

---

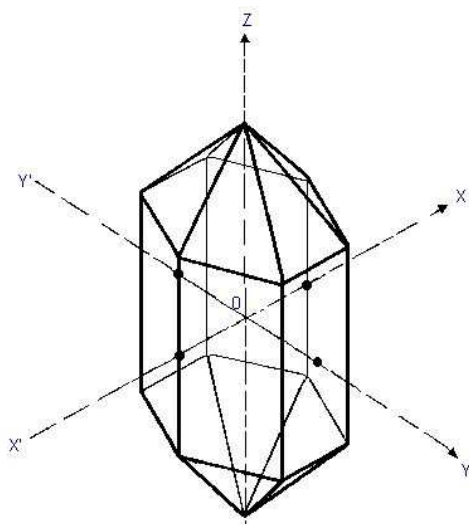
# Les structures algébriques

MPSI Prytanée National Militaire

---

Pascal Delahaye

24 janvier 2018



Dans ce cours, nous présentons les structures que vérifient les principaux ensembles utilisés en mathématiques.

## 1 Loi de composition interne

**DÉFINITION 1 : Loi de composition interne**

Soit  $E$  un ensemble. On appelle *loi de composition interne* une application de  $E \times E$  dans  $E$  :

$$\begin{aligned} \phi : E \times E &\longrightarrow E \\ (a, b) &\longmapsto \phi(a, b) \end{aligned}$$

Pour simplifier les notations, on pourra par exemple noter :  $\phi(a, b) = a \star b$

L'ensemble  $E$  muni de la loi  $\star$  est noté  $(E, \star)$  : on dit alors que c'est un *magma*.

*Remarque 1.*

1. Soient  $a$  et  $b$  deux éléments de  $E$ .

Il n'y a aucune raison pour que  $\phi(a, b) = \phi(b, a)$ , c'est à dire que  $a \star b = b \star a$ .

2. On peut itérer une loi : si  $(a, b, c) \in E^3$ . On notera : 
$$\begin{cases} \phi(\phi(a, b), c) = (a \star b) \star c \\ \phi(a, \phi(b, c)) = a \star (b \star c) \end{cases}$$

Il n'y a a priori aucune raison pour  $(a \star b) \star c = a \star (b \star c)$ .

⚠⚠⚠. Au lieu de  $\star$ , la lci sera souvent notée " + ", "  $\times$  " ou " . ".

Mais attention : ces notations n'auront souvent rien à voir avec l'addition et la multiplication dans  $\mathbb{R}$ . On réservera en général la notation " + " lorsque la lci sera commutative.

**Exemple 1.**

- |                                                          |                                             |               |
|----------------------------------------------------------|---------------------------------------------|---------------|
| 1. Sur $\mathbb{N}$ ,                                    | la multiplication et l'addition des entiers | sont des lci. |
| 2. Sur $E = \mathcal{F}(G, G)$ (où $G$ est un ensemble), | la composition des applications             | est une lci.  |
| 3. Sur $\mathcal{P}(G)$ (où $G$ est un ensemble),        | l'union et l'intersection                   | sont des lci. |
| 4. Sur $\mathbb{R}^{\mathbb{N}}$ ,                       | la multiplication et l'addition             | sont des lci. |
| 5. Sur $\mathbb{R}^3$ ,                                  | le produit vectoriel                        | est une lci.  |

**DÉFINITION 2 : Propriétés possibles d'une lci**

Soit  $\star$  une lci sur un ensemble  $E$ .

On dit que  $\star$  est :  $\begin{cases} \textit{commutative} & \text{lorsque } \forall(a, b) \in E^2, & a \star b = b \star a \\ \textit{associative} & \text{lorsque } \forall(a, b, c) \in E^3, & a \star (b \star c) = (a \star b) \star c \end{cases}$

*Remarque 2.* Le produit vectoriel de  $\mathbb{R}^3$  n'est ni commutatif, ni associatif.

**DÉFINITION 3 :** Si une lci est *associative*, on peut définir les notations suivantes :

- |                                                 |            |                                                   |
|-------------------------------------------------|------------|---------------------------------------------------|
| 1) Lorsque la loi est notée additivement,       | on définit | $\sum_{i=1}^n x_i = x_1 + \dots + x_n$            |
| 2) Lorsque la loi est notée multiplicativement, | on définit | $\prod_{i=1}^n x_i = x_1 \times \dots \times x_n$ |

**DÉFINITION 4 : Élément Neutre**

Un élément  $e \in E$  est dit *neutre* ssi  $\forall x \in E, e \star x = x \star e = x$

- Si la loi est noté " + " alors l'élément neutre de  $E$  sera noté  $0_E$  (ou 0 s'il n'y a pas d'ambiguïté).
- Si la loi est noté "  $\times$  " alors l'élément neutre de  $E$  sera noté  $1_E$  (ou 1 s'il n'y a pas d'ambiguïté).

Pour mq $\star$ est commutative :	Pour mq $\star$ est associative :	Pour mq $e \in E$ est neutre :
1. Soit $(x, y) \in E^2$	1. Soit $(x, y, z) \in E^3$	1. Soit $x \in E$
2. Mq : $x \star y = y \star x \dots$	2. Mq : $x \star (y \star z) = (x \star y) \star z$	2. Mq : $e \star x = x$ et $x \star e = x$
3. Donc $\star$ est commutative	...	...
	3. Donc $\star$ est associative	3. Donc $e$ est neutre.

*Remarque 3.*

- Pour deviner la forme de l'élément neutre, on pourra procéder à une analyse.
- Si la loi est commutative, il suffit de prouver que  $\forall x \in G, x \star e = x$  pour prouver que  $e$  est élément neutre.

**Exemple 2.**

- |                                                     |                                                       |                                                              |
|-----------------------------------------------------|-------------------------------------------------------|--------------------------------------------------------------|
| 1. $(\mathbb{N}, +)$ :                              | + est une lci commutative et associative,             | 0 est l'unique élément neutre                                |
| 2. $(\mathbb{N}, \times)$ :                         | $\times$ est une lci commutative et associative,      | 1 est l'unique élément neutre                                |
| 3. $(\mathcal{F}(\mathbb{R}, \mathbb{R}), \circ)$ : | $\circ$ est une lci associative mais pas commutative, | l'application $\text{id}_{\mathbb{R}}$ est un élément neutre |
| 4. $(\mathcal{P}(G), \cup)$ :                       | $\cup$ est une lci commutative, associative,          | la partie $\emptyset$ est neutre pour cette loi.             |
| 5. $(\mathfrak{M}_{n,p}(\mathbb{R}), +)$ :          | + est une lci commutative, associative                | la matrice nulle est élément neutre.                         |
| 6. $(\mathfrak{M}_n(\mathbb{R}), \times)$ :         | $\times$ est une lci associative mais non commutative | la matrice $I_n$ est élément neutre.                         |

**Exercice : 1**

(\*) Soit  $\mathbb{R}^2$  muni de la loi  $\star$  définie par  $(x, y) \star (x', y') = (xx' - yy', xy' + yx')$ .

Montrer que  $\star$  est une lci, commutative, associative et admettant un élément neutre à déterminer.

**THÉORÈME 1 : Unicité de l'élément neutre**

Si  $(E, \star)$  possède un élément neutre, il est unique.

*Preuve 1 :* On considère  $e$  et  $e'$  deux éléments neutres et on montre facilement qu'ils sont identiques.

**DÉFINITION 5 : Monoïde**

Un ensemble  $(E, \star)$  muni d'une loi associative et admettant un élément neutre est appelé un monoïde.

**Exemple 3.**  $(\mathbb{N}, +)$  est un monoïde d'élément neutre 0.

**Exemple 4.** On considère un ensemble fini  $A$  appelé *alphabet*, et on définit un *mot* sur  $A$  comme étant une suite finie de *lettres* de  $A$ . On notera  $m = a_1 \dots a_n$  un tel mot. On définit également le mot vide  $\varepsilon$ . Sur l'ensemble  $A^*$  des mots de  $A$ , on définit une loi appelée la *concaténation* de deux mots de la façon suivante : si  $m_1 = a_1 \dots a_n$  et si  $m_2 = b_1 \dots b_p$ , on note  $m_1.m_2 = a_1 \dots a_n b_1 \dots b_p$ . Alors l'ensemble des mots muni de la concaténation,  $(A^*, \cdot)$  admet pour élément neutre le mot vide  $\varepsilon$ . La loi étant associative, cet ensemble muni de cette loi est un monoïde très utilisé en informatique théorique et en théorie des langages.

**DÉFINITION 6 : Inverse**

On suppose que  $(E, \star)$  possède un élément neutre  $e$ . Soit un élément  $x \in E$ .

On dit qu'un élément  $y \in E$  est un *inverse* de l'élément  $x$  ssi :  $x \star y = y \star x = e$

Dans ce cas, on dit aussi que  $x$  est *inversible*.

1. Si la loi est notée "+" alors l'inverse de  $x$  (alors appelé l'*opposé*) est noté  $-x$
2. Si la loi est notée "." ou "×" ou "★" alors l'inverse de  $x$  est noté  $x^{-1}$

*Remarque 4.* Impossible de s'intéresser aux inverses des éléments de  $(E, \star)$  si l'on n'a pas prouvé auparavant l'existence d'un élément neutre.

**Exemple 5.**

1. Dans  $(\mathbb{Z}, +)$  tous les éléments admettent un inverse, en revanche, dans  $(\mathbb{N}, +)$  seul 0 admet un inverse.
2. Dans  $(\mathbb{Q}, \times)$ ,  $(\mathbb{R}, \times)$  et  $(\mathbb{C}, \times)$  tous les éléments non nuls admettent un inverse.
3. Dans  $(\mathbb{Z}, \times)$  seuls 1 et  $-1$  admettent un inverse.
4. Dans  $(\mathfrak{M}_n(\mathbb{R}), \times)$  seuls les matrices inversibles admettent un inverse.

**Exemple 6.** Déterminer les éléments des ensembles suivants admettant un inverse.

1.  $(P(E), \cap)$
2.  $(P(E), \cup)$
3.  $(\mathbb{R}^{\mathbb{N}}, +)$
4.  $(\mathbb{R}^{\mathbb{N}}, \times)$
5.  $(\mathbb{R}^{\mathbb{R}}, \circ)$
6.  $(\mathbb{R}^{\mathbb{R}}, \times)$
7.  $(\mathbb{R}^{\mathbb{R}}, +)$

**THÉORÈME 2 : Unicité de l'inverse**

Dans un monoïde  $(E, \star)$ , si un élément  $x \in E$  possède un inverse, cet inverse est unique.

*Preuve 2 :* Très facile ! On suppose qu'il y en a deux ...

Pour déterminer si un élément  $x$  admet un inverse :

1. On commence par une analyse pour déterminer la forme de cet inverse  $y$
2. On vérifie alors que  $y \in E$  et que  $\begin{cases} x \star y = e \\ y \star x = e \end{cases}$ .

*Si la loi  $\star$  est commutative, on peut se contenter de démontrer que  $x \star y = e$*

*Remarque 5.*

1. Lorsqu'on sait que  $x \in (E, \star)$  admet un inverse alors  $x \star y = e$  suffit à prouver que  $y$  est l'inverse de  $x$ .
2. Si un élément  $x \in E$  possède un inverse  $y \in E$ , alors l'élément  $y$  possède également un inverse qui est l'élément  $x$ . En d'autres termes, nous avons :  $(x^{-1})^{-1} = x$  ou  $-(-x) = x$

*Remarque 6.* L'élément neutre est toujours son propre inverse :  $e^{-1} = e$ .

**PROPOSITION 3 : Inversibilité du produit de deux éléments inversibles**

Soit  $a, b$  deux éléments inversibles d'un monoïde  $E, \star$ .

Alors :

$$a \star b \text{ est inversible} \quad \text{et} \quad (a \star b)^{-1} = b^{-1} \star a^{-1}$$

*Preuve 3 :* Simple vérification.

*Remarque 7.*

⚠  $\star$  n'étant pas toujours commutative, il faut impérativement respecter l'ordre des éléments  $b^{-1}$  et  $a^{-1}$ .

**DÉFINITION 7 : Partie stable par une lci**

Soit  $\star$  une lci sur un ensemble  $E$  et  $F \subset E$  non vide.

On dira que  $F$  est *stable* par la lci  $\star$  lorsque :

$$\forall a, b \in F, \quad a \star b \in F$$

## 2 Structure de groupe

### 2.1 Définition d'un groupe

**DÉFINITION 8 : Groupe**

Soient un ensemble  $G$  et  $\star$  une loi sur  $G$ . On dit que  $(G, \star)$  est un *groupe* si :

- |                                   |                                                      |
|-----------------------------------|------------------------------------------------------|
| 1. la loi $\star$ est une lci     | 3. $G$ possède un élément neutre pour cette loi      |
| 2. la loi $\star$ est associative | 4. Tout élément $x$ de $G$ admet un inverse dans $G$ |

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

**Exemple 7.** Les groupes de référence ( $E$  est ici un ensemble quelconque non vide) :

- Groupes additifs :  $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathcal{F}(E, \mathbb{R}), +), (\mathbb{R}^N, +), (\mathfrak{M}_{n,p}(\cdot), +)$ .
- Groupes multiplicatifs :  $(\mathbb{Q}^*, \times), (\mathbb{Q}^{*+}, \times), (\mathbb{R}^*, \times), (\mathbb{R}^{*+}, \times), (\mathbb{C}^*, \times), (\mathbb{U}, \times), (\mathbb{U}_n, \times), (\mathcal{B}(E, E), \circ), (\mathcal{GL}_n(\mathbb{R}), \times)$ .

**DÉFINITION 9 : Groupe des permutations d'un ensemble**

Si  $E$  est un ensemble fini non vide, alors :

$$\mathcal{B}(E, E) \quad \text{est appelé} \quad \text{le groupe des permutations de l'ensemble } E$$

On note alors :  $\mathcal{S}_E = \mathcal{B}(E, E)$ .

*Remarque 8.*

- Un groupe est donc un monoïde dont tous les éléments sont inversibles.
- Si  $E$  un ensemble non vide,  $(\mathcal{S}_E, \circ)$  est un exemple de groupe non abélien.

*Remarque 9.* Notations et propriétés :

Avec la notation Multiplicative $(G, \cdot)$	Avec la notation Additive $(G, +)$
<p><b>Notations</b></p> $\forall n \in \mathbb{N}^*, a^n = \underbrace{a.a.\dots.a}_n \quad \text{et} \quad a^0 = e_G$ $\forall n \in \mathbb{N}^*, a^{-n} = (a^n)^{-1}$	<p><b>Notations</b></p> $\forall n \in \mathbb{N}^*, na = \underbrace{a + a + \dots + a}_n \quad \text{et} \quad 0a = e_G$ $\forall n \in \mathbb{N}^*, (-n)a = -(na)$
<p><b>Propriétés</b></p> $(a.b)^{-1} = b^{-1}.a^{-1}$ $\forall n \in \mathbb{Z}^*, a^n = (a^{-n})^{-1} = (a^{-1})^{-n}$ $\forall (n, m) \in \mathbb{Z}^{*2}, a^{n+m} = (a^n).(a^m)$ $\forall (n, m) \in \mathbb{Z}^{*2}, (a^n)^m = a^{n.m}$	<p><b>Propriétés</b></p> $-(a + b) = (-b) + (-a)$ $\forall n \in \mathbb{Z}^*, na = -(-na) = (-n).(-a)$ $\forall (n, m) \in \mathbb{Z}^{*2}, (n + m)a = na + ma$ $\forall (n, m) \in \mathbb{Z}^{*2}, m(na) = (mn)a$

⚠⚠⚠. Les propriétés  $\begin{cases} (a.b)^n = a^n.b^n \\ n(a + b) = na + nb \end{cases}$  ne sont valables que si la loi est commutative!

## 2.2 Sous-groupes

**DÉFINITION 10 :** Soit  $(G, \star)$  un groupe.

Les sous-groupes de  $G$  sont les sous-ensembles  $H$  de  $G$  tels que  $(H, \star)$  sont des groupes.

**Exemple 8.**

- Si  $(G, \star)$  est un groupe, alors  $(\{e_G\}, \star)$  et  $(G, \star)$  sont 2 sous-groupes de  $(G, \star)$ .
- $(C^0(\mathbb{R}, \mathbb{R}), +)$  est un sous groupe de  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +)$

**PROPOSITION 4 : Caractérisation des Sous-groupes**

Soit  $(G, \star)$  un groupe.  $(H, \star)$  est un *sous-groupe* de  $G$  ssi :

- $H$  est une partie de  $G$
- Elément Neutre :  $e_G \in H$
- Stabilités :
  - $H$  est *stable* par la lci :  $\forall (x, y) \in H^2, x \star y \in H$ .
  - $H$  est stable par *symétrisation* :  $\forall x \in H, x^{-1} \in H$ . (ou  $-x \in H$  avec la notation additive)

*Preuve 4 :* Pas de difficulté, sauf peut-être pour prouver que  $e_G \in H$ .

$H$  étant un sous-groupe, alors il admet un élément neutre noté  $e_H$ . Prouvons que  $e_H = e_G$ .

On a :  $\begin{cases} e_H \star e_H = e_H \\ e_H \star e_G = e_H \end{cases}$  donc  $e_H \star e_H = e_H \star e_G$  et en composant par  $e_H^{-1}$  on obtient  $e_H = e_G$ .

*Remarque 10.*

- L'avantage de cette caractérisation par rapport à la définition est qu'elle nous dispense de vérifier l'associativité de la loi  $\star$ .
- Si  $e_g$  n'appartient pas à  $H$  alors  $H$  ne peut pas être un sous-groupe de  $G$ .  
Ainsi  $(2\mathbb{Z} + 1, +)$  n'est pas un sous-groupe de  $(\mathbb{Z}, +)$ .

Ainsi, pour montrer que  $H$  est un sous-groupe du groupe  $(G, \star)$ , on procède en **4 étapes** :

- On vérifie que :  $H \subset G$
- On vérifie que :  $e_G \in H$
- Stabilité par  $\star$  : Soit  $(x, y) \in H^2$ , on vérifie que  $x \star y \in H$
- Stabilité par symétrisation : Soit  $x \in H$ , on vérifie que  $x^{-1} \in H$

**Exemple 9.** Prouver que  $(\mathbb{U}, \times)$  est un sous-groupe de  $(\mathbb{C}^*, \times)$  où  $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ .

**Exercice : 2**

(\*\*) Montrer que les sous-groupes de  $(\mathbb{Z}, +)$  sont les  $(n\mathbb{Z}, +)$  où  $n \in \mathbb{Z}$ .

**Exercice : 3**

(\*\*\*) **Les sous-groupes de  $(\mathbb{R}, +)$**

Soit  $H$  un sous-groupe de  $\mathbb{R}$  non réduit au singleton  $\{0\}$ .

1. Montrer que  $H \cap \mathbb{R}^{++}$  admet une borne inférieure. On la notera  $a$ .
2. Si  $a$  est en fait le minimum de  $H \cap \mathbb{R}^{++}$ , montrer que  $H$  est le sous-groupe  $a\mathbb{Z}$ .
3. Si  $H \cap \mathbb{R}^{++}$  n'admet pas de minimum, montrer, par l'absurde, que  $a$  est nul puis que  $H$  est alors dense dans  $\mathbb{R}$ .

**Exercice : 4**

(\*) Soit un ensemble  $E$  non-vide et un élément  $a \in E$ . On note  $G = \{f \in \mathcal{B}(E, E), \text{ tq } f(a) = a\}$

$C$  est l'ensemble des bijections de  $G$  laissant invariant l'élément  $a$ .

Montrer que  $(G, \circ)$  est un groupe.

**Exercice : 5**

(\*) Soit  $(G, \cdot)$  un groupe. On note  $C = \{x \in G \mid \forall g \in G, g \cdot x = x \cdot g\}$

$C$  est l'ensemble des éléments de  $G$  qui commutent avec tous les éléments de  $G$ .

Montrer que  $(C, \cdot)$  est un sous-groupe de  $G$  (appelé *centre* du groupe  $G$ ).

#### DÉFINITION 11 : Morphisme de groupes

Soit  $f : G_1 \rightarrow G_2$  une application.

On dit que  $f$  est un *morphisme* de groupes si et seulement si :

1.  $(G_1, \star)$  et  $(G_2, \bullet)$  sont deux groupes
2.  $\forall (x, y) \in G_1^2, \quad f(x \star y) = f(x) \bullet f(y)$

*Remarque 11.* Un morphisme d'un groupe  $G$  vers lui-même est appelé un *endomorphisme* de groupes.

**Exemple 10.** Vous souvenez-vous du morphisme de groupes surjectif de  $(\mathbb{R}, +)$  dans  $(\mathbb{U}, \times)$  ?

Pour montrer que  $f : G_1 \mapsto G_2$  est un morphisme de groupes :

1. On vérifie que  $(G_1, \star)$  et  $(G_2, \bullet)$  sont bien des groupes.
2. On vérifie que pour tout  $(x, y) \in G_1^2$ , on a bien  $f(x \star y) = f(x) \bullet f(y)$ .

**Exemple 11.** Soit  $(G, \cdot)$  un groupe et  $a \in G$ . Prouver que  $f : (\mathbb{Z}, +) \rightarrow (G, \cdot)$  est un morphisme de groupes.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & (G, \cdot) \\ n & \longmapsto & a^n \end{array}$$

**Exemple 12.** Soit  $\mathcal{T}$  l'ensemble des translations du plan  $\mathcal{P}$ . On note  $t_a$  est la translation de vecteur  $\vec{v}_a$  d'affixe  $a \in \mathbb{C}$ .

Prouver que  $f : (\mathbb{C}, +) \rightarrow (\mathcal{T}, \circ)$  est un morphisme de groupes.

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & (\mathcal{T}, \circ) \\ a & \longmapsto & t_a \end{array}$$

### 3 Structure d'anneau

#### DÉFINITION 12 : anneau

Soit  $A$  un ensemble muni de deux lois notées  $+$  et  $\times$ . On dit que  $(A, +, \times)$  est un *anneau* ssi :

1.  $(A, +)$  est un groupe *commutatif*
2. la loi  $\times$  est *associative*
3. la loi  $\times$  est *distributive* par rapport à la loi  $+$  :

$$\forall (x, y, z) \in A^3, \quad \begin{aligned} x \times (y + z) &= x \times y + x \times z \\ (x + y) \times z &= x \times z + y \times z \end{aligned}$$

4. Il existe un *élément neutre* pour  $\times$ , noté  $1_A$  (ou 1 s'il n'y a pas d'ambiguïté)

*Remarque 12.* Si en plus la loi  $\times$  est commutative, on dit que  $(A, +, \times)$  est un anneau commutatif.

*Remarque 13.*

1. Dans un anneau  $(A, +, \times)$ , on note  $-x$  l'inverse de  $x$  pour la loi  $+$  et  $0$  l'élément neutre de la loi  $+$ .
2. Par convention, on conviendra que pour tout  $x \in A$ ,  $x^0 = 1_A$ . (en particulier, on convient que  $0_A^0 = 1_A$ )
3.  $\triangleleft$  Un élément  $x \in A$  n'a pas forcément d'inverse pour la loi  $\times$ , il ne faudra donc pas utiliser abusivement la notation  $x^{-1}$ .

**Exemple 13.** Tous les ensembles suivants sont des anneaux.

1. Ensembles de nombres :  $(\mathbb{Z}, +, \times)$ ,  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$  et  $(\mathbb{C}, +, \times)$ .
2. Applications :  $(\mathbb{R}^I, +, \times)$ ,  $(\mathbb{C}^I, +, \times)$  ( $I$  étant un intervalle de  $\mathbb{R}$ ).
3. Suites :  $(\mathbb{R}^{\mathbb{N}}, +, \times)$ ,  $(\mathbb{C}^{\mathbb{N}}, +, \times)$ .
4. Polynômes :  $(\mathbb{R}[X], +, \times)$ ,  $(\mathbb{C}[X], +, \times)$ .
5. Matrices carrées :  $(\mathfrak{M}_n(\mathbb{R}), +, \times)$ ,  $(\mathfrak{M}_n(\mathbb{C}), +, \times)$  (non commutatifs).

*Remarque 14.* Comme dans le cas des groupes, on définit la notion de *sous-anneau* et il existe un théorème (hors-programme) de caractérisation des sous-anneaux.

**DÉFINITION 13 : L'anneau  $\mathbb{Z}/n\mathbb{Z}$**

Soit  $n \in \mathbb{N}^*$  tel que  $n \geq 2$ .

L'ensemble  $\{0, 1, \dots, n-1\}$  est noté  $\mathbb{Z}/n\mathbb{Z}$  lorsqu'il est muni des lci  $+$  et  $\times$  définies de la façon suivante :

1.  $a + b =$  le reste de la division euclidienne de  $a + b$  par  $n$ .
2.  $a \times b =$  le reste de la division euclidienne de  $a \times b$  par  $n$ .

On montre alors que  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un anneau commutatif.

*Remarque 15.* La particularité de cet anneau est qu'il s'agit d'un anneau de cardinal FINI.

**THÉORÈME 5 : Règles de calcul dans un anneau**

On considère un anneau  $(A, +, \times)$  dont on note  $0$  et  $1$  les éléments neutres respectifs de  $+$  et  $\times$ .

On a les règles de calcul suivantes :

- |                                                                  |                                                       |
|------------------------------------------------------------------|-------------------------------------------------------|
| 1) $\forall a \in A$                                             | $a \times 0 = 0 \times a = 0$                         |
| 2) $\forall a \in A$                                             | $(-1) \times a = -a$ et $a \times (-1) = -a$          |
| 3) $\forall (a, b) \in A^2$                                      | $(-a) \times b = -(a \times b) = a \times (-b)$       |
| 4) $\forall (a, b) \in A^2$                                      | $(-a) \times (-b) = a \times b$                       |
| 5) Si $x$ est inversible, $(-x)$ l'est aussi et :                | $(-x)^{-1} = -x^{-1}$                                 |
| 6) Si $x$ et $y$ sont inversibles, $x \times y$ l'est aussi et : | $(x \times y)^{-1} = y^{-1} \times x^{-1}$            |
| 7) On a la propriété de distributivité suivante :                | $a \cdot \sum_{k=1}^n x_k = \sum_{k=1}^n a \cdot x_k$ |

*Preuve 5 :* On montre que  $a \times 0 = 0$  en remarquant que  $a \times 0 = a \times (0 + 0)$  et en appliquant la distributivité. Les autres démonstrations ne présentent pas de difficulté.

*Remarque 16.* Si  $(A, +, \times)$  est un anneau,  $(A, \times)$  n'est pas un groupe. (car  $0_A$  n'admet pas d'inverse)

**PROPOSITION 6 : Groupe des unités d'un anneau**

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

On note  $A^*$  l'ensemble des éléments inversibles pour la loi  $\times$  :  $A^* = \{a \in A \mid \exists a' \in A \text{ tq } a \times a' = a' \times a = 1_A\}$

L'ensemble  $(A^*, \times)$  a une structure de groupe : c'est le *groupe des unités* de l'anneau  $A$ .

*Preuve 6 :* Pas de difficulté.

**Exemple 14.**

1. Dans l'anneau  $(\mathbb{Z}, +, \times)$ , le groupe des unités est  $(\{1, -1\}, \times)$ .
2. Dans l'anneau  $(\mathcal{F}(I, \mathbb{R}), +, \times)$ , le groupe des unités est constitué des fonctions qui ne s'annulent pas.

⚠⚠⚠. En général, dans un anneau :  $a \times b = 0 \not\Rightarrow a = 0$  ou  $b = 0$

Lorsque  $a \times b = 0$  avec  $a \neq 0$  et  $b \neq 0$ , on dit que  $a$  et  $b$  sont des *diviseurs de zéro*.

**Exemple 15.** (\*) Recherchez des diviseurs de zéro dans les anneaux  $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$ ,  $(\mathbb{Z}/4\mathbb{Z}, +, \times)$  et  $(\mathfrak{M}_n(\mathbb{R}), +, \times)$ .

**THÉORÈME 7 : Formule du binôme de Newton**

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

Alors pour tout  $n \in \mathbb{N}$  et pour tout couple  $(a, b) \in A^2$  tels que  $a.b = b.a$  :

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

*Preuve 7 :* Vous pouvez tenter une démonstration par récurrence de cette formule ...

*Remarque 17.* Cette formule est toujours vraie si l'anneau est commutatif.

**THÉORÈME 8 : Formule de factorisation**

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

Alors pour tout  $n \in \mathbb{N}^*$  et pour tout couple  $(a, b) \in A^2$  tels que  $a.b = b.a$  :

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) = (a - b) \sum_{k=0}^{n-1} a^{n-1-k} b^k$$

*Preuve 8 :* Il suffit de développer ...

*Remarque 18.* Cette formule est toujours vraie si l'anneau est commutatif.

**THÉORÈME 9 : Calcul d'une progression géométrique**

Soit un anneau  $(A, +, \times)$  et un élément  $a \in A$ . On considère un entier  $n \in \mathbb{N}$ ,  $n \geq 1$ .

On déduit de la formule de factorisation que :

$$1 - a^n = (1 - a)(1 + a + a^2 + \dots + a^{n-1})$$

*Preuve 9 :*

On applique la formule du théorème précédent lorsque  $\begin{cases} a = 1_A \\ b = a \end{cases}$

*Remarque 19.* Lorsque  $1 - a$  est inversible, on a alors :  $1 + a + a^2 + \dots + a^{n-1} = (1 - a)^{-1}(1 - a^n)$

*Remarque 20.* Les 3 formules précédentes sont bien entendu valables dans les anneaux usuels  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  et  $\mathbb{C}$ .

## 4 Structure de corps

**DÉFINITION 14 : Corps**

On considère un ensemble  $\mathbb{K}$  muni de deux lois de composition interne, notées  $+$  et  $\times$ .

On dit que  $(\mathbb{K}, +, \times)$  est un *corps* si et seulement si :

1.  $(\mathbb{K}, +, \times)$  est un anneau commutatif non réduit à  $\{0_{\mathbb{K}}\}$ .
2. Tout élément non-nul de  $\mathbb{K}$  est inversible pour la loi  $\times$ .

**Exemple 16.**

1.  $(\mathbb{Q}, +, \times)$ ,  $(\mathbb{R}, +, \times)$ ,  $(\mathbb{C}, +, \times)$  et  $(F(X), +, \times)$  sont des corps.
2.  $(\mathbb{Z}, +, \times)$  n'est pas un corps car 1 et  $-1$  sont les seuls éléments inversibles.
3.  $(\mathfrak{M}_n(\cdot), +, \times)$  n'est pas un corps car seules les "matrices inversibles" sont inversibles.

*Remarque 21.* Si  $(\mathbb{K}, +, \times)$  est un corps, alors  $(\mathbb{K}^*, \times)$  est un groupe, où  $\mathbb{K}^* = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ .



**PROPOSITION 10 : Un corps est un anneau intègre**

Dans un corps  $(\mathbb{K}, +, \times)$ , si deux éléments  $(x, y) \in \mathbb{K}^2$  vérifient  $x \times y = 0_K$ , alors  $x = 0_K$  ou  $y = 0_K$ .  
En particulier, on peut "simplifier par un élément non nul" :

$$\forall (a, x, y) \in \mathbb{K}^3 \quad \text{avec} \quad a \neq 0_K, \quad \text{on a} \quad a \times x = a \times y \Rightarrow x = y$$

*Preuve 10 :* Evident!

**THÉORÈME 11 : Calcul d'une somme géométrique dans un corps**

Soit un élément  $k \in \mathbb{K}$  du corps  $(\mathbb{K}, +, \times)$ .

Alors la formule suivante permet de calculer une progression géométrique de raison  $k$  :

$$\sum_{i=0}^n k^i = 1 + k + k^2 + \dots + k^n = \begin{cases} (1-k)^{-1}(1-k^{n+1}) & \text{si } k \neq 1 \\ (n+1) \cdot 1_{\mathbb{K}} & \text{si } k = 1 \end{cases}$$

⚠ En général, cette formule n'a pas de sens dans un anneau quelconque.

*Preuve 11 :* Vu précédemment!

*Remarque 22.* Les 3 formules vues précédemment dans le cas d'un anneau sont bien entendue valables dans un corps.

*Remarque 23.* On définit aussi la notion de *sous-corps* et il existe un théorème (hors-programme) de caractérisation des sous-corps.

**4.1 Corps des fractions d'un anneau Complément hors-programme**

Voici une méthode permettant de construire un corps à partir d'un anneau.

Elle permet en particulier de construire le corps  $(\mathbb{Q}, +, \times)$  à partir de l'anneau  $(\mathbb{Z}, +, \times)$ .

1. On considère un anneau  $(A, +, \times)$ .
2. Sur l'ensemble  $A \times A^*$ , on définit une relation par :

$$\forall (a, b), (a', b') \in A \times A^*, \quad (a, b) \mathcal{R} (a', b') \iff a \times b' = a' \times b$$

On vérifie que la relation  $\mathcal{R}$  est une relation d'équivalence sur l'ensemble  $A \times A^*$  (réflexive, symétrique et transitive).

On note alors  $\mathbb{K}$  l'ensemble des classes d'équivalences de cette relation.

Un élément  $k \in \mathbb{K}$  est donc la classe d'un couple  $(a, b) \in A \times A^*$ , et on note cette classe :

$$k = \frac{a}{b}$$

3. Sur l'ensemble  $\mathbb{K}$ , on définit deux lois notées  $+$  et  $\times$  de la façon suivante :  
Soient  $k = \text{Cl}(a, b)$  et  $k' = \text{Cl}(a', b')$  deux classes d'équivalences de représentants  $(a, b)$  et  $(a', b')$ .  
On note alors :

$$\begin{aligned} 1) \quad k + k' &= \text{Cl}(a \times b' + b \times a', b \times b') : & \frac{a}{b} + \frac{a'}{b'} &= \frac{a \times b' + b \times a'}{b \times b'} \\ 2) \quad k \times k' &= \text{Cl}(a \times a', b \times b') : & \frac{a}{b} \times \frac{a'}{b'} &= \frac{a \times a'}{b \times b'} \end{aligned}$$

et on vérifie que ces classes sont indépendantes des représentants  $(a, b) \in k$  et  $(a', b') \in k'$  choisis.

4. On montre alors que  $(\mathbb{K}, +, \times)$  est un corps, appelé *corps des fractions* de l'anneau  $(A, +, \times)$ .

5. Comme l'application suivante est injective, elle permet d'inclure l'anneau  $A$  dans le corps  $\mathbb{K}$  :

$$\begin{aligned} \phi : A &\longrightarrow \mathbb{K} \\ a &\longmapsto \text{Cl}(a, 1) \end{aligned}$$

En d'autres termes, on identifiera la fraction  $\frac{a}{1}$  à l'élément  $a$  de l'anneau  $A$ .

*Remarque 24.* Cette construction est aussi utilisée pour définir le corps des fractions rationnelles à partir de l'anneau des polynômes.

## 5 Exercices de TD

Codage :

1. Les exercices avec des coeurs  $\heartsuit$  sont à traiter en priorité.
2. Le nombre d'étoiles  $*$  ou de coeurs  $\heartsuit$  correspond à la difficulté des exercices.

### I] Les groupes

1. Le premier type de question consiste à prouver qu'un ensemble muni d'une loi est un groupe. Pour cela :
  - (a) On montre (si c'est envisageable) que c'est un sous-groupe d'un groupe connu
  - (b) Sinon, on montre que c'est une groupe en vérifiant toutes les conditions de la définition
2. D'autres questions consistent à utiliser le fait qu'un ensemble est un groupe pour démontrer des propriétés.

**Exercice de TD : 1**

( $\heartsuit$ ) Montrer que  $G = \{p\sqrt{2} + q\sqrt{3} \mid p, q \in \mathbb{Z}\}$  est un sous-groupe de  $(\mathbb{R}, +)$  ?

**Exercice de TD : 2**

( $\heartsuit$ ) Soit  $(G, \cdot)$  un groupe et  $a \in G$ .  $H = \{a.g.a^{-1} \mid g \in G\}$  est-il un groupe ?

**Exercice de TD : 3**

( $*$ ) Soit  $(G, \star)$  un groupe et  $x, y \in G$  tels que  $\begin{cases} (x \star y)^{-1} = x^{-1} \star y \\ (y \star x)^{-1} = y^{-1} \star x \end{cases}$ . Montrer que  $\begin{cases} (x^2)^{-1} = y^2 \\ x^4 = y^2 = e \end{cases}$ .

**Exercice de TD : 4**

( $*$ ) Soit  $(G, \star)$  un groupe et  $H \subset G$  fini et stable par  $\star$ . Montrer que  $(H, \star)$  est un sous-groupe de  $G$ .

**Exercice de TD : 5**

( $\heartsuit$ )

1. Montrer que  $(\mathbb{R} \setminus \{1\}, \star)$  où la loi  $\star$  est définie par  $x \star y = x + y - xy$  est un groupe abélien.
2. Soit  $x \in G$  et  $n \in \mathbb{N}^*$ . Calculer  $x^n$ .

**Exercice de TD : 6**

(\*\*). Soit  $(a, b, c) \in \mathbb{R}^3$ . Dans  $\mathbb{R}$ , on définit la loi  $\star$  par :  $x \star y = a(x + y) + bxy + c$ . Déterminer une CNS sur  $(a, b, c)$  pour que  $(\mathbb{R}, \star)$  soit un groupe.

**Exercice de TD : 7**

( $\heartsuit$ ) Soit  $(G, \cdot)$  un groupe tel que :  $\forall a \in G, a^2 = 1_G$ . Montrer que  $G$  est un groupe abélien.

**Exercice de TD : 8**

(\*\*). Soient  $H$  et  $K$  deux sous groupes d'un groupe  $G$ . Montrer que  $H \cup K$  est une sous-groupe de  $G$  si et seulement si  $H \subset K$  ou  $K \subset H$ .

**Exercice de TD : 9**

**Caractérisation du pgcd et du ppcm avec les sous-groupes de  $\mathbb{Z}$**

(\*\*\*) Soient deux entiers non nuls  $a$  et  $b$ .

Prouver que :

1.  $\delta$  est le PGCD de  $a$  et  $b$  ssi  $\delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$  (avec Bezout)
2.  $\mu$  est le PPCM de  $a$  et  $b$  ssi  $\mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$

**Exercice de TD : 10****(♡♡) Test de primalité : le théorème de Wilson**

Soit un entier naturel  $p \geq 3$ .

- On suppose  $(p-1)! \equiv -1 [p]$ . Démontrer que  $p$  est un nombre premier.
- On suppose  $p$  premier.  
Soit  $G = \llbracket 1, p-1 \rrbracket$ .  $\forall (x, y) \in G^2$ ,  $x \circ y$  est le reste de la division euclidienne de  $x \cdot y$  par  $p$ .
  - Démontrer que  $(G, \circ)$  est un groupe dont on précisera l'élément neutre  $e$ . Résoudre  $x \circ x = e$  dans  $G$ .
  - Démontrer que  $(p-1)! \equiv -1 [p]$ .
- Énoncer le théorème démontré. Que dire pour  $p = 2$  ?
- Tester ce théorème pour  $2 \leq p \leq 11$ .

**Exercice de TD : 11**

(\*\*) Cet exercice permet de retrouver certaines propriétés importantes du PGCD.

- Soient  $H_1$  et  $H_2$  deux sous-groupes de  $(\mathbb{Z}, +)$ .  
On définit l'ensemble  $H_1 + H_2 = \{h_1 + h_2 \mid (h_1, h_2) \in H_1 \times H_2\}$ .  
Montrer que  $H_1 + H_2$  est le plus petit (au sens de l'inclusion) sous-groupe de  $(\mathbb{Z}, +)$  qui contient la partie  $H_1 \cup H_2$ .
- Application du résultat précédent :  
Soient  $a$  et  $b$  deux entiers naturels non nuls.
  - Justifier que  $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$  où  $\delta \in \mathbb{N}^*$  est un diviseur commun à  $a$  et  $b$ .
    - Montrer qu'il existe  $u, v \in \mathbb{Z}$  tels que  $\delta = au + bv$ .
    - Conclure que  $\delta$  est le PGCD de  $a$  et  $b$ .
  - Bilan : Citer 2 propriétés importantes liées au PGCD de deux entiers.
  - Déduire des deux questions précédentes le sous-groupe  $4\mathbb{Z} + 6\mathbb{Z}$ .

**Exercice de TD : 12****(♡♡♡) Les sous-groupes de  $(\mathbb{R}, +)$** 

Soit  $H$  un sous-groupe de  $\mathbb{R}$  non réduit au singleton  $\{0\}$ .

- Montrer que  $H \cap \mathbb{R}^{+*}$  admet une borne inférieure. On la notera  $a$ .
- Si  $a$  est en fait le minimum de  $H \cap \mathbb{R}^{+*}$ , montrer que  $H$  est le sous-groupe  $a\mathbb{Z}$ .
- Si  $H \cap \mathbb{R}^{+*}$  n'admet pas de minimum, montrer, par l'absurde, que  $a$  est nul puis que  $H$  est alors dense dans  $\mathbb{R}$ .

**II] Les anneaux**

Dans la très grande majorité des exercices, on montre qu'un ensemble muni de deux lois est un anneau en prouvant que c'est un sous-anneau d'un anneau de référence.

**Exercice de TD : 13**

(♡♡) On considère  $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ . On note alors  $N(a + b\sqrt{2}) = a^2 - 2b^2$ .

- Montrer que  $(A, +, \times)$  est un anneau intègre. (Bien entendu, "+" et "×" sont les ici usuelles)
- Montrer que pour tout  $x, y \in A$ , on a  $N(xy) = N(x)N(y)$ .  
En déduire que :  $x$  est inversible  $\iff N(x) = \pm 1$ .
- Montrer que  $(1 + \sqrt{2})^n$  est inversible pour tout  $n \in \mathbb{N}$ .
- Réciproquement, soit  $x = a + b\sqrt{2}$  un élément inversible de  $A$ .
  - Montrer qu'on peut se ramener au cas où  $a, b \in \mathbb{N}$  avec  $a \neq 0$ .
  - Montrer que  $x = (1 + \sqrt{2})^n$  avec  $n \in \mathbb{N}$ . Aide : si  $b \geq 1$ , on pourra considérer  $x_1 = \frac{x}{1 + \sqrt{2}}$ .

**Exercice de TD : 14**

(♡) Soit  $A$  un anneau. On dit que  $x \in A$  est nilpotent, s'il existe  $n \in \mathbb{N}^*$  tel que  $x^n = 0_A$ .

- Montrer que si  $xy$  est nilpotent, alors  $yx$  l'est aussi.
- On suppose que  $x$  et  $y$  commutent et  $x$  et  $y$  nilpotents. Montrer que  $x + y$  et  $xy$  sont nilpotents.
- On suppose  $x$  nilpotent. Montrer que  $1 - x$  est inversible.

**Exercice de TD : 15**

(\*) Soit  $(A, +, \times)$  un anneau. On dit que  $x \in A$  est nilpotent, s'il existe  $n \in \mathbb{N}$  tel que  $x^n = 0_A$ .

1. Montrer que si  $a$  est nilpotent, alors  $1 - a$  est inversible et calculer son inverse.
2. Soit  $a \in A$ . On définit l'application  $u : A \longrightarrow A$ . Calculer  $u^p = u \circ u \circ \dots \circ u$ .  

$$x \mapsto ax - xa$$
3. Montrer que si  $a$  est nilpotent, il existe  $p \in \mathbb{N}^*$  tel que  $u^p$  soit l'application nulle.

**Exercice de TD : 16**

(\*\*). Soit  $a, b$  deux éléments d'un anneau  $(A, +, \times)$  tels que  $ab$  soit inversible et  $b$  non diviseur de 0. Montrer que  $a$  et  $b$  sont inversibles.

**III] Les corps**

Dans la très grande majorité des exercices, on montre qu'un ensemble muni de deux lois est un corps en prouvant que c'est un sous-corps d'un corps de référence.

**Exercice de TD : 17**

(♥) Pour tout  $a, b \in \mathbb{R}$ , on note  $\begin{cases} a \oplus b = a + b - 1 \\ a \star b = ab - a - b + 2 \end{cases}$ .

Montrer que  $(\mathbb{R}, \oplus, \star)$  est un corps.

**Exercice de TD : 18**

(\*\*) Montrer que si  $F$  est un sous-corps de  $(\mathbb{Q}, +, \times)$ , alors  $F = \mathbb{Q}$ .

**Exercice de TD : 19**

(♥) Soit  $r$  un rationnel ( $r > 0$ ) et que  $\sqrt{r} \notin \mathbb{Q}$ . On note  $\mathbb{Q}(\sqrt{r}) = \{a + b\sqrt{r} \mid (a, b) \in \mathbb{Q}^2\}$ . Montrer que  $\mathbb{Q}(\sqrt{r})$  est un corps pour les lois usuelles de  $\mathbb{R}$ .

**Exercice de TD : 20**

(\*) Montrer que tout anneau intègre fini est un corps.

Aide : vous pourrez commencer par étudier pour tout  $a \in E$  non nul, l'application  $f_a : x \mapsto ax$

**Exercice de TD : 21**

(♥) Soit l'application  $\psi : \mathbb{R}^2 \longrightarrow \mathbb{C}$ . On note  $\mathbb{Z}[i] = \psi(\mathbb{Z}^2)$  et  $\mathbb{Q}(i) = \psi(\mathbb{Q}^2)$ .  

$$(a, b) \mapsto a + ib$$

1. Montrer que  $(\mathbb{Z}[i], +, \times)$  est un anneau intègre qui n'est pas un corps.
2. Montrer que  $(\mathbb{Z}(i), +, \times)$  est un corps dont  $\mathbb{Z}[i]$  est un sous-anneau.
3. Vérifier que toute fraction  $A/B$  avec  $A, B \in \mathbb{Z}[i]$  appartient à  $\mathbb{Z}(i)$  et réciproquement, que tout élément de  $\mathbb{Z}(i)$  s'écrit comme une fraction  $A/B$  avec  $A, B \in \mathbb{Z}[i]$ .