Chapitre 4 ANNEAUX - CORPS

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***)**

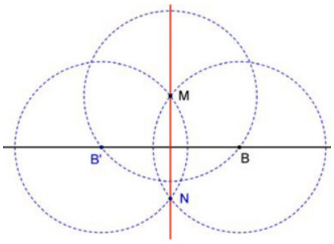
Remarque (théorème de Wedderburn) Tout corps **fini** est nécessairement commutatif.

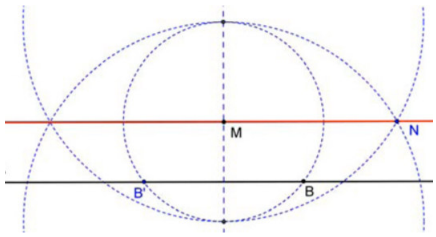
Exemples :

- $(\mathbb{R},+,\times),(\mathbb{C},+,\times),(\mathbb{Q},+,\times)$ 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 $\begin{array}{c|c|c|} + & a & b \\ \hline a & a & b \\ \hline b & b & a \\ \hline \end{array}$ $\begin{array}{c|c|c|} \times & a & b \\ \hline a & a & a \\ \hline b & a & b \\ \hline \end{array}$.

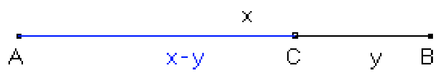
  Prototype : $\mathbb{F}_2=(\mathbb{Z}/2\mathbb{Z},+,\times)$ $\begin{array}{c|c|c|} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline \end{array}$ $\begin{array}{c|c|c|} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ \hline 1 & 0 & 1 \\ \hline \end{array}$
- L'anneau $(\mathcal{M}_n(\mathbb{R}),+,\times)$ des matrices $n\times n$ n'est pas un corps (si $n\geqslant 2$)
- Soit $\mathbb{Q}\left[\sqrt{2}\right]$ l'ensemble des réels de la forme $a+b\sqrt{2}$ où a et b sont des rationnels quelconques.
  $\left(\mathbb{Q}\left[\sqrt{2}\right],+,\times\right)$ est un corps commutatif.
  De même $\mathbb{Q}[\pi]$, $\mathbb{Q}\left[\cos\left(\frac{2\pi}{5}\right)\right]$, $\mathbb{Q}\left[\cos\left(\frac{2\pi}{7}\right)\right]$ sont des corps commutatifs,
  ainsi que $\mathbb{Q}\left[\sqrt{2}\right]\left[\sqrt{5}\right]$ noté $\mathbb{Q}\left[\sqrt{2},\sqrt{5}\right]$, etc…

- 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

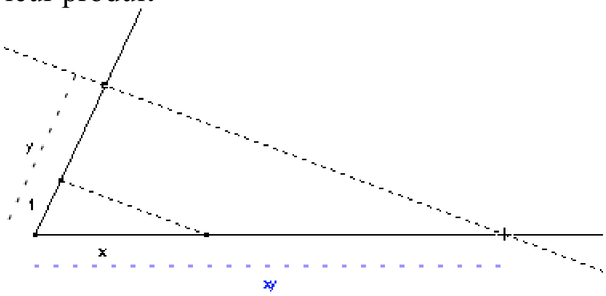


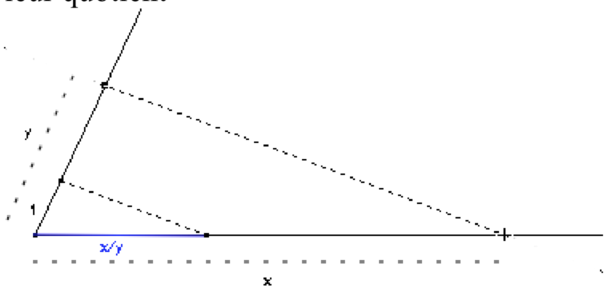


Par conséquent, 2 réels constructibles étant donnés, on peut construire :
leur somme — leur différence



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 $x = -b\,a^{-1}$.
  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 sans 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 :

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

Propriétés :

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

5. Caractéristique d'un corps

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

Soit $f:\begin{array}{ccc}\mathbb{Z} & \rightarrow & K\\ n & \rightarrow & n.e\end{array}$, où 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 $\forall x,y\in K,\forall n\in\mathbb{N}/\ (x+y)^p=x^p+y^p$