ANNEAUX - CORPS

I/ *Anneaux*

1. Distributivité

Soit E un ensemble muni de 2 opérations $\circ$ et $\star$.
On dit que la loi $\star$ est distributive sur la loi $\circ$ ssi :

$$\forall a,b,c \in E \;/\; a \star (b \circ c) = (a \star b) \circ (a \star c) \text{ et } (b \circ c) \star a = (b \star a) \circ (c \star a)$$

Exemples :

- Dans $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ ou $\mathbb{C}$, la multiplication est distributive par rapport à l'addition
- Dans $\mathcal{P}(E)$ on rappelle que $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (A - C)$
  $\cap$ est distributive par rapport à $\cup$
  $\cup$ est distributive par rapport à $\cap$
  $\cap$ est distributive par rapport à Δ
  Δ n'est pas distributive par rapport à $\cap$
- Dans l'ensemble $\mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$,
  on rappelle que $f + g$ est définie par $\forall x \in \mathbb{R} \;/\; (f+g)(x) = f(x) + g(x)$.
  La loi $\circ$ est distributive à droite sur l'addition, mais pas à gauche.
  Exemple $x \xrightarrow{f} x^2$, $x \xrightarrow{g} x$, $x \xrightarrow{h} -x$
- Soient E un espace vectoriel, $\mathcal{L}(E)$ l'ensemble des applications linéaires de E dans E (endomorphismes).
  Dans $\mathcal{L}(E)$, la loi $\circ$ est distributive sur l'addition.

2. Définition

Un ensemble A muni de 2 opérations + et $\star$. est un **anneau** si

- $(A, +)$ est un groupe commutatif .
  On note 0 son élément neutre. On note $-x$ l'opposé de l'élément x.
- La loi $\star$ est associative
- A possède un élément neutre pour la loi $\star$. On le note 1.
- La loi $\star$ est distributive par rapport à la loi +

Si, de plus, la loi $\star$ est commutative, on dit que $(A, +, \star)$ est un **anneau commutatif**.

La loi $\star$ est souvent noté multiplicativement : $\times$, ou .

Si A est muni de deux lois notées autrement que + et . , bien distinguer la loi de groupe (la 1$^{\text{ère}}$) de l'autre.
Ne pas confondre les deux neutres :
le « zéro » 0 neutre pour la loi + (la confusion avec le zéro d'un autre anneau n'étant pas gênante)
l' « unité » 1 neutre pour la loi $\star$ (ou 1_A si il y a possibilité de confondre avec l'unité d'un autre anneau).

Exemples d'anneaux :

- $(\mathbb{Z}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times), (\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont des anneaux commutatifs
- Anneau(x) d'ordre 2 : $(\{a,b\}, +, \star)$ avec les tables

$+$	a	b
a	a	b
b	b	a

$\star$	a	b
a	a	a
b	a	b

- Soient E un ensemble quelconque, et $(A,+,\star)$ un anneau.
  Pour 2 applications f et g de E dans A, on définit $f\oplus g$ et $f\otimes g$ par
  $$\forall x\in E/(f\oplus g)(x)=f(x)+g(x) \text{ et } (f\otimes g)(x)=f(x)\star g(x)$$
  Alors $(A^E,\oplus,\otimes)$ est un anneau. Il est commutatif si A est commutatif.
  Exemples : Fonctions de $\mathbb{R}$ dans $\mathbb{R}$, suites de réels, polynômes …
- Soit E un ensemble quelconque. $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif.
- Matrices $n\times n$: $(\mathcal{M}_2(\mathbb{R}),+,\times)$ est un anneau (non commutatif si $n\geqslant 2$)
- Endomorphismes d'un espace vectoriel : $(\mathcal{L}(E),+,\circ)$ est un anneau (non commutatif si $\dim(E)\geqslant 2$)
- Anneau produit : Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. On définit sur $A\times B$ une addition et une multiplication en posant $(a,b)\oplus(a',b')=(a+a',b+b')$ et $(a,b)\otimes(a',b')=(a\times a',b\times b')$
  $(A\times B,\oplus,\otimes)$ est un anneau. Il est commutatif si A et B le sont.
- Soit $\mathbb{Z}\left[\sqrt{2}\right]$ l'ensemble des réels de la forme $a+b\sqrt{2}$ où a et b sont des entiers quelconques.
  $\left(\mathbb{Z}\left[\sqrt{2}\right],+,\times\right)$ est un anneau commutatif.
  De même l'ensemble $\mathbb{Z}[i]$ des complexes de la forme $a+bi$ où a et b sont des entiers quelconques.
- Soient $(A,+,\star)$ et B une partie de A.
  $(B,+,\star)$ est appelé sous-anneau de A si B est un anneau et s'il a le même élément neutre pour $\star$.
  On montre que $(B,+,\star)$ est un sous-anneau de A $\Leftrightarrow \begin{cases} 1_A\in B \\ \forall x,y\in B/x-y\in B \\ \forall x,y\in B/x\star y\in B\end{cases}$

3. Règles de calcul dans un anneau

Soit $(A,+,\star)$ un anneau

- $\forall x\in A,\ x\star 0=0\star x=0$ on dit que 0 est **absorbant** pour la loi **.**
- Si 0 =1, A est réduit à un élément : On exclut généralement cette éventualité.
- $\forall x,y\in A,\ x\star(-y)=(-x)\star y=-(x\star y)$. On écrit $-x\star y$.
  $\forall x,y\in A,\ (-x)\star(-y)=x\star y$

Pour $n\in\mathbb{N}$ et $x\in A$ on rappelle (définition) que :

$$n\,x=x+x+...+x\ ,\ (-n)x=-(n\,x),\ 0x=0 \text{ (plus précisément } 0_{\mathbb{Z}}x=0_A)$$

On a alors

- $\forall n,p\in\mathbb{Z},\forall x,y\in A,(n+p)x=n\,x+p\,x$ et $n(x+y)=n\,x+n\,y$
  (Attention : ça ressemble à la distributivité, mais ce n'est pas la distributivité)
- $\forall n\in\mathbb{Z},\forall x,y\in A,x\star(n\,y)=n(x\star y)=(n\,x)\star y$. On écrit $n\,x\star y$.
  (Attention : ça ressemble à l'associativité, mais ce n'est pas l'associativité)

Attention : distinguer le produit **interne** $a\star b$, avec a, b $\in$A, et le produit **externe** $n\,a$, avec $n\in\mathbb{Z}$ et $a\in A$

Sommes

- $\forall n\in\mathbb{N},\forall x\in A,\ (1-x)\star(1+x+...+x^n)=(1-x)\star\sum_{k=0}^{n}x^k=\left(\sum_{k=0}^{n}x^k\right)\star(1-x)=1-x^{n+1}$
- $\forall n\in\mathbb{N},\forall x\in A,\ (1+x)\star(1-x+x^2...-x^{2n-1}+x^{2n})=(1+x)\star\sum_{k=0}^{2n}(-1)^k x^k=\left(\sum_{k=0}^{2n}(-1)^k x^k\right)\star(1+x)=1+x^{2n+1}$

Éléments qui commutent

Soient $(A,+,\star)$, x et y deux éléments de A.

On dit que x et y commutent ssi $x \star y = y \star x$

Remarques :

Si l'anneau est commutatif, tous les éléments commutent 2 à 2

Si x commute avec y et avec z, alors x commute avec $y+z$

Formule du binôme

Soient a, b deux éléments qui **commutent** d'un anneau $(A,+,\star)$ et $n \in \mathbb{N}$.

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

Remarque : on a aussi avec les mêmes hypothèses: $a^{n+1} - b^{n+1} = (a-b) \star \sum_{k=0}^{n} a^k \star b^{n-k}$

Remarque : C'est faux a priori si les éléments ne commutent pas. Exemple $\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)^2$

4. Morphisme d'anneaux

Définition :

Soient $(A,+,\star)$ et $(B,+,\times)$ deux anneaux et f une application de A dans B.

On dit que f est un morphisme d'anneaux si et seulement si :

- $f(1_A) = 1_B$
- $\forall x, y \in A \,/\, f(x+y) = f(x) + f(y)$
- $\forall x, y \in A \,/\, f(x \star y) = f(x) \times f(y)$

L'ensemble $Ker(f) = \{x \in A / f(x) = 0_B\}$ est le noyau de f.

Propriétés :

Si f est un morphisme d'anneaux de A dans B, alors :

- $f(0_A) = 0_B$ (i.e. $0_A \in Ker(f)$)
- f est injective si et seulement si $Ker(f) = \{0_A\}$
- Si x est inversible dans A, alors $f(x)$ est inversible dans B

Exemples :

- L'application $x \to x$ est un morphisme injectif de l'anneau $(\mathbb{Z},+,\times)$ dans l'anneau $(\mathbb{R},+,\times)$.
- L'application $x \to x \bmod n$ est un morphisme de l'anneau $(\mathbb{Z},+,\times)$ dans l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$.
  Son noyau est l'ensemble $n\mathbb{Z}$ des multiples de n.
- Soit P une matrice $n \times n$ inversible.
  L'application $\begin{array}{ccc} M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ A & \to & P\,A\,P^{-1} \end{array}$ est un isomorphisme d'anneaux (morphisme bijectif)
- Soit $\mathcal{B}$ une base de $\mathbb{R}^n$. L'application $\begin{array}{ccc} \mathcal{L}(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ f & \to & Mat_{\mathcal{B}}(f) \end{array}$ est un isomorphisme d'anneaux.
- L'application f de $\mathbb{R}$ dans $M_n(\mathbb{R})$ telle que $f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$ n'est pas un morphisme d'anneaux car $f(1) \neq I_n$.

5. Anneau intègre

Définitions :

Soient $(A,+,\star)$ un anneau et a un élément de A différent de 0.

On dit que a est un **diviseur de zéro** si $\exists b \in A-\{0\}$ / $b \star a = 0$ **ou** $\exists c \in A-\{0\}$ / $a \star c = 0$

On dit que a est **régulier** si et seulement si $\forall b,c \in A$ / $(a \star b = a \star c \Rightarrow b = c)$ et $(b \star a = c \star a \Rightarrow b = c)$

Remarques : 0 n'est pas régulier.

si a est inversible, alors a n'est pas diviseur de 0 et a est régulier

Propriété : Soit $a \in A-\{0\}$. a est régulier si et seulement si a n'est pas un diviseur de 0.

- ($\mathbb{Z}$,+, **.**) n'a pas de diviseurs de zéro. Tout entier est régulier, mais seuls -1 et 1 sont inversibles.
- Dans l'anneau $(\mathbb{R}^{\mathbb{R}},+,\times)$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ étudier $f\,g$ pour

  $f(x) = x + |x|$ et $g(x) = x - |x|$, puis pour $f(x) = \begin{matrix} 0 \text{ si } x \notin \mathbb{Q} \\ 1 \text{ si } x \in \mathbb{Q} \end{matrix}$ et $g(x) = \begin{matrix} 1 \text{ si } x \notin \mathbb{Q} \\ 0 \text{ si } x \in \mathbb{Q} \end{matrix}$
- Dans l'anneau $(\mathcal{M}_n(\mathbb{R}),+,\times)$ une matrice est régulière si et seulement si elle est inversible :

  Si A n'est pas inversible, son noyau n'est pas réduit à $\{0\}$ donc 0 est valeur propre.

  Il existe donc P inversible telle que $P^{-1}\,A\,P = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix} = A'$.

  Alors $A'\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} A' = 0$ donc en posant $B = P\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}P^{-1}$, $A\,B = B\,A = 0$

  Exemple : Étudier $A\,B$ et $B\,A$ pour $A = \begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$

Définition :

L'anneau $(A,+,\star)$ est **intègre** si et seulement si il n'a aucun diviseur de 0.

i.e. L'anneau $(A,+,\star)$ est intègre si et seulement tout élément non nul de A est régulier.

Exemples :

- ($\mathbb{Z}$,+, **.**) ($\mathbb{R}$,+, **.**) ($\mathbb{Q}$,+, **.**) sont des anneaux intègres.
- L'anneau des matrices carrées $(\mathcal{M}_n(\mathbb{R}),+,\times)$ n'est pas intègre (si $n \geqslant 2$)
- L'anneau des endomorphismes $(\mathcal{L}(E),+,\circ)$ n'est pas intègre (si $\dim(E) \geqslant 2$)
- $(\mathbb{Z}/6\mathbb{Z},+,\times)$ n'est pas intègre
- $(\mathbb{Z}/5\mathbb{Z},+,\times)$ est intègre
- Si $Card(E) \geqslant 2$, L'anneau $(\mathcal{P}(E),\Delta,\cap)$ n'est pas intègre.

6. Groupe des unités d'un anneau

Soit $(A,+,\star)$ un anneau **commutatif**.

L'ensemble $A^{\times}$ des éléments de A inversibles pour la loi $\star$ est un groupe pour la loi $\star$.

C'est le **groupe des unités** de l'anneau A.

Exemples :

- Le groupe des unités de $(\mathbb{Z},+,\times)$ est $\{-1,+1\}$
- Le groupe des unités de $(\mathbb{R},+,\times)$ est $\mathbb{R}^* = \mathbb{R}-\{0\}$, celui de $(\mathbb{C},+,\times)$ est $\mathbb{C}^* = \mathbb{C}-\{0\}$
- Le groupe des unités de $(\mathcal{M}_n(\mathbb{R}),+,\times)$ est le groupe $GL(n)$ des matrices $n\times n$ inversibles
- Le groupe des unités de $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est l'ensemble des entiers $k\in\{1,2,..,n-1\}$ qui sont premiers avec n.
  l'ordre de ce groupe est $\varphi(n)$ (indicatrice d'Euler)
- Le groupe des unités de $(\mathcal{P}(E),\Delta,\cap)$ ne contient que l'élément neutre de $\cap$: E.

8. Anneau des polynômes

Soit $(A,+,\star)$ un anneau **commutatif**.

Un **polynôme à coefficients dans** A est une suite d'éléments de A <u>nulle à partir d'un certain rang</u>.

La suite $[a_0,a_1,a_2,...,a_n,0,...0,...]$ est notée $a_0+a_1X+a_2X^2+...+a_nX^n = \sum_{k=0}^{n} a_kX^k$

Noter que des coefficients peuvent être nuls et ainsi, quand $a_{n+1}=0$, on a $\sum_{k=0}^{n} a_kX^k = \sum_{k=0}^{n+1} a_kX^k$

Si $P = a_0+a_1X+a_2X^2+...+a_nX^n$ **et** $a_n\neq 0$, on dit que P est de **degré** n :

Si $P\neq 0$, $\deg(P)$ est le **dernier** indice n tel que $a_n\neq 0$.

On définit la somme de 2 polynômes comme la somme des suites :

$$(a_n)+(b_n)=(a_n+b_n) \ : \ \sum_{k=0}^{n} a_kX^k + \sum_{k=0}^{m} b_kX^k = \sum_{k=0}^{\max(n,m)} (a_k+b_k)X^k$$

On définit le produit de 2 polynômes comme le produit de Cauchy :

$$(a_n)+(b_n)=(c_n) \text{ où } c_n=a_0b_n+a_1b_{n-1}+...+a_nb_0 = \sum_{k=0}^{n} a_kb_{n-k}$$

$$(a_0+a_1X+a_2X^2+...)(b_0+b_1X+b_2X^2+...) = a_0b_0+(a_1b_0+a_0b_1)X+(a_2b_0+a_1b_1+a_0b_2)X^2+...$$

en particulier $X^nX^m = X^{n+m}$

Muni de ces 2 opérations, l'ensemble $A[X]$ des polynômes est un anneau commutatif.

Si l'anneau A est intègre, l'anneau $A[X]$ est intègre et dans ce cas, pour deux polynômes P et Q non nuls,

on a $\deg(PQ)=\deg(P)+\deg(Q)$

Remarque : Dans $(\mathbb{Z}/6\mathbb{Z})[\mathbb{X}]$, $(1+2X+3X^2)(1-2X) = 1-X^2-6X^3 = 1-X^2$

Unités de l'anneau $\mathbb{R}[X]$: L'ensemble des polynômes constants (degré 0) non nuls

Unités de l'anneau $\mathbb{Z}[X]$: $\{-1,+1\}$

Dans $\mathbb{Z}/4\mathbb{Z}[X]$, $(1-2X)(1+2X)=1$ donc $(1-2X)$ est inversible bien que son degré soit 1.

Soient $(B,+,\star)$ un anneau **commutatif** et $(A,+,\star)$ un sous-anneau de B.

Pour tout $\alpha \in B$ et tout polynôme $P = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$ à coefficients dans A,

on pose $P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n$.

Alors, α étant fixé, l'application $\varphi_\alpha : \begin{array}{ccc} A[X] & \to & B \\ P & \to & P(\alpha) \end{array}$ est un morphisme d'anneaux.

Son image, notée $A[\alpha] = \{P(\alpha) \; / \; P \in [X]\}$ est un sous-anneau de B qui contient A.

Exemples

- $\mathbb{Z} \subset \mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{R}$.

  Tout élément de $\mathbb{Z}\left[\sqrt{2}\right]$ s'écrit de manière unique $x = a + b\sqrt{2}$

  Le noyau de $\varphi_{\sqrt{2}}$ est l'ensemble des polynômes divisibles par $X^2 - 2$.

  L'étude des unités de $\mathbb{Z}\left[\sqrt{2}\right]$permet de résoudre l'équation de (Pell-)Fermat $x^2 - 2y^2 = \pm 1$, x et $y \in \mathbb{Z}$
- Résultats analogues pour $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$. Les unités de $\mathbb{Z}[i]$ sont $\{1, i, -1, -i\}$
- $\mathbb{R}[i] = \mathbb{C}$

II/ *Corps*

1. Définition - Exemples

Un ensemble K muni de 2 opérations + et $\times$. est un **corps** (*Körper*) si

- $(K,+,\times)$ est un anneau .

  On note 0 son élément neutre de + et 1 l'élément neutre de $\times$
- Tout élément de $K-\{0\}$ a un inverse pour la loi $\times$

Si, de plus, la loi $\times$ est commutative, on dit que $(K,+,\times)$ est un **corps commutatif**.

Quand on parle de **corps**, on sous-entend fréquemment **corps commutatif (***Field***)**

Remarque (théorème de Wedderburn) Tout corps **fini** est nécessairement commutatif.

Exemples :

- $(\mathbb{R},+,\times),(\mathbb{C},+,\times),(\mathbb{Q},+,\times)$ sont des corps commutatifs
- L'anneau $(\mathbb{Z},+,\times)$ n'est pas un corps
- L'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un corps si et seulement si n est premier. Si $n=p$ est premier, on le note $\mathbb{F}_p$
- Corps(s) d'ordre 2 : $(\{a,b\},+,\times)$ avec les tables

$+$	a	b
a	a	b
b	b	a

$\times$	a	b
a	a	a
b	a	b

.

Prototype : $\mathbb{F}_2=(\mathbb{Z}/2\mathbb{Z},+,\times)$

$+$	0	1
0	0	1
1	1	0

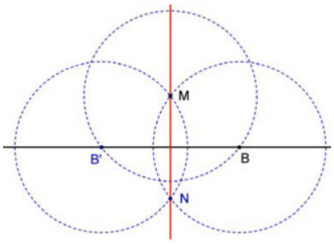
$\times$	0	1
0	0	0
1	0	1

- L'anneau $(\mathcal{M}_n(\mathbb{R}),+,\times)$ des matrices $n\times n$ n'est pas un corps (si $n\geqslant 2$)
- Soit $\mathbb{Q}[\sqrt{2}]$ l'ensemble des réels de la forme $a+b\sqrt{2}$ où a et b sont des rationnels quelconques.

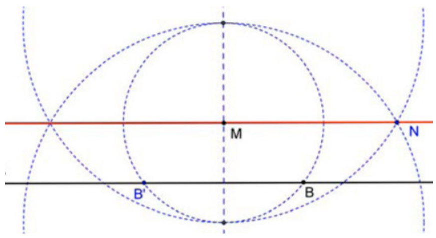
  $(\mathbb{Q}[\sqrt{2}],+,\times)$ est un corps commutatif.

Le « corps des nombres constructibles » (*à la règle et au compas*) est un corps.
Avec la règle et le compas, on peut construire :

la perpendiculaire issue de M à une droite



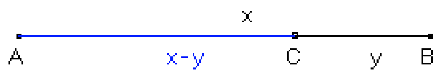
la parallèle issue de M à une droite



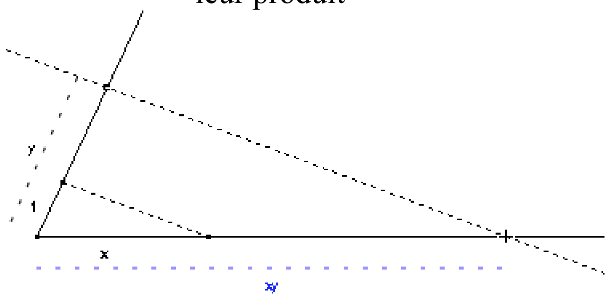
Par conséquent, 2 réels constructibles étant donnés, on peut construire :

leur somme

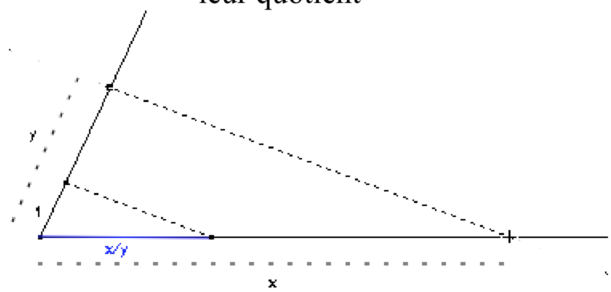
leur différence



leur produit



leur quotient



source : wikipedia

2. Propriétés

- Tout corps est un anneau intègre. (réciproque fausse)
- Propriété caractéristique :
  Dans un corps (commutatif) K, si $a \neq 0$, l'équation $a\,x + b = 0$ a une solution unique $x = -a^{-1}b$.
  On la note souvent $-\dfrac{b}{a}$.
- Dans un corps (commutatif) K, tout polynôme de degré n a au plus n racines.

3. Sous-corps

Soient $(K,+,\times)$ un corps et A une partie de K.

A est un **sous-corps** de K si et seulement si

- $(A,+,\times)$ est un sous-anneau de K .
- Tout élément de $A-\{0\}$ a un inverse dans A pour la loi $\times$ (i.e A est un corps)

Dans ce cas on dit aussi que K est une **extension** de A.

Propriété caractéristique :

- $0 \in A,\ 1 \in A$
- A est stable par les opérations $+$ et $\times$
- $\forall x \in A,\ x^{-1} \in A$.

Exemples :

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{2}\right] \subset \mathbb{Q}\left[\sqrt{2},\sqrt{3}\right] \subset \mathbb{R}$

4. Morphisme de corps

Définition :

Soient $(A,+,\times)$ et $(B,+,\times)$ deux corps et *f* une application de *A* dans *B*.

On dit que *f* est un morphisme de corps si et seulement si c'est un morphisme d'anneaux :

- $f(1_A)=1_B$
- $\forall x,y \in A \ / \ f(x+y)=f(x)+f(y)$
- $\forall x,y \in A \ / \ f(xy)=f(x)f(y)$

Propriétés :

- Tout morphisme de corps est injectif.
- Si *f* est un morphisme de corps $f(x^{-1})=(f(x))^{-1}$

5. Caractéristique d'un corps

Soit $(K,+,\times)$ un corps (commutatif) On note ici *e* l'élément neutre de $\times$

Soit $f: \begin{matrix} \mathbb{Z} & \to & K \\ n & \to & n.e \end{matrix}$ (Rappel : si $n>0$, $n.e=e+e+...+e$, $(-n).e=-(n.e)$ et $0.e=0_K$)

Alors *f* est un morphisme du groupe $(\mathbb{Z},+)$ dans le groupe $(K,+)$.

Son noyau est donc un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$.

- Si $n=0$, on dit que *K* est un corps de caractéristique nulle.
  Dans ce cas, on a $\forall x \in K \ / \ \forall n \in \mathbb{Z} \ / \ n.x=0 \Leftrightarrow (n=0 \text{ ou } x=0)$
  exemples : $\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Q}\left[\sqrt{2}\right]\ldots$
- Sinon, on dit que *K* est un corps de caractéristique *n*.
  Dans ce cas, on démontre que *n* est un nombre premier *p*, et on a alors $\forall x \in K \ / \ p.x=0$
  Exemple : $\mathbb{Z}/p\mathbb{Z}$

Si *K* est un corps de caractéristique *p*, alors $\forall x,y \in K, \forall n \in \mathbb{N} / \ (x+y)^p = x^p + y^p$