CHAPITRE 2

STRUCTURES ALGÉBRIQUES 2 : ANNEAUX ET CORPS

Sommaire

2.1 Anneaux

2.1.1 Définitions et propriétés

Définition 2.1.1

Soit A un ensemble muni de deux lci $\times$ et $+$. On dit que $(A, +, \times)$ est un anneau si

- $(A, +)$ est un groupe commutatif.
- $\times$ est associative.
- $\times$ est distributive par rapport à $+$, ce qui signifie que

$$\forall (x, y, z) \in A^3;\ x \times (y + z) = x \times y + x \times z \text{ et } (y + z) \times x = y \times x + z \times x.$$

- $\times$ admet un élément neutre.

De plus, si $\times$ est commutative, on parlera d'anneau **commutatif**.

Notations :

- L'élément neutre de $+$ sera noté 0_A ou 0, appelé élément nul.
- L'élément neutre de la multiplication sera noté 1_A ou 1, appelé élément unité.

Exemple 18.

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}, +, \times)$ sont des anneaux.
- $(\mathbb{R}[X], +, \times)$ est un anneau, appelé *anneau des polynômes* sur $\mathbb{R}$.
- $(\mathbb{R}(X), +, \times)$ est un anneau, appelé *anneau des fractions rationnelles* sur $\mathbb{R}$.
- $(S(\mathbb{R}), +, \times)$ est un anneau, appelé *anneau des suites numériques réelles* $(S(\mathbb{R}) = \mathbb{R}^{\mathbb{N}})$.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau, appelé *anneau des fonctions de* $\mathbb{R}$ *vers* $\mathbb{R}$ et par fois noté $\mathcal{F}(\mathbb{R}, \mathbb{R})$.
- $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ)$ où $\circ$ est la composition des applications, n'est pas un anneau par manque de la distribution de $\circ$ par rapport à $+$.
- $\{0, 1\}$ muni des lois $+$ et $\times$ suivantes :

$+$	0	1
0	0	1
1	1	0

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

est un anneau.

Définition 2.1.2

Soit $(A, +, \times)$ un anneau. Un élément $x \in A$ est dit inversible s'il est inversible pour la loi $\times$ dans A, i.e. s'il existe un élément $y \in A$ tel que $x \times y = y \times x = 1_A$.
L'ensemble des éléments inversibles de A est noté $\mathcal{U}(A)$.

Exemple 2.1.1.

- $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.
- $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$.
- Soit $n \geq 2$, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid x \wedge n = 1\}$.

Remarque 2.1.1.

- 1_A est inversible.
- 0_A n'est pas inversible.
- Tout élément inversible de A est régulier pour "$\times$".

Exercice 7. Soit $(A, +, \times)$ un anneau. Montrer que $(\mathcal{U}(A), \times)$ est un groupe d'élément neutre 1_A.

2.1.2 Règles de calcul dans un anneau

Proposition 2.1.3

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

- 0_A est absorbant, i.e. $\forall x \in A,\ 0_A \times x = 0_A$.
- $\forall (x, y) \in A^2,\ (-x) \times y = x \times (-y) = -(x \times y)$.

Démonstration.

- Soit $x \in A$. On a $0_A \times x \underset{0_A \text{ neutre}}{=} (0_A + 0_A) \times x \underset{\text{distr}}{=} 0_A \times x + 0_A \times x$. Par simplification, on a alors $0_A \times x = 0_A$.
- Soient $x, y \in A$. On a $(-x) \times y + x \times y \underset{\text{distr}}{=} (-x + x) \times y = 0_A \times y \underset{\text{absor}}{=} 0_A$. $(A, +)$ étant commutatif $(-x) \times y = -(x \times y)$. On prouve de même l'autre égalité.

□

Définition 2.1.4

Un anneau $(A, +, \times)$ commutatif non nul $(A \neq \{0_A\})$ est dit intègre si :

$$\forall (a, b) \in A^2,\ ab = 0 \Rightarrow a = 0 \text{ ou } b = 0$$

Exemple 19. Reprenons les exemples ci-dessus :

- $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{Z}, +, \times)$ sont des anneaux intègres.
- $(\mathbb{R}[X], +, \times)$ est un anneau intègre.
- $(S(\mathbb{R}), +, \times)$ anneau non-intègre : $(0, 1, 0, 1, \dots) \times (1, 0, 1, 0, \dots) = (0, 0, 0, 0, \dots)$.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau non-intègre.

Proposition 2.1.5

Soient $(a_i)_{i\in I}$ une famille finie d'éléments de A et $x \in A$. Alors

$$x\left(\sum_{i\in I} a_i\right) = \sum_{i\in I} xa_i \text{ et } \left(\sum_{i\in I} a_i\right)x = \sum_{i\in I} a_i x$$

Démonstration. Par récurrence triviale sur le cardinal de I. □

On a également dans tout anneau **commutatif** les formules suivantes :

Proposition 2.1.6

Soient $(a,b) \in A^2$ et $n \in \mathbb{N}$. Alors :

$$a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^i b^{n-i-1}$$

En particulier,

$$a^n - 1 = (a-1)\sum_{i=0}^{n-1} a^i$$

Démonstration. On montre cette propriété à l'aide d'un simple calcul :

$$\begin{aligned}(a-b)\sum_{i=0}^{n-1} a^i b^{n-i-1} &= \sum_{i=0}^{n-1} a^{i+1}b^{n-i-1} - \sum_{i=0}^{n-1} a^i b^{n-i} \\ &= \sum_{i=1}^{n} a^i b^{n-i} - \sum_{i=0}^{n-1} a^i b^{n-i} = a^n - b^n.\end{aligned}$$

□

Proposition 2.1.7 (formule du binôme)

Soient $(a,b) \in A^2$ et $n \in \mathbb{N}$. Alors

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

où $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$ (coefficients binomiaux).

Démonstration. Par récurrence sur n.

— Initialisation : par convention, $(a+b)^0 = a^0 = b^0 = 1$, d'où le résultat.

— Hérédité : supposons le résultat vrai pour n. Écrivons

$$\begin{aligned}(a+b)^{n+1} &= a(a+b)^n + b(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{i+1}b^{n-i} + \sum_{i=0}^{n}\binom{n}{i}a^i b^{n+1-i}\\ &= \sum_{i=1}^{n+1}\binom{n}{i-1}a^i b^{n+1-i} + \sum_{i=0}^{n}\binom{n}{i}a^i b^{n+1-i}\\ &= a^{n+1} + b^{n+1} + \sum_{i=1}^{n}\left(\binom{n}{i} + \binom{n}{i-1}\right)a^i b^{n+1-i} = a^{n+1} + b^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}a^i b^{n+1-i}\\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}a^i b^{n+1-i}\end{aligned}$$

□

2.1.3 Sous-anneau

Définition 2.1.8

Soit $(A,+,\times)$ un anneau. On appelle sous-anneau de $(A,+,\times)$ tout anneau de la forme $(B,+,\times)$ où $B \subset A$.

Un sous-anneau est donc simplement un sous-ensemble qui est un anneau **pour les mêmes lois**. En particulier, B doit être stable par $\times$ et $+$.

Exemple 20.

— Soit $(G,+)$ un groupe. $\mathrm{Aut}(G)$ est un sous-anneau de l'anneau $(\mathrm{End}(G),+,\circ)$.

— $(\mathcal{C}(\mathbb{R},\mathbb{R}),+,\times)$ l'ensemble des fonctions continues est un sous-anneau de $(\mathbb{R}^{\mathbb{R}},+,\times)$.

— $(S_0(\mathbb{R}),+,\times)$ l'ensemble des suites de limite nulle est un sous-anneau de $(S(\mathbb{R}),+,\times)$.

Remarque 2.1.2. Pour tout $n \in \mathbb{N}$, $(\mathbb{R}_n[X],+,\times)$, l'ensemble des polynômes de degré au plus n n'est pas un sous-anneau de $(\mathbb{R}[X],+,\times)$ car $\mathbb{R}_n[X]$ n'est pas stable pour la loi $\times$ (la loi $\times$ n'est pas une lci).

Proposition 2.1.9

Soit $(A,+,\times)$ un anneau, et B une partie non vide de A. $(B,+,\times)$ est un sous-anneau de $(A,+,\times)$ si et seulement si

— $(B,+)$ est un sous groupe de $(A,+)$,

— $1_A \in B$,

— B est stable pour la loi $\times$.

Démonstration. En exercice ! □

2.1.4 Idéaux d'un anneau

Définition 2.1.10

On appelle idéal d'un anneau $(A, +, \times)$, toute partie non vide I de A telles que :

1. $(I, +)$ est un sous groupe de $(A, +)$.
2. $\forall x \in I$ et $\forall a \in A \implies ax \in I$ et $xa \in I$.

Exemple 21.

- Soit $(A, +, \times)$ un anneau. $\{0\}$ et A sont des idéaux de A, ils sont appelés les idéaux triviaux de A.
- $(\mathbb{Z}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ mais pas un idéal.
- Les $n\mathbb{Z}$ où $n \in \mathbb{N}$ sont les seuls idéaux de $(\mathbb{Z}, +, \times)$.

Théorème 2.1.11

Soit I un idéal d'un anneau $(A, +, \times)$ d'élément neutre 1_A. Les conditions suivantes sont équivalentes :

1. $1_A \in I$.
2. $I = A$.

Démonstration.

- 1) $\Rightarrow$ 2) On a toujours $I \subseteq A$, soit $x \in A$ et comme on a $1_A \in I$, alors $x = x1_A \in I$, donc $A \subseteq I$, par suite $I = A$.
- La réciproque est triviale.

□

2.1.5 Anneaux principaux

Définition 2.1.12

- Un idéal I d'un anneau $(A, +, \times)$ est **principal** s'il est engendré par un unique élément.
- De plus, si A est commutatif, alors l'idéal I est principal s'il existe $a \in I$ tel que $I = aA = Aa$. Dans ce cas, on note cet idéal (a).

$$I = (a) = aA = Aa \text{ avec } aA = \{ax \mid x \in A\}.$$

Définition 2.1.13

Un anneau intègre $(A, +, \times)$ est dit **principal** si tout idéal de A est principal.

Exemple 2.1.2.

— L'anneau $(\mathbb{Z}, +, \times)$ est principal.

— $(\mathbb{K}[X], +, \times)$ l'ensemble des polynômes à coefficients dans le corps $\mathbb{K}$ est un anneau principal.

Exercice 8. Soit $(A, +, \times)$ un anneau intègre, et a et b deux éléments de A. Montrer que

1. $a \mid b \Leftrightarrow (a) \supset (b)$.
2. $(a) = (b) \Leftrightarrow$ il existe $u \in \mathcal{U}(A)$ tel que $b = au$.

2.1.6 Morphisme d'anneaux

Définition 2.1.14

Soient $(A, +, \times)$ et $(A', +', \times')$ deux anneaux. On dit que $\phi : A \to A'$ est un morphisme d'anneaux de $(A, +, \times)$ vers $(A', +', \times')$ si et seulement si

— ϕ est un morphisme de groupes de $(A, +)$ vers $(A', +')$,

— $\phi(1_A) = 1_{A'}$,

— $\forall (a, b) \in A^2,\ \phi(a \times b) = \phi(a) \times' \phi(b)$.

Tout comme dans le cas des morphismes de groupes, les morphismes d'anneaux transportent les structures :

Proposition 2.1.15

— L'image d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

— L'image réciproque d'un sous-anneau par un morphisme d'anneaux est un sous-anneau.

Démonstration. Soit ϕ un morphisme de $(A, +, \times)$ dans $(A', +', \times')$

— Soit $(B, +, \times)$ un sous-anneau de $(A, +, \times)$
- ϕ est aussi un morphisme de groupe, et donc $(\phi(B), +')$ est un sous-groupe de $(A', +)$.
- $\phi(1_A) = 1_{A'}$ d'où $1_{A'} \in \phi(B)$.
- Soient $a' = \phi(a), b' = \phi(b) \in \phi(B)$. On a $a' \times' b' = \phi(a) \times' \phi(b) = \phi(a \times b) \in \phi(B)$.

— Soit $(B', +, \times)$ un sous-anneau de $(A', +, \times)$
- ϕ est aussi un morphisme de groupe, et donc $(\phi^{-1}(B'), +)$ est un sous-groupe de $(A, +)$.
- $\phi(1_A) = 1_{A'} \in B'$ d'où $1_A \in \phi^{-1}(B')$.
- Soient $(a, b) \in \phi^{-1}(B')$. On a $\phi(a \times b) = \phi(a) \times' \phi(b) \in B'$, d'où $a \times b \in \phi^{-1}(B')$.

□

Comme pour les morphismes de groupes, on définit également les *isomorphismes*, *endomorphismes* et *automorphismes* d'anneaux.

Exemple 22. La conjugaison de $\mathbb{C}$ dans $\mathbb{C}$ est un automorphisme d'anneau :

En effet,

— $\bar{1} = 1$.

— $\forall (z, z') \in \mathbb{C}^2 ; \overline{z + z'} = \bar{z} + \bar{z'}$.

— $\forall (z, z') \in \mathbb{C}^2 ; \overline{zz'} = \bar{z}\bar{z'}$.

2.1.7 Anneaux quotients, théorème d'isomorphisme

Soient $(A,+,\cdot)$ un anneau et I un idéal de A (idéal bilatère). L'idéal I est en particulier un sous-groupe du groupe abélien $(A,+)$. Il est trivialement distingué. On peut donc considérer le groupe quotient $(A/I,+)$. Rappelons que la loi quotient est définie par

$$\forall \overline{x},\overline{y} \in A/I,\ \overline{x}+\overline{y} = \overline{x+y} \text{ et } \overline{x} = x+I,$$

et que l'application $\phi_c : A \longrightarrow A/I,\ x \longmapsto \overline{x} = x+I$ est un morphisme de groupes.
On munit A/I d'une multiplication définie par

$$\forall \overline{x},\overline{y} \in A/I,\ \overline{x}\cdot\overline{y} = \overline{x\cdot y} \text{ (i.e. } (x+I)(y+I) = xy+I).$$

La loi quotient multiplicative est bien définie, en effet, Soient $\overline{a},\overline{b},\overline{c},\overline{d} \in A/I$, on a

$$(\overline{a},\overline{b}) = (\overline{c},\overline{d}) \Leftrightarrow \overline{a} = \overline{c} \text{ et } \overline{b} = \overline{d} \Leftrightarrow a-c \in I \text{ et } b-d \in I.$$

Comme I est un idéal, on a alors $(a-c)b \in I$ et $c(b-d) \in I$, i.e. $ab-cb \in I$ et $cb-cd \in I$, d'où $ab-cd \in I$, et donc $\overline{a\cdot b} = \overline{c\cdot d}$.

Théorème 2.1.16

Soient $(A,+,\cdot)$ un anneau et I un idéal de A. Alors

- $(A/I,+,\cdot)$ est un anneau, appelé anneau quotient de A par I.
- La surjection canonique $\phi_c : A \longrightarrow A/I$ est un morphisme d'anneaux.

Démonstration.

- **$(A/I,+,\cdot)$ est un anneau.**
  - $(A/I,+)$ est un groupe abélien : L'associativité, la commutativité, l'existence de l'élément neutre $(0+I)$ et des opposés $(-a+I)$ découlent directement des propriétés de A et du fait que $(I,+)$ est un sous-groupe du groupe $(A,+)$.
  - La loi multiplicative est associative : Pour tous $a,b,c \in A$, on a

$$(\overline{a}.\overline{b}).\overline{c} = ((a+I)(b+I))(c+I) = (abc+I) = (a+I)((b+I)(c+I)) = \overline{a}.(\overline{b}.\overline{c}).$$

  - La distributivité de '$\cdot$' par rapport à '$+$' : On a,

$$\overline{a}.(\overline{b}+\overline{c}) = (a+I)((b+I)+(c+I)) = a(b+c)+I = ab+ac+I = (ab+I)+(ac+I) = \overline{a}.\overline{b}+\overline{a}.\overline{c}.$$

  La distributivité à droite se montre de façon analogue. Ainsi, $(A/I,+,\cdot)$ est un anneau.

- **La surjection canonique est un morphisme d'anneaux.** Soit $\phi_c : A \to A/I$, $\phi_c(a) = a+I$.
  - $\phi_c(a+b) = (a+b)+I = (a+I)+(b+I) = \phi_c(a)+\phi_c(b)$,
  - $\phi_c(a.b) = ab+I = (a+I)(b+I) = \phi_c(a).\phi_c(b)$,
  - $\phi_c(1_A) = 1_A+I$, qui est l'unité de A/I (à condition que $I \neq A$).
    Donc ϕ_c est un morphisme surjectif d'anneaux.

  Ceci achève la preuve du théorème.

□

Théorème 2.1.17 (Théorème d'isomorphisme)

Soient $(A,+,\times)$ et $(B,+',\times')$ deux anneaux et $\phi : A \longrightarrow B$ un morphisme d'anneaux. Alors

$$A/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi).$$

Démonstration.

— $\mathrm{Ker}(\phi)$ est un idéal de A.

— L'application $\overline{\phi} : A/\mathrm{Ker}(\phi) \longrightarrow \mathrm{Im}(\phi)$, $x + \mathrm{Ker}(\phi) \longmapsto \phi(x)$ est un isomorphisme d'anneaux.

On a donc $A/\mathrm{Ker}(\phi) \simeq \mathrm{Im}(\phi)$. □

2.2 Corps

2.2.1 Définitions

Définition 2.2.1

Soit un ensemble K muni de deux lci $+$ et $\times$. On dit que $(K,+,\times)$ est un corps si et seulement si

— $(K,+,\times)$ est un anneau.

— Tout élément de K différent de 0_K est inversible pour la loi multiplicative.

Nous dirons par ailleurs que le corps est commutatif si la loi $\times$ est commutative.

Il s'agit donc d'une structure plus fine que la structure d'anneau.

On note $K^* = K\backslash\{0_K\}$. Muni de cette notation, on peut proposer la définition équivalente suivante :

Définition 2.2.2

Soit un ensemble K muni de deux lci $+$ et $\times$. On dit que $(K,+,\times)$ est un corps (au sens de corps commutatif) si et seulement si

— $(K,+)$ est un groupe commutatif,

— $(K^*,\times)$ est un groupe commutatif,

— $\times$ est distributive par rapport à $+$.

Exemple 23.

— $(\mathbb{R},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{C},+,\times)$ sont des corps.

— $(\mathbb{Z},+,\times)$ n'est pas un corps : 2 n'est pas inversible.

— $(\mathbb{R}(X),+,\times)$ est un corps on parlera donc de *corps des fractions rationnelles*

— $(\mathbb{R}[X],+,\times)$ n'est pas un corps : tout polynôme de degré plus grand que 1 n'est pas inversible.

— L'ensemble $\{0,1\}$ muni des lois $+$ et $\times$ est un corps : 1 est inversible, et 1 est son propre inverse. Il s'agit du plus petit corps possible.

2.2.2 Sous-corps

Définition 2.2.3

Soit $(K, +, \times)$ un corps. On appelle sous-corps de $(K, +, \times)$ tout corps de la forme $(K', +, \times)$ où $K' \subset K$.

Comme pour les groupes et les anneaux, on obtient une caractérisation, dont la démonstration est laissée en exercice.

Proposition 2.2.4

Soit $(K, +, \times)$ un corps, et K' une partie non vide de K. Alors
$(K', +, \times)$ est un sous-corps de $(K, +, \times)$ si et seulement si

- K' contient 1_K.
- $(K', +)$ est un sous-groupe de $(K, +) : \forall (x, y) \in K'^2 \ \ x - y \in K'$
- $(K'^*, \times)$ est un sous-groupe de $(K^*, \times) : \forall (x, y) \in (K'^*)^2 \ \ xy^{-1} \in K'^*$

Démonstration. En exercice ! □

Exemple 24.

- $(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$, qui est un sous-corps de $(\mathbb{C}, +, \times)$.
- $\mathbb{Q}[i] := \{a + ib \mid (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $(\mathbb{C}, +, \times)$.

2.2.3 Morphismes de corps

Définition 2.2.5

Soient $(K, +, \times)$ et $(K', +', \times')$ deux corps. On dit que $\phi : K \to K'$ est un morphisme de corps de $(K, +, \times)$ vers $(K', +', \times')$ si et seulement si ϕ est un morphisme d'anneaux de $(K, +, \times)$ vers $(K', +', \times')$.

Toutes les propriétés des morphismes d'anneaux se transposent donc. On peut montrer que l'on a de plus préservation de l'inverse pour $\times$ par tout morphisme de corps, et que les images et images réciproques de sous-corps sont des sous-corps.

Exemple 25. La conjugaison est un automorphisme de corps sur $\mathbb{C}$.

Exercice 9. Montrer que les seuls automorphismes de corps **continus** sur $\mathbb{C}$ sont l'identité et la conjugaison.

2.2.4 Caractéristique d'un corps

Définition 2.2.6

La **caractéristique** d'un corps K est le plus petit entier $k \geq 1$, s'il existe, tel que $k.1_K = 0_K$. S'il n'existe pas, on dit que le corps est de caractéristique 0. On la note $\text{car}(K)$.

Lemme 2.2.7

Soit $(K, +, \times)$ un corps. Alors soit $\text{car}(K) = 0$, soit $\text{car}(K)$ est un nombre premier.

Proposition 2.2.8

Soit $(K, +, \times)$ un corps commutatif.

- Si $\text{car}(K) = 0$, alors K est infini.
- Si $\text{car}(K) = p$ avec $p \in \mathbb{N}^*$, alors $\overline{f} : \mathbb{Z}/p\mathbb{Z} \longrightarrow K$ définie par $\overline{f}(\overline{k}) = k.1_K$ (pour tout $k \in \mathbb{Z}$) est un morphisme injectif.

Démonstration.

- Si $\text{car}(K) = 0$, alors par définition, le morphisme $f : \mathbb{Z} \longrightarrow K$ défini par $f(k) = k.1_K$ (pour tout $k \in \mathbb{Z}$) est injectif. D'où, $\mathbb{Z}$ et $f(\mathbb{Z})$ sont isomorphes. En particulier, $f(\mathbb{Z})$ est infini. Donc, K contient une partie infini et alors il est infini aussi.
- Il faut d'abord montrer que $\overline{f}$ est une application bien définie. Soit donc $a, b \in \mathbb{Z}$ tels que $\overline{a} = \overline{b}$. Alors, $b - a = kp$ pour certain $k \in \mathbb{Z}$. Alors,

$$\overline{f}(\overline{b}) - \overline{f}(\overline{a}) = b.1_K - a.1_K = (b-a).1_K = (kp).1_K = k(p.1_K) = k.0_K = 0_K.$$

D'où, $\overline{f}(\overline{b}) = \overline{f}(\overline{a})$, ce qui montre que $\overline{f}$ est une application bien définie.
Il est facile de montrer que $\overline{f}$ est un morphisme de corps. Il reste à montrer qu'il est injectif. Soit $a \in \mathbb{Z}$ tel que $\overline{f}(\overline{a}) = 0_K$. Alors, $a.1_K = 0_K$.

□

Exemple 2.2.1.

- Les corps $(\mathbb{Q}, +, \times)$, $(\mathbb{Q}, +, \times)$ et $(\mathbb{Q}, +, \times)$ sont des corps de caractéristique nulle.
- Si $p \in \mathbb{N}^*$ un nombre premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique p.

Exercice 10. Montrer que tout anneau intègre fini est un corps.