2. Structures usuelles : Anneaux et Corps

2.1 Anneaux

2.1.1 Définitions et règles de calcul

Définition 2.1 On appelle anneau tout triplet $(A,+,\cdot)$ constitué de :

1. un ensemble non vide A,
2. une loi de composition interne $+$ de A, telle que $(A,+)$ est un groupe commutatif,
3. une loi de composition interne $\cdot$, dite multiplication de A, associative, ayant un élément neutre (appelée élément unité) et distributive par rapport à l'addition.

De plus, un anneau $(A,+,\cdot)$ est dit commutatif si sa multiplication est commutative.

R Soient $+$ et $\cdot$ deux lois internes dans un ensemble A, on dit que $\cdot$ est distributive sur $+$ si

$$\forall x,y,z \in A, \quad x\cdot(y+z) = x\cdot y + x\cdot z \quad \text{et} \quad (y+z)\cdot x = y\cdot x + z\cdot x.$$

Exemple. L'ensemble $(\mathbb{Z},+,\cdot)$ est un anneau commutatif.

Notation. *Dans ce qui suit, $(A,+,\cdot)$ désigne un anneau et on adopte les notations suivantes :*

– *L'élément neutre pour l'addition est noté 0_A, et l'élément unité est noté 1_A.*

– *Le symétrique de $a \in A$ pour l'addition (opposé de a) est noté $-a$, et le symétrique de $a \in A$ pour la multiplication (inverse de a), s'il existe, est noté a^{-1}.*

– *Soient $a \in A$ et $n \in \mathbb{Z}$, on définit l'élément $na \in A$ par :*

- *si $n \geqslant 0$, na est la somme de n termes égaux à a, c'est-à-dire*

$$0\,a = 0_A,\ 1\,a = a \ \text{ et pour } n > 1,\ na = \underbrace{a+a+\cdots+a}_{n\ fois}.$$

- *si $n < 0$, $na = (-n)(-a)$ est la somme de $-n$ termes égaux à l'opposé de a, c-à-dire*

$$na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{(-n)\ fois}.$$

- *si $a \in A$ et $n \in \mathbb{N}$, on définit l'élément $a^n \in A$ par :*

$$a^0 = 1,\ a^1 = a \ \text{ et pour } n > 1,\ a^n = a \cdot a^{n-1} = a^{n-1} \cdot a.$$

Proposition 2.1 Pour tout $a \in A$, on a

$$0_A \cdot a = a \cdot 0_A = 0_A.$$

Preuve *La relation $a + 0_A = a$ implique $a \cdot (a + 0_A) = a^2$ et $(a + 0_A) \cdot a = a^2$, d'où*

$$a^2 + a \cdot 0_A = a^2 \quad \text{et} \quad a^2 + 0_A \cdot a = a^2.$$

Finalement, on obtient $a \cdot 0_A = 0_A$ et $0_A \cdot a = 0_A$. ∎

R Si $A = \{a\}$, il n'y a qu'une seule loi de composition interne, donnée par $a * a = a$. Le seul anneau ayant un seul élément est dit anneau nul. Dans le cas contraire, on a le résultat suivant :

Proposition 2.2 Si A est de cardinal $\mathrm{Card}(A) > 1$, alors $\quad 0_A \neq 1_A$.

Preuve *Si $0_A = 1_A$. Soit $a \in A$ quelconque, on a : $a \cdot 1_A = a \cdot 0_A$, d'où $a = 0_A$, absurde.* ∎

Proposition 2.3 Pour tout $(a, b) \in A^2$, on a $\quad (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

Preuve *La relation $x + (-x) = 0_A$ implique successivement*

$$\begin{aligned}
a + (-a) = 0_A &\implies (a + (-a)) \cdot b = 0_A \cdot b \\
&\implies a \cdot b + (-a) \cdot b = 0_A \\
&\implies (-a) \cdot b = -(a \cdot b), \\
b + (-b) = 0_A &\implies a \cdot (b + (-b)) = a \cdot 0_A \\
&\implies a \cdot b + a \cdot (-b) = 0_A \\
&\implies a \cdot (-b) = -(a \cdot b)
\end{aligned}$$

∎

Corollaire 2.1 Soient a, b et c dans A et $n \in \mathbb{Z}$, on a

$$\begin{array}{cc}
(-1_A) \cdot a = -a & (-a) \cdot (-b) = a \cdot b \\
a \cdot (b - c) = a \cdot b - a \cdot c & (b - c) \cdot a = b \cdot a - c \cdot a \\
(na) \cdot b = a \cdot (nb) = n(a \cdot b) & na = (n1_A) \cdot a
\end{array}$$

Exercice 2.1 *Soit* $(A,+,\cdot)$ *un anneau tel que*

$$\forall (x,y) \in A^2,\ \ (x\cdot y)^2 = x^2\cdot y^2 \quad et \quad \forall x \in A\ :\ x+x=0_A \implies x=0_A.$$

En utilisant 1_A+y *et* x*, montrer que* $x\cdot y\cdot x = x^2\cdot y = y\cdot x^2$ *et puis que l'anneau* A *est commutatif.*

Exercice 2.2 *Soit* $(A,+,\cdot)$ *un anneau et* a *un élément de* A *tel que* $a^3=0_A$*. Montrer que* 1_A-a *est inversible et son inverse est* 1_A+a+a^2*.*

Théorème 2.1 — Formule du binôme de Newton. Soient a et b deux éléments d'un anneau $(A,+,\cdot)$ tels que $ab=ba$ et $n\in\mathbb{N}^*$. On a

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k}b^k \quad \text{avec la convention} \quad a^0=b^0=1_A. \tag{2.1}$$

Preuve *L'égalité* (2.1) *est vraie si* $n=1$*. Supposons qu'elle est vraie au rang* $n-1$ *où* $n\geqslant 2$*, alors*

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1}\\
&= (a+b)\sum_{k=0}^{n-1} C_{n-1}^k a^{n-1-k}b^k\\
&= \sum_{k=0}^{n-1} C_{n-1}^k a^{n-k}b^k + \sum_{k=0}^{n-1} C_{n-1}^k a^{n-1-k}b^{k+1}\\
&= \sum_{k=0}^{n-1} C_{n-1}^k a^{n-k}b^k + \underbrace{\sum_{p=1}^{n} C_{n-1}^{p-1} a^{n-p}b^p}_{p=k+1}\\
&= a^n + \sum_{k=1}^{n-1} C_{n-1}^k a^{n-k}b^k + \underbrace{\sum_{k=1}^{n-1} C_{n-1}^{k-1} a^{n-k}b^k}_{k=p} + b^n\\
&= a^n + \sum_{k=1}^{n-1} \underbrace{\left(C_{n-1}^k + C_{n-1}^{k-1}\right)}_{=C_n^k} a^{n-k}b^k + b^n\\
&= a^n + \sum_{k=1}^{n-1} C_n^k a^{n-k}b^k + b^n = \sum_{k=0}^{n} C_n^k a^{n-k}b^k.
\end{aligned}$$

On a donc montrer que si la propriété est vraie au rang $n-1$*, alors elle l'est au rang* n*. Comme elle est aussi vérifié pour* $n=1$*, alors elle l'est pour tout* $n\in\mathbb{N}^*$*.*

■

Corollaire 2.2

$$\sum_{k=0}^{n} C_n^k = 2^n \quad \text{et} \quad \sum_{k=0}^{n} (-1)^k C_n^k = 0.$$

Proposition 2.4 Pour x et y d'un anneau A tels que $x\cdot y = y\cdot x$ et $n\in\mathbb{N}^*$, on a

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^{n-1-k}\cdot y^k.$$

Preuve *On a*

$$\begin{aligned}(x-y)\sum_{k=0}^{n-1} x^{n-1-k}\cdot y^k &= x\sum_{k=0}^{n-1} x^{n-1-k}\cdot y^k - \; y\sum_{k=0}^{n-1} x^{n-1-k}\cdot y^k \\ &= \sum_{k=0}^{n-1} x^{n-k}\cdot y^k - \sum_{k=0}^{n-1} y\cdot x^{n-1-k}\cdot y^k.\end{aligned}$$

Comme y commute avec x, il vient

$$\begin{aligned}(x-y)\sum_{k=0}^{n-1} x^{n-1-k}\cdot y^k &= \sum_{k=0}^{n-1} x^{n-k}\cdot y^k - \sum_{k=0}^{n-1} x^{n-1-k}\cdot y^{k+1} \\ &= \sum_{k=0}^{n-1} x^{n-k}\cdot y^k - \sum_{k=1}^{n} x^{n-k}\cdot y^k \\ &= x^n + \sum_{k=1}^{n-1} x^{n-k}\cdot y^k - \sum_{k=1}^{n-1} x^{n-k}\cdot y^k - y^n \\ &= x^n - y^n.\end{aligned}$$

■

Corollaire 2.3 Pour $x\in A$ et $n\in\mathbb{N}$, on a

$$x^n - 1_A = (x-1_A)\cdot\sum_{k=0}^{n-1} x^k = \left(\sum_{k=0}^{n-1} x^k\right)\cdot(x-1_A).$$

Si $x-1_A$ est inversible d'inverse $(x-1_A)^{-1}$, alors

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

Corollaire 2.4 Pour $x\in A$ et $n\in\mathbb{N}$, on a

$$x^{2n+1} + 1_A = (x+1_A)\cdot\sum_{k=0}^{2n}(-1)^k x^k = \left(\sum_{k=0}^{2n}(-1)^k x^k\right)\cdot(x+1_A).$$

Proposition 2.5 Pour $x_1,\cdots,x_n$ et $y_1,\cdots,y_p$ des éléments de A et n, $p\in\mathbb{N}^*$, on a

$$\sum_{i=0}^{n}\left(\sum_{j=0}^{p} x_i y_j\right) = \sum_{j=0}^{p}\left(\sum_{i=0}^{n} x_i y_j\right) = \left(\sum_{i=0}^{n} x_i\right)\left(\sum_{j=0}^{p} y_j\right).$$

Exercice 2.3 *Soit a et b d'un anneau commutatif A tel que $b^2 = 0_A$, développer $(a+b)^5$.*

2.1.2 Éléments particuliers

Proposition 2.6 L'ensemble U_A des éléments inversibles de l'anneau $(A,+,\cdot)$ est stable pour la multiplication de A. De plus, $(U_A,\cdot)$ est un groupe, appelé groupe des inversibles de A.

Preuve *Soient a et b deux éléments de U_A d'inverses a^{-1} et b^{-1}, on a*

$$(a\cdot b)\cdot(b^{-1}\cdot a^{-1}) = a\cdot(b\cdot b^{-1})\cdot a^{-1} = a\cdot 1_A\cdot a^{-1} = a\cdot a^{-1} = 1_A,$$
$$(b^{-1}\cdot a^{-1})\cdot(a\cdot b) = b^{-1}\cdot(a^{-1}\cdot a)\cdot b = b^{-1}\cdot 1_A\cdot b = b^{-1}\cdot b = 1_A.$$

Par suite, il vient que $a\cdot b$ est inversible d'inverse $b^{-1}\cdot a^{-1}$, et alors

$$a\cdot b \in U_A.$$

De plus, $U_A \neq \emptyset$ puisque $1_A \in U_A$, et avec l'associativité de la multiplication de A, la stabilité de U_A pour cette opération et le fait que tout $a \in U_A$ est l'inverse de a^{-1}, il vient que $(U_A,\cdot)$ est un groupe. ■

Définition 2.2 Soit $(A,+,\cdot)$ un anneau non nul, on dit que $a \in A\setminus\{0_A\}$ est

- diviseur de 0_A à droite s'il existe $x \neq 0_A$ de A tel que : $x\cdot a = 0_A$,
- diviseur de 0_A à gauche si il existe $y \neq 0_A$ de A tel que : $a\cdot y = 0_A$,
- diviseur de 0_A si il est diviseur de 0_A à droite et à gauche.

Définition 2.3 Un anneau $(A,+,\cdot)$ est dit sans diviseurs de 0_A lorsque on a

$$\forall a,b \in A \ : \ a\cdot b = 0_A \implies [a = 0_A \ \text{ ou } \ b = 0_A].$$

Un anneau non nul $(A,+,\cdot)$ est dit intègre si il est commutatif et sans diviseurs de 0_A.

Remarque L'anneau $(\mathbb{Z},+,\cdot)$ est un anneau intègre.

Exercice 2.4 *Soient $(A,+,\cdot)$ un anneau non nul et $(a,b) \in A^2$. On suppose que ab est inversible et que ba n'est un diviseur de 0_A. Montrer que a et b sont inversibles (on peut utiliser l'inverse x de ab et développer $(ba)(bxa - 1_A)$.*

Définition 2.4 Un élément non nul $a \in A$ est dit nilpotent lorsqu'il existe $n \in \mathbb{N}$ tel que

$$a^n = 0_A.$$

R On remarque que si $a^n = 0_A$, alors $a^m = 0_A$ pour tout $m \geq n$.

Exercice 2.5 *Soit a et b des éléments nilpotents d'un anneau commutatif A. Montrer que $a+b$ est nilpotent.*

Exercice 2.6 *Soit a un élément nilpotent d'un anneau A. Montrer que $1_A - a$ est inversible et calculer son inverse.*

Exercice 2.7 *Soit A un anneau et $(a,b) \in A^2$ tel que ab est nilpotent. Montrer que ba l'est aussi.*

2.2 Morphismes d'anneaux

Définition 2.5 On dit que φ est un morphisme d'anneaux, de $(A,+,\cdot)$ dans $(B,+,\cdot)$, lorsque :

- φ est un morphisme de groupes, de $(A,+)$ dans $(B,+)$, c-à-dire
$$\varphi(x+y) = \varphi(x) + \varphi(y),$$
- pour tout x, $y \in A$, on a : $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$,
- $\varphi(1_A) = 1_B$.

Proposition 2.7 Soient $a \in A$ et $n \in \mathbb{Z}$, on a :

- $\varphi(0_A) = 0_B$, $\varphi(-a) = -\varphi(a)$ et $\varphi(na) = n\varphi(a)$.
- Si a est inversible dans A, alors $\varphi(a)$ est inversible dans B et on a
$$\varphi(a^{-1}) = (\varphi(a))^{-1}.$$
- si $n \in \mathbb{N}^*$, alors on a
$$\varphi(a^n) = (\varphi(a))^n.$$

Preuve *À vérifier en exercice.* ■

Exercice 2.8 *Soient $(A,+,\cdot)$ un anneau, on considère l'application $\varphi : A \to A$, $x \mapsto x^2$.*

1. *Montrer que si φ est un morphisme d'anneaux, alors* $\forall x \in A,\ \ x^2 = -x^2$.
2. *Montrer que si en plus φ est surjectif, alors*
$$\forall a \in A, \ \ a = -a,$$
et puis l'anneau A est commutatif.

2.3 Sous-anneau

Définition 2.6 Une partie non vide B de A est sous-anneau de $(A,+,\cdot)$ lorsque :

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

– B est stable pour la multiplication de A, c-à-dire : $\forall x, y \in B, \quad x \cdot y \in B$,

– $1_A \in B$.

Proposition 2.8 Une partie non vide B de A est un sous-anneau de $(A,+,\cdot)$ si et seulement si

– $\forall x, y \in B, \quad x - y \in B$,

– $\forall x, y \in B, \quad x \cdot y \in B$,

– $1_A \in B$.

Preuve *À vérifier en exercice.* ■

R Une partie non vide B de A est un sous-anneau de $(A,+,\cdot)$ si et seulement si c'est une partie contenant 1_A, stable pour les opérations de A, et si, pour les restrictions de ces opérations, $(B,+,\cdot)$ est un anneau.

Proposition 2.9 Soit φ un morphisme d'anneaux de $(A,+,\cdot)$ dans $(B,+,\cdot)$, alors

– si A' est un sous-anneau de $(A,+,\cdot)$, alors $\varphi(A')$ est un sous-anneau de $(B,+,\cdot)$,

– si B' est un sous-anneau de $(B,+,\cdot)$, alors $\varphi^{-1}(B')$ est un sous-anneau de $(A,+,\cdot)$.

Preuve *À vérifier en exercice.* ■

Exercice 2.9
1. *Montrer que $A = \{x + y\sqrt{5}\ ;\ x, y \in \mathbb{Q}\}$ est un anneau pour l'addition et la multiplication usuelles.*
2. *En est-il de même pour $B = \{x + iy\ ;\ x, y \in \mathbb{Q}\}$ et $C = \{x + y\sqrt[3]{2}\ ;\ x, y \in \mathbb{Z}\}$?*
   (on admet, pour cette question, que 2 n'est pas le cube d'un rationnel, ni d'un entier)

2.4 Idéaux

Définition 2.7 Une partie I d'un anneau $(A,+,\cdot)$ est un idéal à gauche (resp. à droite) de A si

– I est sous-groupe commutatif de $(A,+)$,

– pour tout $x \in I$ et $a \in A$, on a : $a \cdot x \in I$ (resp. $x \cdot a \in I$) (stabilité externe).

R La partie I est dite idéal bilatère de A si elle est à la fois un idéal à droite et un idéal à gauche de A. En général, on utilise le mot idéal pour désigner un idéal bilatère. Si en particulier, l'anneau A est commutatif, il y'a équivalence entre idéal à gauche, idéal à droite et idéal bilatère de A.

Exemple. A et $\{0_A\}$ sont des idéaux de l'anneau A, et tout idéal différent de A, est appelé idéal propre (ou strict) de A.

Remarque Si I est un idéal à gauche (resp. à droite ou bilatère) d'un anneau A qui contient 1_A alors $I = A$. En effet, si l'idéal I de A contenant 1_A, alors pour tout $a \in A$, on a

$$a = a \cdot 1_A \in I.$$

Par suite, il vient $A \subset I$ et alors $A = I$.

Exercice 2.10 *Montrer que l'intersection d'une famille non vide d'idéaux d'un anneau A est un idéal de A.*

Exercice 2.11 *Soient I et J deux idéaux de l'anneau commutatif $(A, +, \cdot)$. On considère*

$$I + J = \{x + y \; ; \; x \in I, y \in J\} \quad et \quad I \cdot J = \{\underbrace{x_1 \cdot y_1 + \cdots + x_n \cdot y_n}_{somme\ finie} \; ; \; n \in \mathbb{N}^*, x_i \in I, y_i \in J\}.$$

On dit que les deux idéaux I et J sont premiers entre eux si $I + J = A$.

1. *Montrer que $I + J$ et $I \cdot J$ sont des idéaux de A.*
2. *Montrer que $I \cdot J \subset I \cap J$.*
3. *Montrer que $(I + J) \cdot (I \cap J) \subset I \cdot J$.*
4. *Montrer que si I et J sont premiers entre eux, alors $I \cdot J = I \cap J$.*

Exercice 2.12 *Soient I et J deux idéaux de l'anneau commutatif A. On considère*

$$(I : J) = \{a \in A \; ; \; aJ \subset I\}.$$

1. *Montrer que $(I : J)$ est un idéal de A contenant I.*
2. *Montrer que $(I : J)J \subset I$.*
3. *Montrer que si K est un idéal de A, alors*

$$(I \cap J : K) = (I : K) \cap (J : K) \quad et \quad (I : J + K) = (I : K) \cap (J : K).$$

Proposition 2.10 Soit $\varphi : A \to B$ un morphisme d'anneaux, alors on a

- le noyau de φ est un idéal bilatère de l'anneau A.
- si J est un idéal à gauche (resp. à droite, resp. bilatère) de l'anneau B, alors $I = \varphi^{-1}(J)$ est un idéal à gauche (resp. à droite, resp. bilatère) de l'anneau A.

Preuve *À vérifier en exercice.* ■

Définition 2.8 Soit I un idéal d'un anneau A. On dit que

– I est premier si et seulement si $I \neq A$ et si

$$\forall x, y \in A \ : \quad x \cdot y \in I \implies \left[x \in I \ \text{ ou } \ y \in I\right].$$

– I est principal si il existe $a \in A$ tel que

$$I = \left\{x \cdot a \ ; \ x \in A\right\},$$

autrement dit, I est engendré par un unique élément a de A, et dans ce cas, I est appelé l'idéal engendré par $a \in A$, noté (a).

– I est maximal si il est strict et si il n'est contenu dans aucun idéal autre que A, c-à-dire

$$\text{Pour tout idéal } J \text{ de } A : \quad I \subset J \implies \left[I = J \ \text{ ou } \ J = A\right].$$

Définition 2.9 Un anneau est dit principal si il est intègre et que tous ses idéaux sont principaux.

Théorème 2.2 — de Krull. Soit I un idéal d'un anneau A, alors il existe un idéal maximal de A contenant I.

Preuve *Soit $\mathcal{I}$ l'ensemble des idéaux de A contenant I et non égaux à A. On a $\mathcal{I}$ est non vide car il contient I, $\mathcal{I}$ est un ensemble partiellement ordonné par l'inclusion, et $\mathcal{I}$ est inductif puisque tout partie P non vide de $\mathcal{I}$ totalement ordonnée pour l'inclusion possède un majorant $\bigcup_{I \in P} I$, qui est bien un idéal propre de $\mathcal{I}$ car c'est la réunion d'une suite croissante d'idéaux propres de $\mathcal{I}$. En appliquant le lemme de Zorn, il vient que $\mathcal{I}$ possède un élément maximal. Ce dernier est un idéal propre de A contenant I et qui n'est contenu dans aucun autres idéaux strict de A.*

■

Exercice 2.13 *Soit A un anneau commutatif.*

1. *Déterminer les idéaux premiers de $\mathbb{Z}$.*
2. *Soient I un idéal de A, $x \in A \setminus I$ et J l'idéal engendré par I et x. Montrer que*

$$J = \{a \in A \ ; \ \exists i \in I, \exists k \in A, \ a = i + kx\}.$$

3. *En déduire que tout idéal maximal, est premier.*
4. *Montrer que si l'anneau A est principal, alors tout idéal premier est maximal.*

2.5 Corps

Définition 2.10 Un corps est un anneau commutatif $(K, +, \cdot)$ dont le groupe des inversibles est

$$K^* = K \setminus \{0_K\}.$$

Exemple. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ ont des structures de corps pour leur addition et multiplication respectives.

Définition 2.11 Un sous-corps d'un corps $(K, +, \cdot)$ est un sous-anneau L qui, pour les lois induites sur L par celles de K, est un corps.

Définition 2.12 Un morphisme de corps est un morphisme des anneaux sous-adjacents.

Exercice 2.14 *Soit $f : K \to L$ un morphisme de corps de K dans L. Montrer que f est injectif.*

Proposition 2.11 Soit K un corps, alors $1_K \neq 0_K$ et K ne possède pas de diviseurs de 0 (et par conséquent, K est un anneau intègre).

Preuve *Le premier point est évident puisque tout élément d'un corps, sauf 0_K, est inversible. Pour le second point, supposons qu'il existe x et y dans K tels que $x \cdot y = 0$. Si de plus $x \neq 0_K$, alors x est inversible et donc*

$$x^{-1} \cdot x \cdot y = x^{-1} \cdot 0_K = 0_K.$$

Par conséquent, il vient $y = 0_K$ et donc x, y ne sont pas des diviseurs de 0.

■

Exercice 2.15 *Montrer que tout anneau intègre fini est un corps.*

Proposition 2.12 Les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier. Inversement, si A est un anneau n'ayant comme seuls idéaux que l'idéal nul et lui même alors A est un corps.

Preuve $(\Rightarrow)$ *: Supposons que K est un corps. Soient I un idéal non nul de l'anneau K et soit donc x un élément non nul de I. Par définition d'un corps, x est inversible dans K d'inverse noté x^{-1}. Puisque I est un idéal de K, on a $x^{-1} \cdot x \in I$. Mais $x^{-1} \cdot x = 1_K$, d'où $1_K \in I$ et donc*

$$I = K.$$

$(\Leftarrow)$ *: Supposons maintenant que les seuls idéaux de l'anneau A sont l'idéal nul et A tout entier. Il suffit de montrer que tout les éléments non nuls de A sont inversibles. Soit $x \neq 0_A \in A$ et (x) l'idéal engendré par x. Comme x n'est pas nul, cet idéal n'est pas nul non plus. Il est alors égal à A tout entier. L'unité de A est donc élément de (x). Ceci signifie qu'il existe $y \in A$ tel que*

$$x \cdot y = 1_A$$

Par suite, on obtient que x est inversible d'inverse y et c'est ceci qu'on cherche à prouver.

■

Théorème 2.3 — Corps des fractions d'un anneau intègre. Soit un anneau intègre $(A, +, \cdot)$, alors il existe un corps $(K, +, \cdot)$, unique à un isomorphisme près, tel que

- il existe un sous-anneau A' de $(K, +, \cdot)$ isomorphe à $(A, +, \cdot)$,
- tout sous-anneau de $(K, +, \cdot)$ contenant A' est K lui-même.

Preuve *Admis.* ■

R

1. Le corps K est appelé le corps des fractions de l'anneau intègre A, noté $Frac(A)$.
2. L'isomorphisme φ de A dans A' permet d'identifier a et $\varphi(a)$ pour tout $a \in A$. En particulier, on note
$$\varphi(0_A) = 0_K \text{ et } \varphi(1_A) = 1_K.$$

3. Le corps des rationnels est le corps des fractions de l'anneau intègre $(\mathbb{Z},+,\cdot)$.
4. Une construction des corps de fractions consiste à examiner les couples (a,b) de $A\times A^*$ où $A^*=A\setminus\{0_A\}$, en convenant que deux couples (a,b) et (a',b') définissent le même élément du corps des fractions de A, noté $\frac{a}{b}$, lorsque on a
$$a\cdot b'=a'\cdot b.$$
5. L'ensemble $Frac(A)$ est muni d'une structure de corps pour les deux lois
$$\frac{a}{b}+\frac{a'}{b'}=\frac{a\cdot b'+a'\cdot b}{b\cdot b'} \quad \text{et} \quad \frac{a}{b}*\frac{a'}{b'}=\frac{a\cdot a'}{b\cdot b'}$$

Exercice 2.16 *Soit I un idéal d'un anneau commutatif A. On considère l'ensemble quotient*
$$A/I=\{\bar{x},\ x\in A\}\ \textit{avec}\ \bar{x}=\{y\in A\,,\ x-y\in I\}.$$
Cet ensemble est un anneau, dit anneau quotient, quand on le munit des lois qui font de la projection canonique $\pi : A\to A/I$, $x\mapsto\bar{x}$ un morphisme d'anneau, c'est-à-dire
$$\bar{x}+\bar{y}=\overline{x+y}\ \textit{et}\ \bar{x}\cdot\bar{y}=\overline{x\cdot y}.$$
1. *Montrer que I est premier si et seulement si A/I est un anneau intègre.*
2. *Montrer que I est maximal si et seulement si A/I est un corps.*
3. *En déduire une autre preuve de : I maximal implique que I est premier.*