# CHP 12 : STRUCTURES ALGÉBRIQUES USUELLES

## 1. Lois de composition internes ($\ell ci$)

**Définition**

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

$$* : \begin{cases} E \times E & \longrightarrow & E \\ (x, y) & \longmapsto & x * y \end{cases}$$

**Associativité, Commutativité**

Une $\ell ci$ " $*$ " dans E est dite :

- **associative** , si $\forall (x, y, z) \in E^3, \ (x * y) * z = x * (y * z)$
- **commutative** , si $\forall (x, y) \in E^2, \ x * y = y * x$

**Remarque**

L'associativité nous permet d'enlever les parenthèses : $(x * y) * z = x * (y * z) = x * y * z$

### Exemples

- Dans $\mathscr{F}(E, E)$, "$* = o$"

$$\forall f, g, h \in \mathscr{F}(E, E), \quad (fog)oh = fo(goh)$$

$$\boxed{\text{La composée est associative mais pas commutative.}}$$

- Dans $\mathscr{P}(E)$, "$* = \cap$"

$$\forall A, B, C \in \mathscr{P}(E), \quad (A \cap B) = A \cap (B \cap C), \quad A \cap B = B \cap A$$

$$\boxed{\text{L'intersection est associative et commutative.}}$$

- Dans $\mathscr{M}_n(\mathbb{K})$, "$* = \times$"

$$\boxed{\text{Le produit matriciel est une } \ell ci \text{ associative et pas commutative.}}$$

### Élément neutre, unicité

Soit E un ensemble muni d'une $\ell ci$ " $*$ " .

- **Élément neutre :** Un élément $e \in \mathrm{E}$ est dit **élément neutre** , si :

$$\forall x \in \mathrm{E}, \quad x * e = e * x = x$$

- **Unicité de l'élément neutre :** S'il existe, l'élément neutre est unique.

### Preuve

..................................................................................................................

..................................................................................................................

..................................................................................................................

..................................................................................................................

..................................................................................................................

### Éléments inversibles

Soit E un ensemble muni d'une $\ell ci$ "$*$" d'élément neutre $e$ .

- **Éléments inversibles :**Un élément $x \in \mathrm{E}$ est **inversible** (ou symétrisable),si :

$$\exists b \in \mathrm{E}, \quad x * b = e \text{ et } b * x = e$$

- Dans ce cas ,on dit $b$ est **l'inverse** (ou le sumétrique ) de $x$ pour la $\ell ci$ "$*$"

## Exemples

- Dans $\mathscr{F}(\mathrm{E},\mathrm{E})$, "$* = \circ$"

$$\boxed{\text{Les applications bijectives sont les éléments inversibles .}}$$

- Dans $\mathbb{Z}$, "$* = \times$"

$$\boxed{-1 \text{ et } 1 \text{ sont les seuls éléments inversibles .}}$$

- Dans $\mathscr{M}_n(\mathbb{K})$, "$* = \times$"

$$\boxed{\text{Les matrices inversibles sont les éléments inversibles .}}$$

**Unicité de l'inverse**

Soit E un ensemble muni d'une $\ell ci$ " $*$ " est **associative** .

**L'inverse** (ou le sumétrique ),**s'il existe**, est **unique**.

## Preuve

.......................................................................................................

.......................................................................................................

.......................................................................................................

.......................................................................................................

## Remarque

Soit E un ensemble muni d'une $\ell ci$ "$*$" **associative**.

Si $x$ est **inversible**,alors

- $\forall y, z \in \mathrm{E}, \quad x * y = x * z \Longrightarrow y = z$
- $\forall y, z \in \mathrm{E}, \quad y * x = z * x \Longrightarrow y = z$

$\boxed{\text{Tout élément inversible est simplifiable}}$

## Preuve

.......................................................................................................

**Proposition : $(x * y)^{-1}$**

- Si $x$ et $y$ sont inversibles, alors $\begin{cases} \bullet \quad x * y \text{ est inversible} \\ \bullet \quad (x * y)^{-1} = y^{-1} * x^{-1} \end{cases}$
- Si $x$ est inversible, alors $x^{-1}$ est inversible et $(x^{-1})^{-1} = x$

## Preuve

.......................................................................................................

.......................................................................................................

..........................................................................................................................................

..........................................................................................................................................

## Exemples

- Dans $\mathscr{F}(E,E)$, "$* = \circ$"
  Si $f$ et $g$ sont deux bijections de E vers E , alors $f\circ g$ est une bijection et :
  $$(f\circ g)^{-1} = g^{-1}\circ f^{-1}$$
- Dans $\mathscr{M}_n(\mathbb{K})$, "$* = \times$"
  Le produit de deux matrices inversibles A et B est encore inversible, et que :
  $$(A\times B)^{-1} = B^{-1}\times A^{-1}$$

### Définitions :Parties stables

Soit E un ensemble non vide muni d'une $\ell ci$ "$*$" .Soit F une partie non vide de E .

- F est **stable** par la $\ell ci$ "$*$" $\Longleftrightarrow$ $\forall (x,y)\in F^2,\quad x*y\in F$
- L'application $\left\{\begin{array}{ccc} F\times F & \longrightarrow & F \\ (x,y) & \longmapsto & x*y \end{array}\right.$ est appelée $\ell ci$ induite par $*$ sur F

## Notations usuelles

| | **Notation additive** $*=+$ | **Notation multiplicative** $*=\times$ |
|---|---|---|
| **Élément neutre** | $0_E$ ou $0$ | $1_E$ ou $1$ |
| **Symétrique de** $x$ | opposée : $-x$ | inverse : $x^{-1}$ |
| $\forall n\in\mathbb{N}^*$ | $\overbrace{x+x\cdots+x}^{n\text{ fois}} = nx$ | $\overbrace{x.x\cdots x}^{n\text{ fois}} = x^n$ |
| Si $x$ est symétrisable $\forall n\in\mathbb{N}^*$ | $(-n)x = n(-x)$ | $x^{-n} = (x^{-1})^n$ |
| $\forall (n,p)\in\mathbb{Z}^2$ | $nx+px=(n+p)x$ | $x^nx^p = x^{n+p}$ |

## 2. Structure de groupes

### a) Groupes

**Définition**

$(G,*)$ est groupe si :

- " $*$ " est une $(\ell ci)$ sur G
- la $(\ell ci)$ $*$ est associative.
- la $(\ell ci)$ $*$ admet un élément neutre noté $e_G$ ou $e$.
- tout élément de G est inversible.

Si de plus la $(\ell ci)$ $*$ est **commutative** , on dit que $(G,*)$ est un **groupe abélien** .

### Groupes usuels

- **Groupes additifs :** $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathscr{F}(E,\mathbb{R}),+)$, $\left(\mathbb{R}^{\mathbb{N}},+\right)$, $\left(\mathscr{M}_{n,p}(\mathbb{K}),+\right)$.
- **Groupes multiplicatifs :**
  - **Groupes abéliens :** $\left(\mathbb{Q}^*,\times\right)$, $\left(\mathbb{Q}^{*+},\times\right)$, $\left(\mathbb{R}^*,\times\right)$, $\left(\mathbb{R}^{*+},\times\right)$, $\left(\mathbb{C}^*,\times\right)$.
  - **Groupes non abéliens :** $(\mathscr{S}_E,\circ)$, $(\mathbb{GL}_n(\mathbb{K}),\times)$.

■ $\mathscr{S}_E$ désigne l'ensemble des applications bijectives de E vers E.

**Règles de calcul dans un groupe**

Soient $(G,*)$ un groupe , $a,b,y,z\in G$

- $(a*b)^{-1}=b^{-1}*a^{-1}$.
- $a*y=a*z\Longrightarrow y=z$
- $a*y*a^{-1}=z\Longleftrightarrow a*y=z*a\Longleftrightarrow y=a^{-1}*z*a$
- Pour tout $k\in\mathbb{Z}$ ,

$$a^k=\begin{cases}\overbrace{a*a*\ldots*a}^{k\text{ fois}} & \text{si } k>0\\ e_G & \text{si } k=0\\ \left(a^{-1}\right)^{(-k)} & \text{si } k<0\end{cases}$$

- $e_G^n=e_G$
- Si a et b **commutent** ,alors $\forall n\in\mathbb{Z},\quad (a*b)^n=a^n*b^n$ .
- $\forall p,q\in\mathbb{Z},\quad (a^p*a^q)=a^{p+q},\quad (a^p)^q=a^{pq}$
- Si $a$ et $b$ **ne commutent pas**, $\forall n\in\mathbb{N}^*,\quad (a*b)^n=\overbrace{(a*b)*(a*b)*\ldots*(a*b)}^{n\text{ fois}}$

**Groupe produit** $G \times H$

Soient $(G, *)$ et $(H, \triangle)$ deux groupes. On note "**T**" la *ℓci* sur $G \times H$ définie par :

$$\text{Pour tout } (g,h),(g',h') \in G \times H, \qquad (g,h)\mathbf{T}(g',h') = (g * g', h \triangle h')$$

Alors $(G \times H, \mathbf{T})$ a une structure de groupe.

- $(e_G, e_H)$ l'élément neutre de $(G \times H, \mathbf{T})$.
- L'inverse de $(g,h) \in G \times H$ est $(g^{-1}, h^{-1})$.

**Preuve**

................................................................................................................................

................................................................................................................................

### b) Sous-groupes

**Définition :Sous-groupes**

Soit $(G, *)$ un groupe et $H \subset G$.
On dit que H un sous-groupe de $(G, *)$ si :

- $H \neq \emptyset$
- H est stable par $*$ : $\forall (x,y) \in H^2, \quad x * y \in H$
- H est stable par inverse : $\forall x \in H, \quad x^{-1} \in H$

- $\{e_G\}$ et G sont des sous-groupes ( triviaux) de $(G, *)$

## Exemples

- $\mathscr{T}_n(\mathbb{K}),\ \mathscr{D}_n(\mathbb{K}),\ \mathscr{S}_n(\mathbb{K}),\ \mathscr{A}_n(\mathbb{K})$ sont des sous-groupes de $(\mathscr{M}_n(\mathbb{K}), +)$.
- $\mathbb{U},\ \mathbb{U}_n$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.

**Caractérisation d'un sous groupe**

Soient $(G, *)$ un groupe et $H \subset G$.

$$H \text{ sous-groupe de } (G,*) \iff \begin{cases} \bullet\ e_G \in H \\ \bullet\ \forall (x,y) \in H^2, \quad x * y^{-1} \in H \end{cases}$$

## Les sous groupe de $(\mathbb{Z},+)$

$$\boxed{\text{Les sous groupes de } (\mathbb{Z},+) \text{ sont de la forme } n\mathbb{Z}, \quad n\in\mathbb{N}}$$

**Preuve**

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

**Proposition**

Soit H et K deux sous-groupes d'un groupe $(G,*)$

$$\boxed{H\cap K \text{ est un sous-groupe de } G.}$$

**Preuve**

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

### Remarques

Soit H un sous-groupe de $(G,*)$ ,alors

- $(H,*)$ est un groupe d'élément neutre $e_H = e_G$
- L'inverse dans H est l'inverse dans G

## Exemples

$(\mathbb{U},\times),(\mathbb{U}_n,\times)$, $n\in\mathbb{N}^*$ sont des groupes commutatifs.

### c) Morphismes de groupes

Soient $(G,\perp)$ et $(G',*)$ deux groupes .

### Définition

Une application $\varphi : G \longrightarrow G'$ est dite **morphisme de groupes** si :

$$\forall x,y\in G,\qquad \varphi(x\perp y)=\varphi(x)*\varphi(y)$$

- On note $\mathrm{Hom}(G,G')$ l'ensemble des morphismes de $(G,*)$ dans $(G',T)$.

### Vocabulaire

Soit $\varphi\in\mathrm{Hom}(G,G')$

- **Isomorphisme si** $\varphi$ est bijective. On note $\varphi\in\mathbf{Isom}(G,G')$.
- **Endomorphisme si** $G=G'$ . On note $\varphi\in\mathbf{End}(G)$.
- **Automorphisme si** $G=G'$ et $\varphi$ bijective. On note $\varphi\in\mathbf{Aut}(G)$.

## Exemples

- $\varphi_1 : \begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (\mathbb{R}^*,\times)\\ n & \longmapsto & 2^n\end{array}$
- $\varphi_2 : \begin{array}{ccc}(\mathbb{R}^{+*},\times) & \longrightarrow & (\mathbb{R},+)\\ x & \longmapsto & \ln x\end{array}$
- $\varphi_3 : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{R}^{+*},\times)\\ x & \longmapsto & \exp x\end{array}$
- $\varphi_4 : \begin{array}{ccc}(\mathbb{R},+) & \longrightarrow & (\mathbb{U}(\mathbb{C}),\times)\\ \theta & \longmapsto & e^{i\theta}\end{array}$
- $\varphi_5 : \begin{array}{ccc}(\mathbb{C},+) & \longrightarrow & (\mathbb{C}^{+*},\times)\\ z & \longmapsto & e^{z}\end{array}$

### Remarques

Si $\varphi \in \text{Hom}(G, G')$, alors :

- $\varphi(e_G) = e_{G'}$
- $\forall x \in G, \quad \varphi(x^{-1}) = \left(\varphi(x)\right)^{-1}$
- $\forall x \in G, \ \forall n \in \mathbb{Z}, \quad \varphi(x^n) = (\varphi(x))^n$

### Preuve

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

### Proposition :Image directe -Image réciproque

Soit $\varphi \in \text{Hom}(G, G')$, alors :

- A sous groupe de G $\Longrightarrow$ $\varphi(A)$ sous groupe de $G'$
- B sous groupe de $G'$ $\Longrightarrow$ $\varphi^{-1}(B)$ sous groupe de G

### Preuve

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

........................................................................................................................

.............................................................................................................................................

.............................................................................................................................................

## Définition

Soit $\varphi \in \mathrm{Hom}\left(G, G'\right)$.

- **L' image** de $\varphi$ :

$$Im(\varphi) \stackrel{\text{déf}}{=} \{\varphi(x) / \quad x \in G\} = \varphi(G)$$

- **Le noyau** de $\varphi$ :

$$Ker(\varphi) \stackrel{\text{déf}}{=} \{x \in G / \quad \varphi(x) = e_{G'}\}$$

## Remarques

Soit $\varphi \in \mathrm{Hom}\left(G, G'\right)$.

- $y \in Im\varphi \Longleftrightarrow$ .................................
- $x \in Ker\varphi \Longleftrightarrow$ .................................
- $Ker\varphi \subset$ , $Im\varphi \subset$

## Exemple

Le morphisme de groupes

$$f : (\mathbb{R}, +) \longrightarrow \left(\mathbb{C}^*, \times\right)$$
$$x \longmapsto e^{ix}$$

## Corollaire

Soit $\varphi \in \mathrm{Hom}\left(G, G'\right)$.

- $\ker\varphi$ est un sous groupe de $G$.
- $\mathrm{Im}\,\varphi$ est un sous groupe de $G'$.

### Preuve

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

### Proposition

Soit $\varphi \in \text{Hom}\left(G, G'\right)$.

- $\varphi$ est **injective** $\iff$ $\ker(\varphi) = \{e_G\}$
- $\varphi$ est **serjective** $\iff$ $\text{Im}\,(\varphi) = G'$

### Preuve

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

# 3. Structure d'anneaux

## a) ANNEAUX

### Définition

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

- $(A, +)$ est un groupe abélien
- la loi $\times$ est associative
- la loi $\times$ admet un élément neutre , noté $1_A$
- la loi $\times$ est distributive par rapport à la loi $+$

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

- Si de plus la $(\ell ci)$ $\times$ est **commutative**, on dit que l'anneau $(A, +, \times)$ est **commutatif**.

## Anneaux usuels

- $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$, $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \times)$ sont des anneaux commutatifs.
- $(\mathscr{M}_n(\mathbb{K}), +, \times)$ anneau non commutatif.

  ........................................................................................................

  ........................................................................................................
- $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ n'a pas une structure d'anneau.

  ........................................................................................................

  ........................................................................................................

### Définition

Soient $(A, +, x)$ un anneau , $a \in A$.

$$a \text{ est dit inversible} \overset{\text{déf}}{\iff} a \text{ est inversible pour } \ell ci \ \times$$

On note $U(A)$ ou $A^{\times}$ l'ensemble des éléments inversibles de A.

### Remarques

- Les éléments d'un anneau **ne sont pas forcément** inversibles pour la loi $\times$.
- L'élément $1_A$ appartient à $U(A)$ et $1_A^{-1} = 1_A$.
- Si $(x, y) \in U(A)^2$, alors $x \times y \in U(A)$ et $(x \times y)^{-1} = y^{-1} \times x^{-1}$.

- Si $x \in \mathrm{U}(\mathrm{A})$, alors $x^{-1} \in \mathrm{U}(\mathrm{A})$ et $\left(x^{-1}\right)^{-1} = x$.

**Groupe des inversibles d'un anneau**

Soient $(\mathrm{A}, +, \times)$ un anneau,

$(\mathrm{U}(\mathrm{A}), \times)$ est **un groupe** appelé **groupe des inversibles** de A.

## Exemples

- Le groupe des inversibles de l'anneau $(\mathbb{Z}, +, \times)$

$$\mathrm{U}(\mathbb{Z}) = \mathbb{Z}^{\times} =$$

- Le groupe des inversibles de l'anneau $(\mathbb{Q}, +, \times)$ est
- Le groupe des inversibles de l'anneau $(\mathscr{M}_n(\mathbb{K}), +, \times)$

$$\mathrm{U}(\mathscr{M}_n(\mathbb{K})) = \mathscr{M}_n(\mathbb{K})^{\times} =$$

### Régles de calcul dans un anneau

Si $(\mathrm{A}, +, \times)$ est un anneau ,alors :

- $0_\mathrm{A}$ est absorbant :
$$\forall a \in \mathrm{A}, \quad a \times 0_\mathrm{A} = 0_\mathrm{A} \times a = 0_\mathrm{A}.$$
- $\forall a, b \in \mathrm{A}, (-a) \times b = a \times (-b) = -(a \times b)$.
- $\forall a \in \mathrm{A}, \ (-1).a = -a$
- $\forall (a, b, c) \in \mathrm{A}^3, \ \begin{cases} a \times (b - c) = a \times b - a \times c \\ (a - b) \times c = a \times c - b \times c \end{cases}$
- Si $n, p \in \mathbb{Z}$ et $a, b \in \mathrm{A}$,
  - $n(a \pm b) = na \pm nb$,
  - $n(ab) = (na)b = a(nb)$
  - $n(pa) = (np)b$
  - $na = (n1_\mathrm{A})\, a = a\,(n1_\mathrm{A})$
- Si $a \times b = b \times a$, $\qquad (ab)^n = a^n b^n$
- **Formule du binôme de Newton :** Si $a \times b = b \times a$,
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$
- **Factorisation de $a^n - b^n$ :** Si $a \times b = b \times a$
$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

- **Somme géométrique :** En particulier, pour tout $x \in A$;

$$1_A - x^n = (1_A - x) \times \sum_{k=0}^{n-1} x^k$$

## Définition

Un anneau $(A, +, \times)$ est dit intègre si :

- A est commutatif,
- $A \neq \{0_A\}$ (c-à-d : $1_A \neq 0_A$)
- A n'admet aucun diviseur de zéro, c-à-d :

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

..........................................................................................

..........................................................................................

## Exemples

- $(\mathbb{Z}, +, \times)$ est un anneau intègre.
- $(\mathscr{M}_n(\mathbb{K}), + \times)$,$\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ ,$(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \times)$ sont des anneaux non intègres.

..........................................................................................

..........................................................................................

..........................................................................................

..........................................................................................

## Remarque

Dans un anneau intègre ,tout élément $a$ non nuls est simplifiable à droie et à gauche. c-à-d

- $\forall y, z \in E, \quad a * y = a * z \Longrightarrow y = z$
- $\forall y, z \in E, \quad y * a = z * a \Longrightarrow y = z$

### b) Sous-anneaux

**Définition :Sous-anneaux**

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

On dit que B est un sous-anneau de $(A,+,\times)$ si :

- $\mathbf{1}_A \in B$
- $\forall (x,y) \in B^2, \quad x - y \in B$
- $\forall (x,y) \in B^2, \quad x \times y \in B$

## Exemples

- $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$ qui est un sous-anneau de $(\mathbb{C},+,\times)$.
- $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ est un sous-anneau de $\left(\mathbb{C}^{\mathbb{N}},+,\times\right)$.
- L'anneau $(\mathcal{M}_n(\mathbb{R}),+,\times)$ est un sous-anneau de l'anneau $(\mathcal{M}_n(\mathbb{C}),+,\times)$.

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

**Remarque**

$$B \text{ un sous-anneau de } (A,+,\times) \iff (B,+,\times) \text{ est un anneau}$$

### c) Morphisme d'anneaux

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

**Définition**

Une application $f : A \longrightarrow B$ est dite **morphisme d'anneaux** si :

- $f(1_A) = 1_B$
- $\forall (x,y) \in A^2, \quad f\left(x+y\right) = f(x) + f(y)$
- $\forall (x,y) \in A^2, \quad f\left(x \times y\right) = f(x) \times f(y)$

Si de plus $f$ est bijectif ,$f$ est dit isomorphisme d'anneaux .

## Exemple

L'identité $\mathrm{id}_{\mathbb{Z}}$ est l'unique morphisme d'anneaux de $(\mathbb{Z},+,\times)$ dans $(\mathbb{Z},+,\times)$.

..........................................................................................................

..........................................................................................................

..........................................................................................................

## Remarques

Si $f : A \longrightarrow B$ est un morphisme d'anneaux

- $f(0_A) = 0_B, \quad f(1_A) = 1_B$
- $\forall x \in A, \forall n \in \mathbb{Z}, \quad f(nx) = nf(x)$
- $\forall x \in A^{\times}, \quad \forall n \in \mathbb{Z}, \quad f(x^n) = (f(x))^n$

..........................................................................................................

..........................................................................................................

..........................................................................................................

..........................................................................................................

### d) Corps

## Définition

Soit A un ensemble muni de deux $\ell ci$ notées + et ×.

On dit que $(A,+,\times)$ est un corps si :

- $A \neq \{0_A\}$ c-à-d $1_A \neq 0_A$
- $(A,+,\times)$ est un anneau commutatif,
- tout élément de $A/\{0_A\}$ est inversible . $(U(A) = A/\{0_A\})$

de manière équivalente,

- $(A, +)$ est un groupe abélien.
- $(A/\{0_A\}, \times)$ est un groupe .
- la loi $\times$ est commutatif et distributive par rapport à la loi $+$.

## Exemples

- $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ sont des corps .
- $(\mathbb{Z}, +, \times)$ n'est pas un corps.
- $\mathbb{Q}[\sqrt{3}] = \left\{a + b\sqrt{3}, (a, b) \in \mathbb{Q}^2\right\}$ est un corps.

.......................................................................................................

.......................................................................................................

.......................................................................................................

.......................................................................................................

## Remarques

- Un corps est un anneau commutatif dans lequel tout élément **non nul** est inversible.
- Tout corps est un anneau intègre.

**Preuve**

.......................................................................................................

.......................................................................................................

# 4. Exercices d'entrainement

**Exercice 1**

Soit $(G, *)$ un groupe.

1. On suppose $\forall a, b \in G, \quad (a * b)^{-1} = a^{-1} * b^{-1}$ ,Montrer que G est un groupe abélien.
2. On suppose $\forall a, b \in G, \quad (a * b)^2 = a^2 * b^2$ ,Montrer que G est un groupe abélien.
3. On suppose $\forall a \in G, \quad a^2 = e$ ,Montrer que G est un groupe abélien.

## Exercice 2

1. Montrer que $A = \begin{pmatrix} 0 & 1 & -\sin\theta \\ -1 & 0 & \cos\theta \\ -\sin\theta & \cos\theta & 0 \end{pmatrix}$ est nilpotente d'indice 3.
2. La matrice A est-elle inversible ?
3. On pose $M(t) = I_3 + tA + \dfrac{t^2}{2}A^2$.
   Montrer que l'ensemble $G = \{M(t) \mid t \in \mathbb{R}\}$ est un groupe pour le produit matriciel.

## Exercice 3

Soit A un anneau non réduit à $\{0\}$, tel que : $\forall x \in A, \quad x^2 = x$.

1. Montrer que $\forall a \in A : \quad a + a = 0$ .
2. En déduire que A est commutatif .
3. Montrer que $\forall a, b \in A : \quad ab(a+b) = 0$ .

## Exercice 4

On note $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ l'ensemble des entiers de Gauss.

1. Démontrer que $(\mathbb{Z}[i], +, \times)$ est un anneau.
2. Déterminer ses éléments inversibles.

## Exercice 5

Soit H et K deux sous-groupes d'un groupe $(G, *)$

1. Montrer que $H \cap K$ est un sous-groupe.
2. Montrer que $\quad H \cup K \quad$ est un sous-groupe $\iff \quad H \subset K$ ou $K \subset H$.

## Exercice 6

L'application transposée

$$\psi : \left\{ \begin{array}{lcl} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ M & \longrightarrow & {}^tM \end{array} \right.$$

est-elle un isomorphisme de l'anneau $(\mathcal{M}_n(\mathbb{R}), +, \times)$ dans lui-même ?

## Exercice 7

Pour tout réel $x$, on pose $R(x) = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$.

1. Calculer $R(x)^n$ pour tout entier $n \geq 1$.
2. Montrer que $\{R(x) / \ \ x \in \mathbb{R}\}$ est un sous-groupe abélien de $(GL_2(\mathbb{R}), \times)$.
3. Pour $\theta \in ]-\dfrac{\pi}{2}, +\dfrac{\pi}{2}[$, on pose $T = \begin{pmatrix} 1 & -\tan\theta \\ \tan\theta & 1 \end{pmatrix}$.
   Calculer $T^n$ pour tout entier $n$.

**Exercice 8**

Soit $n \geq 2$ . On pose $w = e^{i\frac{2\pi}{n}}$ . On définit l'ensemble $\mathbb{Z}[w]$ par :

$$\mathbb{Z}[w] = \left\{ \sum_{k=0}^{n-1} a_k w^k; \quad (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n \right\}$$

Démontrer que $\mathbb{Z}[w]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

**Exercice 9**

On pose $\mathrm{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}; \quad a, b \in \mathbb{C} \right\}$.

1. Montrer que $(\mathrm{H}, +, \times)$ est un corps non commuttif.
2. Résoudre dans H l'équation $\mathrm{A}^2 = -\mathrm{I}_2$.