2.3 Structure de corps

2.3.1 Proposition

Soit $(R, +, \times)$ un anneau unitaire commutatif non trivial *(Cf. 2.1.3)*.
Alors, $(R, +, \times)$ est un un anneau intègre si et seulement si il vérifie la règle de simplification suivante :

$$(\forall a \in R)\,(\forall b \in R)\,(\forall c \in R)\,((ab = ac \text{ et } a \neq 0) \Longrightarrow (b = c))$$

Démonstration

1. Supposons que $(R, +, \times)$ soit un anneau intègre.
   Soient donc $a \in R$ avec $a \neq 0$, $b \in R$ $c \in R$ tels que $ab = ac$.
   Alors $ab = ac \Longleftrightarrow ab - ac = 0 \Longleftrightarrow a\,(b - c) = 0$. Comme $a \neq 0$ et $(R, +, \times)$, intègre nous avons $b - c = 0$, c'est à dire $b = c$
2. Supposons que $(R, +, \times)$ vérifie la règle de simplification.
   Soient $a \in R$ et $b \in R$ tels que $a \neq 0$ et $ab = 0$. Alors

   $$ab = 0 \Longleftrightarrow a\,(b - 0) = 0 \overset{Simplification}{\Longrightarrow} b - 0 = 0 \Longleftrightarrow b = 0$$

   Donc R est un anneau intègre.

2.3.2 Définition de corps

Un ensemble $(\mathbb{F}, +, \times)$ est un corps commutatif si et seulement si

1. $(\mathbb{F}, +, \times)$ est un anneau unitaire commutatif
2. Tout élément $a \in \mathbb{F}$ non nul admet un inverse

Remarque 11 :

On note $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$

1. Ainsi $(\mathbb{F}, +, \times)$ est un corps commutatif si et seulement si
   $\Rightarrow$ $(\mathbb{F}, +)$ est un groupe additif commutatif
   $\Rightarrow$ $(\mathbb{F}^*, \times)$ est un groupe multiplicatif commutatif
2. Pour $a \in \mathbb{F}$ et $b \in \mathbb{F}^*$, le produit ab^{-1} est noté comme le quotient $\dfrac{a}{b}$ et ce quotient est la seule solution à l'équation $bx = a$
3. Pour $b \in \mathbb{F}^*$ et $d \in \mathbb{F}^*$, l'égalité de 2 quotients $\dfrac{a}{b} = \dfrac{c}{d} \Longleftrightarrow ab^{-1} = cd^{-1} \Longleftrightarrow ad = bc$
4. **Somme, produit, quotient**
   $\Rightarrow$ Pour $b \in \mathbb{F}^*$ et $d \in \mathbb{F}^*$, nous avons $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$
   $\Rightarrow$ Pour $b \in \mathbb{F}^*$ et $d \in \mathbb{F}^*$, nous avons $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{ac}{bd}$
   $\Rightarrow$ Pour $b \in \mathbb{F}^*$, nous avons $-\dfrac{a}{b} = \dfrac{-a}{b} = \dfrac{a}{-b}$
   $\Rightarrow$ Pour $a \in \mathbb{F}^*$ et $b \in \mathbb{F}^*$, nous avons $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$
5. Il existe des corps non commutatif qu'on appelle **corps gauche**

2.3.3 Caractéristique d'un corps

Soit $(\mathbb{F}, +, \times)$ un corps commutatif

1. La caractéristique d'un corps $\mathbb{F}$ est le plus petit entier n tel que $n \times 1 = 0$
2. La caractéristique d'un corps $\mathbb{F}$ est un nombre premier

Démonstration

Soit $(\mathbb{F},+,\times)$ un corps commutatif de caractéristique p.
Supposons que p ne soit pas premier. Alors, $p = kh$ et $p \times 1 = (k \times 1)(h \times 1) = 0$
Le corps $\mathbb{F}$ étant intègre, alors $(k \times 1) = 0$ ou $(h \times 1) = 0$ car il n'y a a pas de diviseurs de zéro dans un corps.
Donc $h \leqslant p$ ou $k \leqslant p$
Ce qui contredit la définition de p. p est donc un nombre premier.

Remarque 12 :

Nous reprenons le morphisme d'anneau $f : \mathbb{Z} \longrightarrow \mathbb{F}$ défini par :

$$\left\{\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & \mathbb{F} \\ n & \longmapsto & f(n) = n1 = \underbrace{1+1+\cdots+1+1}_{n \text{ fois}} \end{array}\right.$$

Alors

1. Si $\mathbb{F}$ est de caractéristique nulle $\ker f = \{0\}$
2. Si $\mathbb{F}$ est de caractéristique p, $\ker f = p\mathbb{Z}$ et $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exemple 6 :

Des exemples de corps

1. De manière classique, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs
2. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier

   En effet ; on sait déjà que les $(\mathbb{Z}/n\mathbb{Z},+,\times)$ sont des anneaux commutatifs. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ soont les éléments premiers avec n. Ainsi, si p est premier tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont inversibles et donc $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps.

   Si n n'est pas premier, $(\mathbb{Z}/n\mathbb{Z},+,\times)$ possède de véritables diviseurs de zéro et donc ne peut être un corps.
3. Soit $(R,+,\times)$ un anneau unitaire intègre **fini**. Alors $(R,+,\times)$ est un corps

   Pour le démontrer il suffit de prouver que tout élément de R^* admet un inverse pour la multiplication.

   Pour ce faire, soit $a \in R^*$ et considérons $\psi_a : R^* \longrightarrow R^*$ défini par :

$$\left\{\begin{array}{rcl} \psi_a : R^* & \longrightarrow & R^* \\ x & \longmapsto & \psi_a(x) = ax \end{array}\right.$$

   → ψ_a est injective.
   En effet, soient $x \in R^*$ et $y \in R^*$ tels que $\psi_a(x) = \psi_a(y)$. Or :

$$\psi_a(x) = \psi_a(y) \Longleftrightarrow ax = ay \Longleftrightarrow a(x-y) = 0$$

   Comme $a \neq 0$ et que R est intègre, nous avons $a(x-y) = 0 \Longrightarrow x - y = 0 \Longleftrightarrow x = y$
   Donc ψ_a est injective.

   → Comme ψ_a est injective et que R^* est un ensemble fini, ψ_a est surjective. Il existe donc un élément a_1 tel que $aa_1 = 1$, c'est à dire que $a \in R^*$ est inversible

   $(R,+,\times)$ est donc un corps

2.3.4 Définition de sous-corps

Soit $(\mathbb{F},+,\times)$ un corps commutatif
On appelle sous-corps de $(\mathbb{F},+,\times)$, toute partie non vide $\mathbb{L} \subset \mathbb{F}$, stable pour les lois de $\mathbb{F}$ et telle que la structure induite sur $\mathbb{L}$ par ces lois, soit une structure de corps.
On dit que $\mathbb{F}$ est un sur-corps ou une extension du corps $\mathbb{L}$

Remarque 13 :

1. On appelle sous-anneau R d'un corps $\mathbb{F}$, tout sous-anneau de $\mathbb{F}$ où $\mathbb{F}$ est considéré comme un anneau *(Par exemple, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$)*
2. $\mathbb{F}$ est un sous-corps de $\mathbb{F}$. On dit qu'un corps est premier s'il ne contient d'autre sous-corps autre que lui-même. $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ où p est un nombre premier, est un exemple de corps premier

2.3.5 Théorème

Soit $(\mathbb{F}, +, \times)$ un corps commutatif et $\mathbb{L} \subset \mathbb{F}$ un sous-ensemble non vide de $\mathbb{F}$. Alors $\mathbb{L}$ est un sous-corps de $\mathbb{F}$ si et seulement si :

1. Pour tout $a \in \mathbb{L}$ et tout $b \in \mathbb{L}$ nous avons $a - b \in \mathbb{L}$ et $ab \in \mathbb{L}$
2. Pour tout $a \in \mathbb{L}^*$, alors $a^{-1} \in \mathbb{L}^*$

Démonstration

La démonstration est évidente

Remarque 14 :

Soit $(\mathbb{F}, +, \times)$ un corps commutatif. Alors l'intersection de 2 sous-corps de $\mathbb{F}$ est aussi un sous-corps de $\mathbb{F}$

Exemple 7 :

$\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$

Exercice 23 :

Nous appelons $\mathbb{Q}\left(\sqrt{2}\right) = \left\{u = p + q\sqrt{2} \text{ où } p \in \mathbb{Q} \text{ et } q \in \mathbb{Q}\right\}$. Montrer que $\mathbb{Q}\left(\sqrt{2}\right)$ est un sous-corps de $\mathbb{R}$, contenant $\mathbb{Q}$ *(C'est donc une extension de $\mathbb{Q}$)*

Exercice 24 :

Dans $\mathcal{M}_2(\mathbb{C})$, on considère l'ensemble $\mathbb{H}$ défini par :

$$\mathbb{H} = \left\{\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \text{ où } a \in \mathbb{C} \text{ et } b \in \mathbb{C}\right\}$$

Il faut montrer que $\mathbb{H}$ muni de l'addition et de la multiplication des matrices est un corps non commutatif *(corps gauche)*

2.3.6 Proposition

Un anneau unitaire commutatif non trivial est un corps si et seulement si il n'admet que des idéaux triviaux

Démonstration

Un idéal trivial d'un anneau R est un idéal I tel que $I = R$ ou $I = \{0\}$

1. **Soit $(R, +, \times)$ un anneau commutatif unitaire n'admettant que des idéaux triviaux**
   Démontrons que $(R, +, \times)$ est un corps.
   Soit $r \in R$ tel que $r \neq 0$ et regardons l'ensemble rR des multiples de r dans R ; rR est un idéal de $(R, +, \times)$ *(démonstration évidente)*
   $(R, +, \times)$ n'admettant que des idéaux triviaux, et comme $rR \neq \{0\}$, nous avons $rR = R$.
   R étant unitaire, $1 \in R$ et donc, il existe $a \in R$ tel que $ar = 1$ et donc r admet un inverse dans R et que cet inverse est a.
   $(R, +, \times)$ est donc un corps.

2. **Supposons que $(\mathbb{F}, +, \times)$ soit un corps commutatif**
Démontrons qu'il n'admet que des idéaux triviaux.
Soit donc $I \subset \mathbb{F}$ un idéal de $\mathbb{F}$ non trivial ; en particulier $I \neq \{0\}$; il existe donc $u \in I$ tel que $u \neq 0$. Comme $u \in \mathbb{F}$, u est inversible et donc u^{-1} existe.
Soit $x \in \mathbb{F}$; alors $x = \left(xu^{-1}\right) u$. I étant un idéal, alors, comme $u \in I$, nous avons $\left(xu^{-1}\right) u \in I$, c'est à dire $x \in I$, et donc nous concluons que $I = \mathbb{F}$
$\mathbb{F}$ n'admet donc que des idéaux triviaux.

2.3.7 Morphisme de corps

Soient $(\mathbb{F}_1, +, \times)$ et $(\mathbb{F}_2, +, \times)$ 2 corps commutatifs.
$\alpha : \mathbb{F}_1 \longrightarrow \mathbb{F}_2$ est un morphisme de corps si et seulement si, pour tout $x \in \mathbb{F}_1$ et tout $y \in \mathbb{F}_1$, nous avons :

1. $\alpha(x + y) = \alpha(x) + \alpha(y)$
2. $\alpha(x \times y) = \alpha(x) \times \alpha(y)$

Remarque 15 :

1. Un morphisme de corps est aussi un morphisme d'anneaux
2. Nous avons toujours le noyau d'un morphisme de corps $\ker \alpha = \{x \in \mathbb{F}_1 \text{ tels que } \alpha(x) = 0\}$
3. Nous avons, bien entendu : $\alpha(0) = 0$ et $\alpha(1) = 1$

2.3.8 Proposition

Tout morphisme de corps est injectif

Démonstration

Soient $(\mathbb{F}_1, +, \times)$ et $(\mathbb{F}_2, +, \times)$ 2 corps commutatifs et $\alpha : \mathbb{F}_1 \longrightarrow \mathbb{F}_2$ un morphisme de corps. Nous allons montrer que $\ker \alpha$ est réduit à 0, c'est à dire que $\ker \alpha = \{0\}$ et nous aurons ainsi montré que $_alpha$ est injective.
En 2.2.8, nous avons montré que $\ker \alpha$ est un idéal de $\mathbb{F}_1$; or, $\mathbb{F}_1$ étant un corps n'admet que des idéaux triviaux, c'est à dire $\ker \alpha = \{0\}$ ou $\ker \alpha = \mathbb{F}_1$

- ⋆ Tout d'abord $\ker \alpha \neq \mathbb{F}_1$ puisque $\alpha(1) = 1$ et donc , $1 \notin \ker \alpha$
- ⋆ Donc, $\ker \alpha = \{0\}$, ce qui montre que α est injectif

Donc, tout morphisme de corps est injectif

Remarque 16 :

1. Un morphisme injectif est aussi appelé **monomorphisme**
2. Un corps peut, bien entendu, ne pas être commutatif