a_1 \star a_2 \star \dots \star a_p?$$

---

**19.2** [◆◆◆] Soit  $(a_n)_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ . Posons

$$H = \{x \in \mathbb{R} \mid \cos(a_n x) \rightarrow 1\}.$$

Montrer que  $H$  est un sous-groupe de  $(\mathbb{R}, +)$ .

---

**19.3** [◆◆◆] Soient  $(G, \star)$  un groupe et  $H$  un sous-groupe de  $G$ . Pour  $a \in G$ , on pose

$$aHa^{-1} = \{a \star h \star a^{-1} \mid h \in H\}.$$

Montrer que  $aHa^{-1}$  est un sous-groupe de  $G$ .

---

**19.4** [◆◆◆] Soit  $(G, \star)$  un groupe et  $f$  la fonction  $x \mapsto x^{-1}$ , application de  $G$  dans lui-même. Démontrer que  $f$  est un morphisme de groupes si et seulement si  $G$  est abélien.

---

**19.5** [◆◆◆] Soit l'ensemble d'applications  $G = \{x \mapsto ax + b \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$ .

En vous appuyant sur un groupe connu, montrer que  $(G, \circ)$  est un groupe.

---

**19.6** [◆◆◆] Soit  $G$  un groupe noté multiplicativement, et  $H$  et  $K$  deux sous-groupes de  $G$ . On définit

$$HK = \{x \in G \mid \exists h \in H \exists k \in K, x = hk\} \quad \text{et} \quad KH = \{x \in G \mid \exists k \in K \exists h \in H, x = kh\}.$$

Démontrer l'équivalence entre

1.  $HK$  et  $KH$  sont des sous-groupes de  $G$ .
  2.  $HK = KH$ .
- 

**19.7** [◆◆◆] [Sous-groupes de  $(\mathbb{R}, +)$ ]

Montrer que si  $H$  est un sous-groupe de  $(\mathbb{R}, +)$ , alors

- ou bien il existe un réel  $a$  positif tel que  $H = a\mathbb{Z}$ , en notant  $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$ ,
  - ou bien  $H$  est dense dans  $\mathbb{R}$ .
- 

**19.8** [◆◆◆] Pour  $x$  et  $y$  dans  $] -1, 1[$ , on pose  $x \star y = \frac{x+y}{1+xy}$ . Montrer que  $(] -1, 1[, \star)$  est un groupe abélien.

---

**19.9** [◆◆◆] Soit  $G$  un groupe noté multiplicativement. Pour  $a \in G$ , on pose  $\tau_a : x \mapsto ax$ .

1. Pour tout  $a \in G$ , montrer que  $\tau_a \in S_G$ .
  2. Montrer que  $a \mapsto \tau_a$  est un morphisme injectif de  $G$  dans  $S_G$ .
- 

**19.10** [◆◆◆] Démontrer que  $(\mathbb{C}^*, \times)$  est isomorphe à  $(\mathbb{R}_+^* \times \mathbb{U}, \times)$ .

---

---

**19.11** [◆◆◆] Soit  $G$  un groupe. Montrer qu'une partie  $H$  finie, non vide et stable par la loi de  $G$  est nécessairement un sous-groupe de  $G$ .

---

**19.12** [◆◆◆] Soit  $(G, \cdot)$  un groupe. On note  $\text{Aut}(G)$  l'ensemble des automorphismes de  $G$ . Pour  $g \in G$ , on note  $\sigma_g$  l'application  $x \mapsto gxg^{-1}$ .

1. Démontrer que  $(\text{Aut}(G), \circ)$  est un groupe.
  2. Montrer que pour tout  $g \in G$ ,  $\sigma_g \in \text{Aut}(G)$ .
  3. Démontrer que l'application  $\sigma : g \mapsto \sigma_g$  est un morphisme de groupes de  $G$  dans  $\text{Aut}(G)$ .
  4. Montrer que  $\text{Ker}(\sigma) = Z(G)$ , où  $Z$  est le centre de  $G$ .
- 

**19.13** [◆◆◆] Soit  $(G, \cdot)$  un groupe fini et  $\chi$  un morphisme de groupes de  $(G, \cdot)$  dans  $(\mathbb{C}^*, \times)$ . Calculer

$$S = \sum_{x \in G} \chi(x).$$


---

**19.14** [◆◆◆] Soit  $(G, \star)$  un groupe et  $x$  un élément de  $G$ . On note  $\langle x \rangle$  l'ensemble des itérés de  $x$  :

$$\langle x \rangle = \{x^p \mid p \in \mathbb{Z}\}.$$

1. Montrer que  $\langle x \rangle$  est un sous-groupe de  $G$ . On l'appelle sous-groupe engendré par  $x$ .
  2. Prouver que c'est le plus petit sous-groupe de  $G$  contenant  $x$ .
- 

**19.15** [◆◆◆] Soit  $(E, \star)$  un magma associatif fini.

Démontrer qu'il existe dans  $E$  un élément idempotent, c'est-à-dire un élément  $x$  tel que  $x^2 = x$ .

---

## Anneaux, corps.

**19.16** [◆◆◆]

Montrer que dans un anneau, la somme de deux éléments nilpotents qui commutent est nilpotent.

---

**19.17** [◆◆◆] Soit  $(A, +, \times)$  un anneau. On suppose qu'il existe deux éléments  $a, b$  de  $A$  tels que

$$ab + ba = 1_A \quad \text{et} \quad a^2b + ba^2 = a$$

1. Montrer que  $a^2b = ba^2$  et  $2aba = a$ .
  2. Montrer que  $a$  est inversible et que  $a^{-1} = 2b$ .
- 

**19.18** [◆◆◆] Soit  $E$  un ensemble. On définit sur  $E$  la différence symétrique

$$\Delta : \begin{cases} E \times E & \rightarrow E \\ (A, B) & \mapsto A\Delta B = (A \cup B) \setminus (A \cap B) \end{cases}.$$

1. Montrer que  $(\mathcal{P}(E), \Delta)$  est un groupe commutatif.
  2. Montrer que  $(\mathcal{P}(E), \Delta, \cap)$  est un anneau commutatif.
  3. Démontrer que si  $E$  possède au moins deux éléments, alors l'anneau  $(\mathcal{P}(E), \Delta, \cap)$  n'est pas intègre.
- 

**19.19** [◆◆◆] Soit  $(A, +, \times)$  un anneau commutatif fini.

Démontrer que  $A$  est un corps si et seulement si il possède exactement un élément nilpotent et exactement deux éléments idempotents (éléments  $x$  tels que  $x^2 = x$ ).

---