Master 1 Mathématiques 2017–2018

Cours d'Algèbre

Paul LESCOT

Bureau n^{o} M.2.24

paul.lescot@univ-rouen.fr

Université de Rouen

Laboratoire de Mathématiques Raphaël Salem,

Avenue de l'Université, BP.12,

F76801 Saint-Étienne-du-Rouvray.

Rédigé avec LaTeX

par Hicham AMARIR

le 13 septembre 2026

Table des matières

Chapitre 1

Anneaux — Définitions et généralités

Définition 1.1 : (*Anneau*)

On appelle ***anneau*** un ensemble A muni de deux lois de composition interne $+$ et $\cdot$ telles que

$$(A_1) \quad \forall (a,b,c) \in A^3, \quad (a+b)+c = a+(b+c)$$

$$(A_2) \quad \exists 0_A \in A, \forall a \in A, \quad a+0_A = 0_A + a = a$$

$$(A_3) \quad \forall a \in A, \exists a' \in A, \quad a+a' = a'+a = 0_A$$

$$(A_4) \quad \forall (a,b) \in A^2, \quad a+b = b+a$$

$$(A_5) \quad \forall (a,b,c) \in A^3, \quad a\cdot(b\cdot c) = (a\cdot b)\cdot c \qquad \text{(associativité de } \cdot\text{)}$$

$$(A_6) \quad \forall (a,b,c) \in A^3, \quad a\cdot(b+c) = (a\cdot b)+(a\cdot c) \qquad \text{(distributivité à gauche de } \cdot \text{ par rapport à } +\text{)}$$

$$(A_7) \quad \forall (a,b,c) \in A^3, \quad (a+b)\cdot c = (a\cdot c)+(b\cdot c) \qquad \text{(distributivité à droite de } \cdot \text{ par rapport à } +\text{)}$$

Remarque :

$$(A_1), (A_2), (A_3) \text{ et } (A_4) \Longleftrightarrow (A,+) \text{ est un groupe abélien}$$

Définition 1.2 : (*Anneau unitaire*)

Soit $(A\,;+\,;\cdot)$ un anneau.

Si de plus

$$(A_8) \quad \exists 1_A \in A, (\forall a \in A), \quad a\cdot 1_A = 1_A \cdot a = a$$

alors l'anneau est dit ***unitaire*** et 1_A est appelé l'***unité*** de A.

Définition 1.3 : (*Anneau commutatif*)

Soit $(A\,;+\,;\cdot)$ un anneau.

Si on a

$$(A_9) \quad \forall (a,b) \in A^2, \quad a\cdot b = b\cdot a$$

alors l'anneau est dit ***commutatif***.

Remarque :

⊛ En présence de $(A_1), (A_2), (A_3), (A_4), (A_5)$ et (A_9), les axiomes (A_6) et (A_7) sont équivalents : l'un entraîne l'autre. Par exemple, (A_6) et (A_9) entraînent (A_7) :

Soit $(a,b,c) \in A^3$.

$$\begin{aligned} (a+b)\cdot c &= c\cdot(a+b) && \text{par } (A_9) \\ &= c\cdot a + c\cdot b && \text{par } (A_6) \\ &= a\cdot c + b\cdot c && \text{par } (A_9) \end{aligned}$$

⊛ $(A_1), (A_2), (A_3), (A_5), (A_6), (A_7)$ et (A_8) entraînent (A_4).

Soit $(a,b) \in A^2$.

$$\begin{aligned}
(a+b)+(a+b) &= 1_A \cdot (a+b) + 1_A \cdot (a+b) && \text{par } (A_8)\\
&= (1_A + 1_A) \cdot (a+b) && \text{par } (A_7)\\
&= ((1_A + 1_A) \cdot a) + ((1_A + 1_A) \cdot b) && \text{par } (A_6)\\
&= (1_A \cdot a + 1_A \cdot a) + (1_A \cdot b + 1_A \cdot b) && \text{par } (A_7)\\
&= (a+a)+(b+b) && \text{par } (A_8)
\end{aligned}$$

D'une part,

$$\begin{aligned}
(a+b)+(a+b) &= a+(b+(a+b)) && \text{par } (A_1)\\
&= a+((b+a)+b) && \text{par } (A_1)
\end{aligned}$$

D'autre part,

$$\begin{aligned}
(a+a)+(b+b) &= a+(a+(b+b)) && \text{par } (A_1)\\
&= a+((a+b)+b) && \text{par } (A_1)
\end{aligned}$$

Comme $(a+b)+(a+b) = (a+a)+(b+b)$, on obtient

$$a+((b+a)+b) = a+((a+b)+b) \qquad (*)$$

Soit a' un symétrique de a pour $+$ (donné par (A_3)). En ajoutant a' à gauche de chaque membre de $(*)$:

$$\begin{aligned}
a'+(a+((b+a)+b)) &= \left(a'+a\right)+((b+a)+b) && \text{par } (A_1)\\
&= 0_A+((b+a)+b) && \text{par } (A_3)\\
&= (b+a)+b && \text{par } (A_2)
\end{aligned}$$

et de même

$$\begin{aligned}
a'+(a+((a+b)+b)) &= \left(a'+a\right)+((a+b)+b) && \text{par } (A_1)\\
&= 0_A+((a+b)+b) && \text{par } (A_3)\\
&= (a+b)+b && \text{par } (A_2)
\end{aligned}$$

D'après $(*)$, ces deux quantités sont égales, donc

$$(b+a)+b = (a+b)+b$$

Soit b' un symétrique de b pour $+$. En ajoutant b' à droite de chaque membre :

$$\begin{aligned}
&((b+a)+b)+b' = ((a+b)+b)+b'\\
\iff &(b+a)+\left(b+b'\right) = (a+b)+\left(b+b'\right) && \text{par } (A_1)\\
\iff &(b+a)+0_A = (a+b)+0_A && \text{par } (A_3)\\
\iff &b+a = a+b && \text{par } (A_2)
\end{aligned}$$

Donc $a+b = b+a$.

Propriété 1.4 : (*Unicité de l'unité*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau.

Si l'on a (A_8), l'élément 1_A est unique.

Plus généralement, si $*$ est une loi de composition interne sur un ensemble E, il existe au plus un élément neutre pour $*$.

Preuve :

Soient e et e' deux éléments neutres pour $*$.

$$\forall x \in E, \quad x * e = e * x = x$$

$$\forall x \in E, \quad x * e' = e' * x = x$$

Si $x = e'$,

$$e' * e = e * e' = e'$$

Si $x = e$,

$$e * e' = e' * e = e$$

Donc

$$e' = e * e' = e$$

Donc

$$e' = e$$

Autrement dit, si deux éléments sont neutres alors ils sont égaux. Ce qui prouve l'unicité de l'élément neutre.

Exemple :

Exemples d'anneaux :

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs, unitaires.
- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \;\middle|\; (a,b) \in \mathbb{Z}^2\right\}$
- $\mathbb{C}[x]$
- $\mathbb{C}[x,y]$
- $\mathcal{M}_2(\mathbb{R})$ est un anneau unitaire non commutatif.
- $\mathbb{H}$

Convention 1.5 : (*Notations et conventions du chapitre*)

Dans toute la suite du chapitre, si ce n'est pas précisé alors A est un anneau, $0 = 0_A$, $-a = a'$, $1 = 1_A$ (s'il y a lieu).

Propriété 1.6 : (*Absorption du zéro*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau.

$$\forall a \in A, \quad a \cdot 0 = 0 \cdot a = 0$$

Preuve :

Soit $a \in A$.

$$\begin{aligned} a\cdot 0 + a\cdot 0 &= a\cdot(0+0) && \text{par } (A_6)\\ &= a\cdot 0 \end{aligned}$$

Soit $(a\cdot 0)'$ un symétrique de $a\cdot 0$ pour $+$ (donné par (A_3), $(A,+)$ étant un groupe).

En ajoutant $(a\cdot 0)'$ à droite de chaque membre :

$$\begin{aligned} & (a\cdot 0 + a\cdot 0) + (a\cdot 0)' = a\cdot 0 + (a\cdot 0)' \\ \iff & a\cdot 0 + \big(a\cdot 0 + (a\cdot 0)'\big) = 0 && \text{par } (A_1) \text{ et } (A_3)\\ \iff & a\cdot 0 + 0 = 0 && \text{par } (A_3)\\ \iff & a\cdot 0 = 0 && \text{par } (A_2) \end{aligned}$$

De même,

$$0\cdot a = 0$$

Donc

$$a\cdot 0 = 0\cdot a = 0$$

Propriété 1.7 : (*Règle des signes*)

Soit $(A\,;+\,;\cdot)$ un anneau.

Pour tous éléments a et b de A, le produit de l'un par l'opposé de l'autre est égal à l'opposé de leur produit :

$$\forall\,(a,b)\in A^2,\quad a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$$

Preuve :

Soit $(a,b)\in A^2$.

$$\begin{aligned} a\cdot b + a\cdot(-b) &= a\cdot(b+(-b)) && \text{par } (A_6)\\ &= a\cdot 0 && \text{par } (A_3)\\ &= 0 && \text{par la proposition 1.6} \end{aligned}$$

Ainsi, $a\cdot(-b)$ est le symétrique de $a\cdot b$ pour $+$, c'est-à-dire :

$$a\cdot(-b) = -(a\cdot b)$$

De même,

$$\begin{aligned} a\cdot b + (-a)\cdot b &= (a+(-a))\cdot b && \text{par } (A_7)\\ &= 0\cdot b && \text{par } (A_3)\\ &= 0 && \text{par la proposition 1.6} \end{aligned}$$

Donc $(-a)\cdot b$ est également le symétrique de $a\cdot b$ pour $+$, soit :

$$(-a)\cdot b = -(a\cdot b)$$

On en conclut donc que :

$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

Corollaire 1.8 : (*Produit de deux opposés*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau.

Le produit des opposés de deux éléments de A est égal au produit de ces deux éléments :

$$\forall\,(a,b) \in A^2, \quad (-a) \cdot (-b) = a \cdot b$$

Preuve :

Soit $(a,b) \in A^2$.

$$\begin{aligned} (-a) \cdot (-b) &= -(a \cdot (-b)) && \text{par la proposition 1.7} \\ &= -(-(a \cdot b)) && \text{par la proposition 1.7} \\ &= a \cdot b && \text{car } -(-x) = x \text{ dans le groupe } (A,+) \end{aligned}$$

Définition 1.9 : (*Puissances dans un anneau*)

Soient $(A\,;\,+\,;\,\cdot)$ un anneau et $a \in A$.

Pour tout $m \in \mathbb{N}^*$, on définit la puissance m-ième de a par récurrence :

$$a^1 = a$$
$$a^{m+1} = a^m \cdot a$$

Si, de plus, A est unitaire, on pose :

$$a^0 = 1_A$$

Propriété 1.10 : (*Règle des puissances*)

Soient $(A\,;\,+\,;\,\cdot)$ un anneau et $a \in A$.

Pour tout $m \in \mathbb{N}^*$ et pour tout $n \in \mathbb{N}^*$, on a :

$$a^{m+n} = a^m \cdot a^n = a^n \cdot a^m$$

Si, de plus, A est unitaire, cette égalité reste vraie pour tout $m \in \mathbb{N}$ et pour tout $n \in \mathbb{N}$.

Preuve :

Cas des exposants strictement positifs.

Montrons par récurrence sur $n \in \mathbb{N}^*$ que, pour tout $m \in \mathbb{N}^*$, on a :

$$a^{m+n} = a^m \cdot a^n$$

Initialisation $(n = 1)$:

Pour tout $m \in \mathbb{N}^*$, la définition des puissances donne :

$$\begin{aligned} a^{m+1} &= a^m \cdot a \\ &= a^m \cdot a^1 \end{aligned}$$

La propriété est donc vraie au rang 1.

Hérédité :

Soit $n \in \mathbb{N}^*$. Supposons que, pour tout $m \in \mathbb{N}^*$, on ait :

$$a^{m+n} = a^m \cdot a^n$$

Soit $m \in \mathbb{N}^*$. Alors :

$$\begin{aligned}
a^{m+(n+1)} &= a^{(m+n)+1} && \text{par associativité de + dans } \mathbb{N} \\
&= a^{m+n} \cdot a && \text{par définition de } a^{m+1} \\
&= \left(a^m \cdot a^n\right) \cdot a && \text{par hypothèse de récurrence} \\
&= a^m \cdot \left(a^n \cdot a\right) && \text{par associativité de } \cdot \text{ dans } A \\
&= a^m \cdot a^{n+1} && \text{par définition de } a^{n+1}
\end{aligned}$$

La propriété est donc vraie au rang $n+1$.

Par récurrence, pour tout $m \in \mathbb{N}^*$ et pour tout $n \in \mathbb{N}^*$, on a :

$$a^{m+n} = a^m \cdot a^n$$

De plus, l'addition dans $\mathbb{N}$ étant commutative, on a $m+n = n+m$. Par conséquent :

$$\begin{aligned}
a^m \cdot a^n &= a^{m+n} \\
&= a^{n+m} && \text{car } m+n = n+m \text{ dans } \mathbb{N} \\
&= a^n \cdot a^m && \text{d'après ce qui précède}
\end{aligned}$$

Ainsi, pour tout $m \in \mathbb{N}^*$ et pour tout $n \in \mathbb{N}^*$:

$$a^{m+n} = a^m \cdot a^n = a^n \cdot a^m$$

Cas d'un anneau unitaire.

Supposons que A est unitaire.

Soit $m \in \mathbb{N}$. Lorsque $n = 0$, on a :

$$\begin{aligned}
a^{m+0} &= a^m \\
&= a^m \cdot 1_A \\
&= a^m \cdot a^0
\end{aligned}$$

De même, lorsque $m = 0$, pour tout $n \in \mathbb{N}$, on a :

$$\begin{aligned}
a^{0+n} &= a^n \\
&= 1_A \cdot a^n \\
&= a^0 \cdot a^n
\end{aligned}$$

Ainsi, l'égalité reste vraie pour tout $m \in \mathbb{N}$ et pour tout $n \in \mathbb{N}$:

$$a^{m+n} = a^m \cdot a^n = a^n \cdot a^m$$

Définition 1.11 : (*Sous-anneau*)

Soit $(A\,;+\,;\cdot)$ un anneau.

On appelle ***sous-anneau*** de A une partie B de A qui, munie de la restriction sur B des opérations $+$ et $\cdot$, est un anneau.

Théorème 1.12 : (*Caractérisation des sous-anneaux*)

Soit $(A\,;+\,;\cdot)$ un anneau et B une partie de A.

B est un sous-anneau de A si et seulement si :

$$(i)\quad B \neq \emptyset$$

$$(ii)\quad \forall (x,y) \in B^2,\quad x-y \in B$$

$$(iii)\quad \forall (x,y) \in B^2,\quad x\cdot y \in B$$

Preuve :

Sens direct ($\Rightarrow$) :

Supposons que B est un sous-anneau de A.

- Par définition de sous-anneau, B muni des restrictions des lois de A est un anneau.

  Tout anneau possède un élément neutre pour l'addition, noté ici 0_B.

  Par définition de cet élément neutre, on a $0_B \in B$, ce qui implique que $B \neq \emptyset$.

  La condition (i) est donc vérifiée.

- 0_B est l'élément neutre de $(B,+)$ donc

  $$0_B + 0_B = 0_B$$

  Comme $(A,+)$ est un groupe et que l'élément neutre est unique :

  $$0_B = 0_A$$

  B muni de la restriction de $+$ vérifie l'axiome (A_3), donc il existe $z \in B$ tel que :

  $$y+z = z+y = 0_B = 0_A$$

  Ainsi,

  $$y+z = 0_A$$

  donc

  $$z = -y$$

  Autrement dit, z est l'opposé de y dans A.

  Comme $z \in B$, cela implique que $-y \in B$.

  Par conséquent, pour tout $x \in B$:

  $$x-y = \underbrace{x}_{\in B} + \underbrace{(-y)}_{\in B} \in B$$

  La somme appartient effectivement à B car B est un anneau.

  La condition (ii) est donc vérifiée.

⊛ B est un sous-anneau, donc B est un anneau. B est donc stable pour la multiplication, donc :

$$x \cdot y \in B$$

Donc la condition (iii) est vérifiée.

Sens réciproque ($\Leftarrow$) :

Supposons que les conditions (i), (ii) et (iii) sont vérifiées. Montrons que B est un anneau.

⊛ Comme $B \neq \emptyset$, il existe $u \in B$. Alors :

$$0_A = u - u \in B \qquad \text{par } (ii)$$

⊛ Soient $(x, y) \in B^2$. On a :

$$-y = \underbrace{0_A}_{\in B} - \underbrace{y}_{\in B} \in B \qquad \text{par } (ii)$$

Donc :

$$x + y = \underbrace{x}_{\in B} - \underbrace{(-y)}_{\in B} \in B \qquad \text{par } (ii)$$

De plus, par (iii), $x \cdot y \in B$.

Ainsi, B est stable pour $+$ et $\cdot$. Ce sont donc des lois de composition interne.

⊛ B vérifie les axiomes (A_1), (A_4), (A_5), (A_6) et (A_7) par héritage de A (les opérations sont les restrictions de celles de A).

⊛ On a $0_A \in B$ et pour tout $x \in B$:

$$x + 0_A = 0_A + x = x$$

Donc B vérifie l'axiome (A_2) avec $0_B = 0_A$.

⊛ Soit $x \in B$.

Soit $x' = -x$ l'opposé de x dans A. On a :

$$x + x' = x' + x = 0_A$$

De plus, $x' \in B$ (car $x' = 0_A - x \in B$ par (ii)).

Donc :

$$x + x' = x' + x = 0_B$$

Ainsi, B satisfait l'axiome (A_3).

Finalement, B est un sous-ensemble de A qui satisfait la définition d'anneau 1.1.

Donc B est un sous-anneau de A.

Propriété 1.13 : (*Sous-anneau d'un anneau commutatif*)

Si A est un anneau commutatif, tout sous-anneau de A est également commutatif.

Preuve :

Soit B un sous-anneau de A. Soient $x, y \in B$.

Comme $B \subseteq A$, on a $x, y \in A$. Puisque A est commutatif :

$$x \cdot y = y \cdot x$$

Donc B est commutatif.

Définition 1.14 : (*Sous-anneau unitaire*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau unitaire.

On dit que B est un ***sous-anneau unitaire*** de A si B est un sous-anneau de A et $1_A \in B$.

Propriété 1.15 : (*Unité d'un sous-anneau unitaire*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau unitaire et B un sous-anneau unitaire de A.

Alors B est un anneau unitaire et l'unité de B est l'unité de A :

$$1_B = 1_A$$

Preuve :

Soit B un sous-anneau unitaire de A.

Par définition, $1_A \in B$.

Soit $b \in B$.

Comme $B \subseteq A$, on a $b \in A$.

Puisque 1_A est l'unité de A :

$$b \cdot 1_A = 1_A \cdot b = b$$

De plus, $1_A \in B$ par hypothèse. Donc 1_A est un élément neutre pour la multiplication dans B.

Par unicité de l'élément neutre (proposition 1.4), on en déduit que :

$$1_B = 1_A$$

Ainsi, B est un anneau unitaire d'unité 1_A.

Remarque :

▲ On peut avoir :

(i) A anneau unitaire ;

(ii) B sous-anneau de A ;

(iii) B unitaire ;

(iv) B n'est pas un sous-anneau unitaire de A.

Exemple :

⊛ Soit $A = \mathbb{R} \times \mathbb{R}$ muni des lois usuelles.

Alors A est un anneau unitaire d'unité $1_A = (1,1)$.

Considérons $B = \mathbb{R} \times \{0\} = \{(x,0) \mid x \in \mathbb{R}\}$.

- ⊛ B est un sous-anneau de A (stable par + et $\cdot$, contient $0_A = (0,0)$).
- ⊛ B est unitaire d'unité $1_B = (1,0)$ car pour tout $(x,0) \in B$:

$$(x,0) \cdot (1,0) = (1,0) \cdot (x,0) = (x,0)$$

- ⊛ Cependant, $1_A = (1,1) \notin B$ (car la deuxième composante n'est pas nulle).

Donc B n'est pas un sous-anneau unitaire de A au sens de la définition 1.14, bien que B soit lui-même un anneau unitaire.

⊛ Soit $A = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}\,;\,\overline{1}\,;\,\overline{2}\,;\,\overline{3}\,;\,\overline{4}\,;\,\overline{5}\}$.

A est un anneau commutatif unitaire d'unité $1_A = \overline{1}$.

Considérons $B = \{\overline{0}\,;\,\overline{3}\}$.

Les tables d'addition et de multiplication dans B (par restriction des lois de A) sont :

$+$	$\overline{0}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{3}$	$\overline{0}$	$\overline{3}$

B muni des restrictions des opérations est un anneau unitaire d'unité $1_B = \overline{3}$.

B est un sous-anneau de A.

Cependant, B n'est pas un sous-anneau unitaire de A car $1_A = \overline{1} \notin B$.

Chapitre 2

Idéaux et morphismes d'anneaux

Définition 2.1 : (*Idéal à droite et à gauche*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau.

On appelle ***idéal à droite*** de A une partie I de A telle que :

$$(i)\quad (I,+) \text{ est un sous-groupe de } (A,+)$$
$$(ii)\quad \forall i \in I,\ \forall a \in A,\quad i\cdot a \in I$$

On appelle ***idéal à gauche*** de A une partie I de A telle que :

$$(i)\quad (I,+) \text{ est un sous-groupe de } (A,+)$$
$$(ii)\quad \forall i \in I,\ \forall a \in A,\quad a\cdot i \in I$$

Définition 2.2 : (*Idéal bilatère*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau.

On appelle ***idéal bilatère*** de A un idéal à la fois à droite et à gauche de A.

Propriété 2.3 : (*Idéaux dans un anneau commutatif*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau commutatif et I une partie de A.

Les assertions suivantes sont équivalentes :

$$I \text{ est un idéal à droite} \iff I \text{ est un idéal à gauche}$$
$$\iff I \text{ est un idéal bilatère}$$

Preuve :

Soit $(A\,;\,+\,;\,\cdot)$ un anneau commutatif et I une partie de A.

Sens direct ($\Rightarrow$) :

Supposons que I est un idéal à droite de A.

Par définition :

- $\circledast$ $(I,+)$ est un sous-groupe de $(A,+)$;
- $\circledast$ $\forall i \in I,\ \forall a \in A,\quad i\cdot a \in I$.

Comme A est commutatif, pour tous $a \in A$ et $i \in I$, on a :

$$a\cdot i = i\cdot a$$

Or $i\cdot a \in I$ (car I est un idéal à droite). Donc :

$$a\cdot i \in I$$

Ainsi, I vérifie également la condition de stabilité par multiplication à gauche.

Par conséquent, I est un idéal à gauche de A, et donc un idéal bilatère.

Sens réciproque ($\Leftarrow$) :

Si I est un idéal bilatère, alors par définition (définition 2.2), I est à la fois un idéal à droite et un idéal à gauche de A.

Les trois assertions sont donc équivalentes.

Exemple :

(i) Les idéaux de $\mathbb{Z}$ sont les $a\mathbb{Z}$ pour $a \in \mathbb{N}$, où :

$$a\mathbb{Z} = \{a \cdot x \mid x \in \mathbb{Z}\}$$

Comme $\mathbb{Z}$ est un anneau commutatif, par 2.3 les $a\mathbb{Z}$ sont des idéaux bilatères.

(ii) Soit $A = \mathcal{M}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| (a,b,c,d) \in \mathbb{R}^4 \right\}$.

Les seuls idéaux bilatères de A sont $\{0_A\}$ et A.

Cependant, A possède une infinité d'idéaux à droite.

Preuve : Soit I un idéal bilatère de A tel que $I \neq \{0_A\}$.

Il existe donc $M \in I$ tel que $M \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. On note $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a \neq 0$ ou $b \neq 0$ ou $c \neq 0$ ou $d \neq 0$.

Étape 1 : Isoler un coefficient non nul.

On effectue des multiplications par des matrices élémentaires (qui sont dans A) pour déplacer les coefficients :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} M = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} \in I$$

$$M \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} \in I$$

Par ces permutations, on voit que si un coefficient est non nul, on peut obtenir une matrice dans I ayant un coefficient non nul en position $(1,1)$.

On peut donc supposer que $a \neq 0$.

Étape 2 : Obtenir la matrice identité dans I.

Puisque $a \neq 0$, on a $a^{-1} \in \mathbb{R}$.

$$M \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I \quad \text{(notée } E_{11}\text{)}$$

À partir de E_{11}, on engendre les autres matrices élémentaires :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in I \quad \text{(notée } E_{21}\text{)}$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I \quad \text{(notée } E_{22}\text{)}$$

Par somme :

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \in I$$

Conclusion :

Soit $N \in A$. Puisque $I_2 \in I$ et que I est un idéal (stable par multiplication à gauche par tout élément de A) :

$$N = N \cdot I_2 \in I$$

Donc $A \subset I$, et comme $I \subset A$, on a $I = A$.

Remarque : L'ensemble

$$\Delta = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| \, (a,b) \in \mathbb{R}^2 \right\}$$

est un idéal **à gauche** de A.

En effet, pour toute matrice $\begin{pmatrix} c & d \\ e & f \end{pmatrix} \in A$ et $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in \Delta$:

$$\begin{pmatrix} c & d \\ e & f \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \in \Delta$$

(La deuxième colonne reste nulle).

Définition 2.4 : (*Morphisme d'anneaux*)

Soient $(A\,;\,+_A\,;\,\times_A)$ et $(B\,;\,+_B\,;\,\times_B)$ deux anneaux.

On appelle ***morphisme*** de A dans B une application $\varphi\colon A \longrightarrow B$ telle que :

$$\forall (x,y) \in A^2, \quad \varphi(x +_A y) = \varphi(x) +_B \varphi(y)$$
$$\text{et} \quad \varphi(x \times_A y) = \varphi(x) \times_B \varphi(y)$$

Exemple :

Il est important de ne pas confondre morphismes de groupes et morphismes d'anneaux.

- La fonction exponentielle $\exp\colon (\mathbb{R},+) \longrightarrow (\mathbb{R}_+^*,\times)$ définie par $\exp(x) = e^x$ est un **morphisme de groupes** car :

$$\forall (x,y) \in \mathbb{R}^2, \quad \exp(x+y) = \exp(x) \times \exp(y)$$

Cependant, ce n'est **pas** un morphisme d'anneaux de $(\mathbb{R},+,\times)$ dans $(\mathbb{R},+,\times)$ car :

$$\exp(x+y) \neq \exp(x) + \exp(y)$$
$$\exp(x \times y) \neq \exp(x) \times \exp(y)$$

- L'identité $\mathrm{id}\colon \mathbb{R} \longrightarrow \mathbb{R}$ définie par $\mathrm{id}(x) = x$ est un **morphisme d'anneaux** (et même un isomorphisme) car :

$$\forall (x,y) \in \mathbb{R}^2, \quad \mathrm{id}(x+y) = \mathrm{id}(x) + \mathrm{id}(y)$$
$$\mathrm{id}(x \times y) = \mathrm{id}(x) \times \mathrm{id}(y)$$

- L'application nulle $0\colon A \longrightarrow B$ définie par $0(x) = 0_B$ pour tout $x \in A$ est un morphisme de groupes additifs, mais ce

n'est généralement **pas** un morphisme d'anneaux (sauf si B est l'anneau nul) car :

$$0\,(1_A) = 0_B \neq 1_B$$

(sauf dans le cas trivial où $0_B = 1_B$, c'est-à-dire $B = \{0_B\}$).

Définition 2.5 : (*Noyau et image d'un morphisme*)

Soient $(A\,;\,+_A\,;\,\times_A)$ et $(B\,;\,+_B\,;\,\times_B)$ deux anneaux et $\varphi\colon A \longrightarrow B$ un morphisme d'anneaux.

On définit :

$$\operatorname{Ker}\varphi = \{x \in A \mid \varphi(x) = 0_B\} \quad \text{le noyau de } \varphi$$

$$\operatorname{Im}\varphi = \{\varphi(x) \mid x \in A\} \quad \text{l'image de } \varphi$$

Notations : $\operatorname{Ker}\varphi = \ker\varphi = \operatorname{Ker}(\varphi) = \ker(\varphi)$.

Théorème 2.6 : (*Propriétés du noyau et de l'image*)

Soient $(A\,;\,+_A\,;\,\times_A)$ et $(B\,;\,+_B\,;\,\times_B)$ deux anneaux et $\varphi\colon A \longrightarrow B$ un morphisme d'anneaux.

① $\operatorname{Ker}\varphi$ est un idéal de A.

② $\operatorname{Im}\varphi$ est un sous-anneau de B.

Preuve :

① **$\operatorname{Ker}\varphi$ est un idéal de A.**

⊛ **$\operatorname{Ker}\varphi$ est un sous-groupe de $(A,+)$.**

★ $\operatorname{Ker}\varphi$ *est non vide :*

On a :

$$\begin{aligned} \varphi(0_A) &= \varphi(0_A + 0_A) && \text{car } 0_A \text{ est l'élément neutre de } (A,+) \\ &= \varphi(0_A) + \varphi(0_A) && \text{car } \varphi \text{ conserve l'addition} \end{aligned}$$

En soustrayant $\varphi(0_A)$ dans les deux membres, on obtient :

$$\varphi(0_A) = 0_B$$

Donc $0_A \in \operatorname{Ker}\varphi$, ce qui implique que $\operatorname{Ker}\varphi \neq \emptyset$.

★ *Stabilité par soustraction :*

Soient $(x,y) \in (\operatorname{Ker}\varphi)^2$. On a $\varphi(x) = 0_B$ et $\varphi(y) = 0_B$.

On peut écrire :

$$\begin{aligned} 0_B = \varphi(x) &= \varphi((x-y)+y) && \text{car } x = (x-y)+y \\ &= \varphi(x-y) + \varphi(y) && \text{car } \varphi \text{ conserve l'addition} \\ &= \varphi(x-y) + 0_B && \text{car } y \in \operatorname{Ker}\varphi \\ &= \varphi(x-y) \end{aligned}$$

Donc $\varphi(x-y) = 0_B$, ce qui signifie que $x - y \in \operatorname{Ker}\varphi$.

Ainsi, $\operatorname{Ker}\varphi$ est un sous-groupe de $(A,+)$.

⊛ **Stabilité par multiplication.**

Soit $x \in \operatorname{Ker}\varphi$ et $y \in A$. On a $\varphi(x) = 0_B$.

$$\begin{aligned}\varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y) && \text{car } \varphi \text{ conserve la multiplication}\\ &= 0_B \cdot \varphi(y)\\ &= 0_B && \text{par absorption du zéro dans } B\end{aligned}$$

Donc $x \cdot y \in \operatorname{Ker}\varphi$.

De même :

$$\begin{aligned}\varphi(y \cdot x) &= \varphi(y) \cdot \varphi(x)\\ &= \varphi(y) \cdot 0_B\\ &= 0_B\end{aligned}$$

Donc $y \cdot x \in \operatorname{Ker}\varphi$.

Finalement, $\operatorname{Ker}\varphi$ est un idéal bilatère de A.

② $\operatorname{Im}\varphi$ **est un sous-anneau de** B**.**

⊛ $\operatorname{Im}\varphi$ *est non vide :*

On a :

$$0_B = \varphi(0_A) \in \operatorname{Im}\varphi$$

Donc $\operatorname{Im}\varphi \neq \emptyset$.

⊛ *Stabilité par soustraction et multiplication :*

Soient $(x, y) \in (\operatorname{Im}\varphi)^2$. Par définition de l'image, il existe $a \in A$ et $a' \in A$ tels que :

$$\begin{aligned}x &= \varphi(a)\\ y &= \varphi(a')\end{aligned}$$

★ **Soustraction :**

$$\begin{aligned}x - y &= \varphi(a) - \varphi(a')\\ &= \varphi(a - a') && \text{car } \varphi \text{ conserve l'addition}\end{aligned}$$

Comme $a - a' \in A$, on a $x - y \in \operatorname{Im}\varphi$.

★ **Multiplication :**

$$\begin{aligned}x \cdot y &= \varphi(a) \cdot \varphi(a')\\ &= \varphi(a \cdot a') && \text{car } \varphi \text{ conserve la multiplication}\end{aligned}$$

Comme $a \cdot a' \in A$, on a $x \cdot y \in \operatorname{Im}\varphi$.

Finalement, $\operatorname{Im}\varphi$ est un sous-anneau de B.

Théorème 2.7 : (*Construction d'un morphisme à partir d'un idéal*)

Soit $(A\,;+\,;\cdot)$ un anneau et I un idéal bilatère de A.

Il existe un anneau B et un morphisme $\varphi\colon A \longrightarrow B$ tels que :

$$I = \operatorname{Ker}\varphi$$

Preuve :

① **Définition d'une relation d'équivalence $\mathcal{R}_I$.**

Définissons une relation $\mathcal{R}_I$ sur A par :

$$x\,\mathcal{R}_I\,y \iff x-y\in I$$

et montrons que c'est une relation d'équivalence.

⊛ *Réflexivité :*

Pour tout $x\in A$:

$$x-x=0_A\in I \qquad \text{car } I \text{ est un sous-groupe de } (A,+)$$

Donc $x\,\mathcal{R}_I\,x$.

⊛ *Symétrie :*

Soient $x,y\in A$ tels que $x\,\mathcal{R}_I\,y$, c'est-à-dire $x-y\in I$.

Comme I est un sous-groupe de $(A,+)$:

$$-(x-y)\in I$$

Donc $y-x\in I$, ce qui signifie que $y\,\mathcal{R}_I\,x$.

⊛ *Transitivité :*

Soient $x,y,z\in A$ tels que $x\,\mathcal{R}_I\,y$ et $y\,\mathcal{R}_I\,z$.

On a $x-y\in I$ et $y-z\in I$.

Comme I est un sous-groupe de $(A,+)$:

$$(x-y)+(y-z)\in I$$

Donc $x-z\in I$, ce qui signifie que $x\,\mathcal{R}_I\,z$.

Ainsi, $\mathcal{R}_I$ est une relation d'équivalence sur A.

② **Classes d'équivalence.**

Pour $a\in A$, on notera $\overline{a}$ sa classe d'équivalence pour $\mathcal{R}_I$:

$$\begin{aligned}\overline{a} &= \{b\in A \mid b\,\mathcal{R}_I\,a\}\\ &= \{b\in A \mid b-a\in I\}\\ &= \{a+i \mid i\in I\}\\ &= a+I\end{aligned}$$

③ **Construction de l'anneau quotient $B=A/I$.**

Soit $B=\dfrac{A}{I}=\{\overline{a}\;\big|\;a\in A\}$.

Pour $(x,y) \in B^2$, avec $x = \overline{a}$ et $y = \overline{a'}$ (où $a, a' \in A$), définissons :

$$x + y = \overline{a + a'}$$
$$x \cdot y = \overline{a \cdot a'}$$

④ **Les opérations sont bien définies.**

⊛ *Pour l'addition :*

Soient $x = \overline{a} = \overline{a'}$ et $y = \overline{b} = \overline{b'}$.

On a $a \mathcal{R}_I a'$, donc $a - a' \in I$. De même, $b - b' \in I$.

Alors :

$$(a+b) - (a'+b') = (a-a') + (b-b') \in I \quad \text{car } I \text{ est un sous-groupe de } (A,+)$$

Donc $a + b \mathcal{R}_I a' + b'$, ce qui signifie que $\overline{a+b} = \overline{a'+b'}$.

Ainsi, $x + y$ est bien définie.

⊛ *Pour la multiplication :*

On a :

$$\begin{aligned} a \cdot b - a' \cdot b' &= a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' \\ &= \underbrace{(a-a') \cdot b}_{\in I} + \underbrace{a' \cdot (b-b')}_{\in I} \end{aligned}$$

où :

★ $(a-a') \cdot b \in I$ car I est un idéal à droite et $a - a' \in I$;

★ $a' \cdot (b-b') \in I$ car I est un idéal à gauche et $b - b' \in I$.

Donc $a \cdot b - a' \cdot b' \in I$, ce qui signifie que $a \cdot b \mathcal{R}_I a' \cdot b'$.

Ainsi, $\overline{a \cdot b} = \overline{a' \cdot b'}$, et $x \cdot y$ est bien définie.

⑤ B **est un anneau (anneau quotient de** A **par** I**).**

⊛ *Associativité de* $+_B$ *:*

Soient $(x,y,z) \in B^3$ avec $x = \overline{a}$, $y = \overline{a'}$ et $z = \overline{a''}$.

$$\begin{aligned} (x+y)+z &= \left(\overline{a} + \overline{a'}\right) + \overline{a''} \\ &= \overline{a+a'} + \overline{a''} \\ &= \overline{(a+a')+a''} \\ &= \overline{a+(a'+a'')} && \text{car } +_A \text{ est associative} \\ &= \overline{a} + \overline{a'+a''} \\ &= \overline{a} + \left(\overline{a'} + \overline{a''}\right) \\ &= x + (y+z) \end{aligned}$$

Donc $+_B$ est associative : B satisfait (A_1).

⊛ *Commutativité de* $+_B$ *:*

Soient $x = \overline{a}$ et $y = \overline{b}$ dans B.

$$\begin{aligned} x + y &= \overline{a} + \overline{b} \\ &= \overline{a + b} \\ &= \overline{b + a} && \text{car } +_A \text{ est commutative} \\ &= \overline{b} + \overline{a} \\ &= y + x \end{aligned}$$

Donc B satisfait (A_4).

⊛ *Associativité de $\cdot_B$:*

Soient $x = \overline{a}$, $y = \overline{b}$ et $z = \overline{c}$ dans B.

$$\begin{aligned} (x \cdot y) \cdot z &= \left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} \\ &= \overline{a \cdot b} \cdot \overline{c} \\ &= \overline{(a \cdot b) \cdot c} \\ &= \overline{a \cdot (b \cdot c)} && \text{car } \cdot_A \text{ est associative} \\ &= \overline{a} \cdot \overline{b \cdot c} \\ &= \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right) \\ &= x \cdot (y \cdot z) \end{aligned}$$

Donc B satisfait (A_5).

⊛ *Distributivité de $\cdot_B$ sur $+_B$:*

Soient $x = \overline{a}$, $y = \overline{b}$ et $z = \overline{c}$ dans B.

$$\begin{aligned} x \cdot (y + z) &= \overline{a} \cdot \left(\overline{b} + \overline{c}\right) \\ &= \overline{a} \cdot \overline{b + c} \\ &= \overline{a \cdot (b + c)} \\ &= \overline{a \cdot b + a \cdot c} && \text{par distributivité dans } A \\ &= \overline{a \cdot b} + \overline{a \cdot c} \\ &= \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c} \\ &= x \cdot y + x \cdot z \end{aligned}$$

De même pour l'autre distributivité. Donc B satisfait (A_6) et (A_7).

⊛ *Élément neutre pour $+_B$:*

Soit $b \in B$ avec $b = \overline{a}$ (où $a \in A$).

$$\begin{aligned} \overline{0_A} + b &= \overline{0_A} + \overline{a} \\ &= \overline{0_A + a} \\ &= \overline{a} \\ &= b \end{aligned}$$

De même, $b + \overline{0_A} = b$.

Il existe donc $0_B = \overline{0_A}$ et B satisfait (A_2).

⊛ *Opposé :*

Soit $b = \overline{a} \in B$. Posons $b' = \overline{-a}$.

Alors :

$$\begin{aligned} b + b' &= \overline{a} + \overline{-a} \\ &= \overline{a + (-a)} \\ &= \overline{0_A} \\ &= 0_B \end{aligned}$$

De même, $b' + b = 0_B$.

Donc B satisfait (A_3) avec $b' = \overline{-a}$.

⑥ **Construction du morphisme φ.**

Soit $\varphi = \pi_{A,I} : A \longrightarrow \dfrac{A}{I}$ définie par :

$$a \longmapsto \overline{a}$$

⊛ *φ est un morphisme d'anneaux :*

Pour tous $a, a' \in A$:

$$\begin{aligned} \varphi\left(a + a'\right) &= \overline{a + a'} \\ &= \overline{a} + \overline{a'} \\ &= \varphi(a) + \varphi\left(a'\right) \end{aligned}$$

et :

$$\begin{aligned} \varphi\left(a \cdot a'\right) &= \overline{a \cdot a'} \\ &= \overline{a} \cdot \overline{a'} \\ &= \varphi(a) \cdot \varphi\left(a'\right) \end{aligned}$$

Donc φ est un morphisme d'anneaux.

⊛ *Calcul du noyau :*

$$\begin{aligned} a \in \mathrm{Ker}\left(\varphi\right) &\Longleftrightarrow \varphi(a) = 0_B \\ &\Longleftrightarrow \overline{a} = \overline{0_A} \\ &\Longleftrightarrow a \,\mathcal{R}_I\, 0_A \\ &\Longleftrightarrow a - 0_A \in I \\ &\Longleftrightarrow a \in I \end{aligned}$$

Donc $\mathrm{Ker}\left(\varphi\right) = I$.

Finalement, la projection canonique :

$$\begin{aligned} \pi_{A,I} \colon A &\longrightarrow \frac{A}{I} \\ a &\longmapsto \overline{a} \end{aligned}$$

est un morphisme d'anneaux de noyau I.

Propriété 2.8 : (*Anneau quotient commutatif*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau commutatif et I un idéal bilatère de A.

Alors l'anneau quotient A/I est commutatif.

Preuve :

Soient $\overline{x}, \overline{y} \in A/I$.

Par définition de la multiplication dans A/I :

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Comme A est commutatif, on a $x \cdot y = y \cdot x$. Donc :

$$\begin{aligned} \overline{x \cdot y} &= \overline{y \cdot x} \\ &= \overline{y} \cdot \overline{x} \end{aligned}$$

Ainsi, $\overline{x} \cdot \overline{y} = \overline{y} \cdot \overline{x}$ pour tous $\overline{x}, \overline{y} \in A/I$.

Finalement, A/I est commutatif.

Propriété 2.9 : (*Anneau quotient unitaire*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau unitaire et I un idéal bilatère de A.

Alors l'anneau quotient A/I est unitaire et :

$$1_{A/I} = \overline{1_A}$$

Preuve :

Soit $\overline{a} \in A/I$.

Par définition de la multiplication dans A/I :

$$\begin{aligned} \overline{1_A} \cdot \overline{a} &= \overline{1_A \cdot a} \\ &= \overline{a} \end{aligned}$$

et :

$$\begin{aligned} \overline{a} \cdot \overline{1_A} &= \overline{a \cdot 1_A} \\ &= \overline{a} \end{aligned}$$

Donc $\overline{1_A}$ est l'élément neutre pour la multiplication dans A/I.

Finalement, A/I est unitaire et $1_{A/I} = \overline{1_A}$.

Définition 2.10 : (*Isomorphisme d'anneaux*)

Soient $(A\,;+\,;\cdot)$ et $(B\,;+\,;\cdot)$ deux anneaux.

On appelle ***isomorphisme*** entre A et B un morphisme bijectif $\varphi\colon A\longrightarrow B$.

Propriété 2.11 : (*Réciproque d'un isomorphisme*)

Soient $(A\,;+\,;\cdot)$ et $(B\,;+\,;\cdot)$ deux anneaux et $\varphi\colon A\longrightarrow B$ un isomorphisme.

Alors $\varphi^{-1}\colon B\longrightarrow A$ est un isomorphisme.

Preuve :

Soient $b, b'\in B$.

Puisque φ est un morphisme :

$$\begin{aligned}\varphi\left(\varphi^{-1}(b)\cdot\varphi^{-1}\left(b'\right)\right)&=\varphi\left(\varphi^{-1}(b)\right)\cdot\varphi\left(\varphi^{-1}\left(b'\right)\right)\\&=b\cdot b'\end{aligned}$$

En appliquant φ^{-1} aux deux membres :

$$\varphi^{-1}(b)\cdot\varphi^{-1}\left(b'\right)=\varphi^{-1}\left(b\cdot b'\right)$$

De même pour l'addition :

$$\varphi^{-1}\left(b+b'\right)=\varphi^{-1}(b)+\varphi^{-1}\left(b'\right)$$

Ainsi, φ^{-1} est un morphisme. Comme φ^{-1} est bijective (réciproque d'une bijection), φ^{-1} est un isomorphisme.

Définition 2.12 : (*Anneaux isomorphes*)

Soient $(A\,;+\,;\cdot)$ et $(B\,;+\,;\cdot)$ deux anneaux.

On dit que A et B sont ***isomorphes***, et on note $A\simeq B$, s'il existe un isomorphisme $\varphi\colon A\longrightarrow B$.

Propriété 2.13 : (*Relation d'équivalence d'isomorphisme*)

La relation d'isomorphisme $\simeq$ est une relation d'équivalence sur l'ensemble des anneaux.

Preuve :

Démontrons que la relation $\simeq$ est une relation d'équivalence en vérifiant les trois propriétés suivantes.

- *Réflexivité :*

  L'application identité $\mathrm{id}_A\colon A\longrightarrow A$ est un isomorphisme.

  Donc $A\simeq A$.

  Donc $\simeq$ est réflexive.

- *Symétrie :*

  Si $A\simeq B$, il existe un isomorphisme $\varphi\colon A\longrightarrow B$. D'après la proposition précédente, $\varphi^{-1}\colon B\longrightarrow A$ est un isomorphisme.

  Donc $B\simeq A$.

  Donc $\simeq$ est symétrique.

- *Transitivité :*

  Soient A, B et C trois anneaux tels que $A\simeq B$ et $B\simeq C$.

  Il existe donc un isomorphisme $\varphi\colon A\longrightarrow B$ et un isomorphisme $\psi\colon B\longrightarrow C$.

La composée $\psi \circ \varphi : A \longrightarrow C$ est un morphisme d'anneaux (composée de deux morphismes) et est bijective (composée de deux bijections).

Donc $\psi \circ \varphi$ est un isomorphisme, ce qui signifie que $A \simeq C$.

Donc $\simeq$ est transitive.

Finalement, $\simeq$ est une relation d'équivalence.

Théorème 2.14 : (*Premier théorème d'isomorphisme*)

Soient $(A\,;+\,;\cdot)$ et $(B\,;+\,;\cdot)$ deux anneaux et $\varphi : A \longrightarrow B$ un morphisme d'anneaux.

Alors :

$$\frac{A}{\operatorname{Ker}\varphi} \simeq \operatorname{Im}\varphi$$

Preuve :

Soit $x \in \dfrac{A}{\operatorname{Ker}\varphi}$, donc $x = \overline{a}$ (avec $a \in A$).
Définissons $\theta(x) = \varphi(a) \in \operatorname{Im}\varphi$.

- θ **est bien définie :**

  Soient $x = \overline{a} = \overline{a'}$.

  Alors $\overline{a} = \overline{a'} \iff a \,\mathcal{R}_{\operatorname{Ker}\varphi}\, a'$.

  Donc $a - a' \in \operatorname{Ker}\varphi$.

  Ainsi :

$$\begin{aligned}\varphi(a-a') &= 0_B \\ &= \varphi(a) - \varphi(a')\end{aligned}$$

  Donc $\varphi(a) = \varphi(a')$.

  Ainsi, $\theta : \dfrac{A}{\operatorname{Ker}\varphi} \longrightarrow \operatorname{Im}\varphi$ est bien définie.

- θ **est un morphisme d'anneaux :**

  Soit $(x,y) \in \left(\dfrac{A}{\operatorname{Ker}\varphi}\right)^2$ avec $x = \overline{a}$ et $y = \overline{a'}$.

$$\begin{aligned}\theta(x+y) &= \theta\left(\overline{a} + \overline{a'}\right) \\ &= \theta\left(\overline{a+a'}\right) \\ &= \varphi\left(a+a'\right) \\ &= \varphi(a) + \varphi\left(a'\right) \\ &= \theta(x) + \theta\left(y\right)\end{aligned}$$

  et :

$$\begin{aligned}\theta(x\cdot y) &= \theta\left(\overline{a} \cdot \overline{a'}\right) \\ &= \theta\left(\overline{a\cdot a'}\right) \\ &= \varphi\left(a\cdot a'\right) \\ &= \varphi(a) \cdot \varphi\left(a'\right)\end{aligned}$$

$$= \theta(x) \cdot \theta(y)$$

⊛ **θ est injective :**

Soient $(x, y) \in \left(\dfrac{A}{\operatorname{Ker}\varphi}\right)^2$ tels que $\theta(x) = \theta(y)$.

Avec $x = \overline{a}$ et $y = \overline{a'}$, on a :

$$\begin{aligned}\varphi(a) &= \theta(x)\\ &= \theta(y)\\ &= \varphi(a')\end{aligned}$$

Donc :

$$\begin{aligned}\varphi(a) - \varphi(a') &= 0_B\\ \varphi(a - a') &= 0_B\end{aligned}$$

Ainsi, $a - a' \in \operatorname{Ker}\varphi$, donc $a \mathcal{R}_{\operatorname{Ker}\varphi} a'$.

Finalement :

$$x = \overline{a} = \overline{a'} = y$$

Donc $x = y$ et θ est injective.

⊛ **θ est surjective :**

Soit $x \in \operatorname{Im}\varphi$.

Il existe $a \in A$ tel que $x = \varphi(a)$.

Alors $x = \theta(\overline{a})$.

Ainsi, θ est un isomorphisme et :

$$\frac{A}{\operatorname{Ker}\varphi} \simeq \operatorname{Im}\varphi$$

Théorème 2.15 : (*Théorème de correspondance*)

Soit $(A\,;\,+\,;\,\cdot)$ un anneau et I un idéal bilatère de A.

Les idéaux bilatères de $\dfrac{A}{I}$ sont les $\dfrac{J}{I}$, pour J idéal bilatère de A tel que $I \subset J$, où :

$$\frac{J}{I} = \left\{\overline{j} \;\middle|\; j \in J\right\} = \pi_{A,I}(J)$$

De plus, on a :

$$\frac{\dfrac{A}{I}}{\dfrac{J}{I}} \simeq \frac{A}{J}$$

Preuve :

① **$\frac{J}{I}$ est un idéal de $\frac{A}{I}$.**

Soit J un idéal bilatère de A contenant I.

Montrons que $\frac{J}{I} = \left\{\overline{j} \;\middle|\; j \in J\right\}$ est un idéal bilatère de $\frac{A}{I}$.

⊛ *Sous-groupe additif :*

Puisque J est un idéal de A, on a $0_A \in J$, donc $\overline{0_A} = 0_{A/I} \in \frac{J}{I}$.

Soient $x, y \in \frac{J}{I}$. Il existe $j, j' \in J$ tels que $x = \overline{j}$ et $y = \overline{j'}$.

Alors :

$$x - y = \overline{j} - \overline{j'} = \overline{j - j'}$$

Comme J est un sous-groupe de A, on a $j - j' \in J$, donc $x - y \in \frac{J}{I}$.

⊛ *Stabilité par multiplication :*

Soit $x \in \frac{J}{I}$ et $a \in \frac{A}{I}$.

Il existe $j \in J$ et $a' \in A$ tels que $x = \overline{j}$ et $a = \overline{a'}$.

Alors :

$$a \cdot x = \overline{a'} \cdot \overline{j} = \overline{a' \cdot j}$$

Comme J est un idéal à gauche de A et $j \in J$, on a $a' \cdot j \in J$.

Donc $a \cdot x \in \frac{J}{I}$.

De même :

$$x \cdot a = \overline{j} \cdot \overline{a'} = \overline{j \cdot a'}$$

Comme J est un idéal à droite de A et $j \in J$, on a $j \cdot a' \in J$.

Donc $x \cdot a \in \frac{J}{I}$.

Finalement, $\frac{J}{I}$ est un idéal bilatère de $\frac{A}{I}$.

② **Tout idéal de $\frac{A}{I}$ est de la forme $\frac{J}{I}$.**

Soit T un idéal de $\frac{A}{I}$.

Posons $J = \pi_{A,I}^{-1}(T) = \left\{x \in A \;\middle|\; \pi_{A,I}(x) \in T\right\} = \left\{x \in A \;\middle|\; \overline{x} \in T\right\}$.

⊛ *J est un idéal de A :*

Puisque T est un idéal de $\frac{A}{I}$, on a $0_{A/I} = \overline{0_A} \in T$, donc $0_A \in J$.

Soient $(x, x') \in J^2$. Alors $\overline{x} \in T$ et $\overline{x'} \in T$.

On a :

$$\overline{x} + \overline{x'} = \overline{x + x'} \in T$$

Donc $x + x' \in J$.

Soit $x \in J$ et $a \in A$. Alors $\overline{x} \in T$ et $\overline{a} \in \frac{A}{I}$.

Puisque T est un idéal de $\dfrac{A}{I}$:

$$\overline{a}\cdot\overline{x}=\overline{a\cdot x}\in T$$

Donc $a\cdot x\in J$.

De même, $\overline{x}\cdot\overline{a}=\overline{x\cdot a}\in T$, donc $x\cdot a\in J$.

Ainsi, J est un idéal bilatère de A.

⊛ *$I\subset J$:*

Soit $i\in I$. Alors $\overline{i}=\overline{0_A}=0_{A/I}\in T$ (car T est un idéal).

Donc $i\in J$.

Ainsi, $I\subset J$.

⊛ *$T=\dfrac{J}{I}$:*

★ **Inclusion $\dfrac{J}{I}\subset T$:**

Soit $x\in\dfrac{J}{I}$. Alors $x=\overline{j}$ avec $j\in J$.

Par définition de J, on a $\overline{j}\in T$, donc $x\in T$.

★ **Inclusion $T\subset\dfrac{J}{I}$:**

Soit $b\in T$.

Il existe $a\in A$ tel que $b=\overline{a}$.

Puisque $\overline{a}\in T$, on a $a\in J$ par définition de J.

Donc $b=\overline{a}\in\dfrac{J}{I}$.

Finalement, $T=\dfrac{J}{I}$.

③ **Isomorphisme $\dfrac{A/I}{J/I}\simeq\dfrac{A}{J}$.**

Soit $\psi:\dfrac{A}{I}\longrightarrow\dfrac{A}{J}$ définie par $\overline{a}^I\longmapsto\overline{a}^J$.

⊛ *ψ est bien définie :*

Soient $a,a'\in A$ tels que $\overline{a}^I=\overline{a'}^I$.

Alors $a-a'\in I$.

Comme $I\subset J$, on a $a-a'\in J$, donc $\overline{a}^J=\overline{a'}^J$.

Ainsi, ψ est bien définie.

⊛ *ψ est un morphisme d'anneaux :*

Soient $x=\overline{a}^I$ et $y=\overline{a'}^I$ dans $\dfrac{A}{I}$.

$$\begin{aligned}\psi(x+y)&=\psi\left(\overline{a}^I+\overline{a'}^I\right)\\&=\psi\left(\overline{a+a'}^I\right)\\&=\overline{a+a'}^J\\&=\overline{a}^J+\overline{a'}^J\\&=\psi(x)+\psi(y)\end{aligned}$$

et :

$$\begin{aligned}\psi(x\cdot y) &= \psi\left(\overline{a}^I\cdot\overline{a'}^I\right)\\ &= \psi\left(\overline{a\cdot a'}^I\right)\\ &= \overline{a\cdot a'}^J\\ &= \overline{a}^J\cdot\overline{a'}^J\\ &= \psi(x)\cdot\psi(y)\end{aligned}$$

⊛ $\ker\psi = \dfrac{J}{I}$:

$$\begin{aligned}x\in\ker\psi &\iff \psi(x) = 0_{A/J}\\ &\iff \psi\left(\overline{a}^I\right) = \overline{0_A}^J\\ &\iff \overline{a}^J = \overline{0_A}^J\\ &\iff a\in J\\ &\iff \overline{a}^I\in\frac{J}{I}\\ &\iff x\in\frac{J}{I}\end{aligned}$$

⊛ *ψ est surjective :*

Soit $y\in\dfrac{A}{J}$.

Il existe $a\in A$ tel que $y=\overline{a}^J$.

Alors $y=\psi\left(\overline{a}^I\right)$.

Donc ψ est surjective.

D'après le premier théorème d'isomorphisme :

$$\frac{\frac{A}{I}}{\ker\psi}\simeq\operatorname{Im}\psi=\frac{A}{J}$$

Or $\ker\psi=\dfrac{J}{I}$, donc :

$$\frac{\frac{A}{I}}{\frac{J}{I}}\simeq\frac{A}{J}$$

Chapitre 3

Opérations sur les idéaux et Fonction d'Euler

Définition 3.1 : (*Somme d'idéaux*)

Soit A un anneau commutatif et I, J deux idéaux de A.

On appelle ***somme*** de I et J l'ensemble :

$$I+J=\{i+j \mid i\in I,\ j\in J\}$$

Propriété 3.2 : (*Plus petit idéal contenant I et J*)

Soit A un anneau commutatif et I, J deux idéaux de A.

$I+J$ est un idéal de A.

De plus, c'est le plus petit idéal de A contenant à la fois I et J.

Preuve :

① **$I+J$ est un idéal de A.**

⊛ *$I+J$ est un sous-groupe de $(A,+)$.*

★ Comme I et J sont des idéaux, on a $0\in I$ et $0\in J$. Donc :

$$0=0+0\in I+J$$

Ainsi, $I+J\neq\emptyset$.

★ Soient $x,y\in I+J$. Il existe $i,i'\in I$ et $j,j'\in J$ tels que $x=i+j$ et $y=i'+j'$.

Alors :

$$\begin{aligned}x-y&=(i+j)-(i'+j')\\&=(i-i')+(j-j')\end{aligned}$$

Comme I est un idéal (donc un sous-groupe), on a $i-i'\in I$. Comme J est un idéal (donc un sous-groupe), on a $j-j'\in J$.

Donc $x-y\in I+J$.

Ainsi, $I+J$ est un sous-groupe de $(A,+)$.

⊛ *Stabilité par multiplication par un élément de A.*

Soit $x\in I+J$ et $a\in A$.

Il existe $i\in I$ et $j\in J$ tels que $x=i+j$.

Alors :

$$\begin{aligned}a\cdot x&=a\cdot(i+j)\\&=a\cdot i+a\cdot j&&\text{par distributivité dans } A\end{aligned}$$

Comme I est un idéal et $i\in I$, on a $a\cdot i\in I$. Comme J est un idéal et $j\in J$, on a $a\cdot j\in J$.

Donc $a\cdot x\in I+J$.

Finalement, $I+J$ est un idéal de A.

② **$I+J$ contient I et J.**

Soit $i \in I$. Comme J est un idéal, on a $0 \in J$. Donc :

$$i = i + 0 \in I + J$$

Ainsi, $I \subset I+J$. De même, $J \subset I+J$.

③ **$I+J$ est le plus petit idéal contenant I et J.**

Soit K un idéal de A tel que $I \subset K$ et $J \subset K$.

Soit $x \in I+J$. Il existe $i \in I$ et $j \in J$ tels que $x = i+j$.

Comme $I \subset K$, on a $i \in K$. Comme $J \subset K$, on a $j \in K$.

Puisque K est un idéal (donc un sous-groupe pour $+$), on a :

$$x = \underbrace{i}_{\in K} + \underbrace{j}_{\in K} \in K$$

Ainsi, $I+J \subset K$.

Finalement, $I+J$ est le plus petit idéal de A contenant à la fois I et J.

Définition 3.3 : (*Produit d'idéaux*)

Soit A un anneau commutatif et I, J deux idéaux de A.

On appelle ***produit*** de I et J l'ensemble :

$$I \cdot J = \left\{ \sum_{k=1}^{m} i_k \cdot j_k \;\middle|\; m \in \mathbb{N},\ i_k \in I,\ j_k \in J \right\}$$

Propriété 3.4 : (*Inclusion du produit dans l'intersection*)

Soit A un anneau commutatif et I, J deux idéaux de A.

$I \cdot J$ est un idéal de A et on a l'inclusion :

$$I \cdot J \subset I \cap J$$

Preuve :

① **$I \cdot J$ est un idéal de A.**

⊛ *$I \cdot J$ est un sous-groupe de $(A,+)$.*

★ Pour $m = 0$, la somme vide est égale à 0. Donc $0 \in I \cdot J$.

★ Soient $x, y \in I \cdot J$. Il existe $m, n \in \mathbb{N}$, $i_k \in I$, $j_k \in J$ (pour $k \in [\![1,m]\!]$) et $i'_\ell \in I$, $j'_\ell \in J$ (pour $\ell \in [\![1,n]\!]$) tels que :

$$x = \sum_{k=1}^{m} i_k \cdot j_k$$
$$y = \sum_{\ell=1}^{n} i'_\ell \cdot j'_\ell$$

Alors :

$$\begin{aligned} x - y &= \sum_{k=1}^{m} i_k \cdot j_k - \sum_{\ell=1}^{n} i'_\ell \cdot j'_\ell \\ &= \sum_{k=1}^{m} i_k \cdot j_k + \sum_{\ell=1}^{n} (-i'_\ell) \cdot j'_\ell \end{aligned}$$

Comme I est un idéal et $i'_\ell \in I$, on a $-i'_\ell \in I$.

Donc $x-y$ est une somme finie de produits d'éléments de I par des éléments de J, ce qui signifie que $x-y \in I \cdot J$.

Ainsi, $I \cdot J$ est un sous-groupe de $(A,+)$.

⊛ *Stabilité par multiplication par un élément de A.*

Soit $x \in I \cdot J$ et $a \in A$.

Il existe $m \in \mathbb{N}$, $i_k \in I$ et $j_k \in J$ tels que :

$$x = \sum_{k=1}^{m} i_k \cdot j_k$$

Alors :

$$\begin{aligned} a \cdot x &= a \cdot \left(\sum_{k=1}^{m} i_k \cdot j_k \right) \\ &= \sum_{k=1}^{m} a \cdot (i_k \cdot j_k) && \text{par distributivité} \\ &= \sum_{k=1}^{m} (a \cdot i_k) \cdot j_k && \text{par associativité} \end{aligned}$$

Comme I est un idéal et $i_k \in I$, on a $a \cdot i_k \in I$.

Donc $a \cdot x \in I \cdot J$.

Finalement, $I \cdot J$ est un idéal de A.

② **Inclusion $I \cdot J \subset I \cap J$.**

Soit $x \in I \cdot J$. Il existe $m \in \mathbb{N}$, $i_k \in I$ et $j_k \in J$ tels que :

$$x = \sum_{k=1}^{m} i_k \cdot j_k$$

Pour tout $k \in [\![1, m]\!]$:

⊛ Comme $i_k \in I$ et $j_k \in J \subset A$, on a $i_k \cdot j_k \in I$ (car I est un idéal de A).

⊛ Comme $j_k \in J$ et $i_k \in I \subset A$, on a $i_k \cdot j_k \in J$ (car J est un idéal de A).

Ainsi, pour tout k, $i_k \cdot j_k \in I$ et $i_k \cdot j_k \in J$.

Par stabilité de I et J pour l'addition :

$$x = \sum_{k=1}^{m} i_k \cdot j_k \in I \quad \text{et} \quad x = \sum_{k=1}^{m} i_k \cdot j_k \in J$$

Donc $x \in I \cap J$.

Finalement, $I \cdot J$ est un idéal de A et $I \cdot J \subset I \cap J$.

Exemple :

Soit $A = \mathbb{Z}$ et $I = J = 2\mathbb{Z}$.

On a :

$$I \cap J = 2\mathbb{Z} \quad \text{et} \quad I \cdot J = 4\mathbb{Z}$$

Donc $I \cdot J \subsetneq I \cap J$.

L'inclusion de la proposition 3.4 est en général stricte.

Définition 3.5 : (*Idéaux étrangers*)

Soit A un anneau commutatif unitaire et I, J deux idéaux de A.

On dit que I et J sont ***étrangers*** si :

$$I + J = A$$

Théorème 3.6 : (*Théorème des Restes Chinois*)

Soit A un anneau commutatif unitaire et I, J deux idéaux étrangers de A.

Alors :

① $I \cdot J = I \cap J$

② $\dfrac{A}{I \cap J} \simeq \dfrac{A}{I} \times \dfrac{A}{J}$

Preuve :

① **Démontrons que $I \cdot J = I \cap J$.**

⊛ *Inclusion $I \cdot J \subset I \cap J$:*

D'après la proposition 3.4, on a déjà $I \cdot J \subset I \cap J$.

⊛ *Inclusion $I \cap J \subset I \cdot J$:*

Puisque I et J sont étrangers, on a $I + J = A$.

En particulier, $1_A \in A = I + J$. Il existe donc $i_0 \in I$ et $j_0 \in J$ tels que :

$$1_A = i_0 + j_0$$

Soit $x \in I \cap J$. Alors $x \in I$ et $x \in J$.

On peut écrire :

$$\begin{aligned} x &= x \cdot 1_A \\ &= x \cdot (i_0 + j_0) \\ &= x \cdot i_0 + x \cdot j_0 \end{aligned}$$

Or :

★ $x \in J$ et $i_0 \in I$, donc $x \cdot i_0 \in I \cdot J$;

★ $x \in I$ et $j_0 \in J$, donc $x \cdot j_0 \in I \cdot J$.

Comme $I \cdot J$ est un idéal (donc stable par addition), on a :

$$x = x \cdot i_0 + x \cdot j_0 \in I \cdot J$$

Ainsi, $I \cap J \subset I \cdot J$.

Finalement, $I \cdot J = I \cap J$.

② **Démontrons que $\dfrac{A}{I \cap J} \simeq \dfrac{A}{I} \times \dfrac{A}{J}$.**

Soit $\varphi : A \longrightarrow \dfrac{A}{I} \times \dfrac{A}{J}$ définie par :

$$a \longmapsto \left(\overline{a}^I \, ; \, \overline{a}^J\right)$$

où $\overline{a}^I = \pi_{A,I}(a)$ et $\overline{a}^J = \pi_{A,J}(a)$.

⊛ *φ est un morphisme d'anneaux :*

Soient $a, a' \in A$.

Pour l'addition :

$$\begin{aligned}\varphi(a+a') &= \left(\overline{a+a'}^I \,;\, \overline{a+a'}^J\right)\\ &= \left(\overline{a}^I + \overline{a'}^I \,;\, \overline{a}^J + \overline{a'}^J\right)\\ &= \left(\overline{a}^I \,;\, \overline{a}^J\right) + \left(\overline{a'}^I \,;\, \overline{a'}^J\right)\\ &= \varphi(a) + \varphi(a')\end{aligned}$$

Pour la multiplication :

$$\begin{aligned}\varphi(a\cdot a') &= \left(\overline{a\cdot a'}^I \,;\, \overline{a\cdot a'}^J\right)\\ &= \left(\overline{a}^I \cdot \overline{a'}^I \,;\, \overline{a}^J \cdot \overline{a'}^J\right)\\ &= \left(\overline{a}^I \,;\, \overline{a}^J\right)\cdot\left(\overline{a'}^I \,;\, \overline{a'}^J\right)\\ &= \varphi(a)\cdot\varphi(a')\end{aligned}$$

Donc φ est un morphisme d'anneaux.

⊛ *Calcul du noyau :*

$$\begin{aligned}a \in \mathrm{Ker}(\varphi) &\iff \varphi(a) = 0_{\frac{A}{I}\times\frac{A}{J}}\\ &\iff \left(\overline{a}^I \,;\, \overline{a}^J\right) = \left(0_{\frac{A}{I}} \,;\, 0_{\frac{A}{J}}\right)\\ &\iff \overline{a}^I = 0_{\frac{A}{I}} \quad \text{et} \quad \overline{a}^J = 0_{\frac{A}{J}}\\ &\iff a \in I \quad \text{et} \quad a \in J\\ &\iff a \in I \cap J\end{aligned}$$

Donc $\mathrm{Ker}(\varphi) = I \cap J$.

D'après le premier théorème d'isomorphisme :

$$\frac{A}{I\cap J} = \frac{A}{\mathrm{Ker}(\varphi)} \simeq \mathrm{Im}(\varphi)$$

Il reste donc à démontrer que φ est surjective.

⊛ *Surjectivité de φ :*

Soit $(u, v) \in \dfrac{A}{I} \times \dfrac{A}{J}$.

Il existe $a \in A$ et $a' \in A$ tels que :

$$u = \overline{a}^I \quad \text{et} \quad v = \overline{a'}^J$$

Posons $x = a\cdot j_0 + a'\cdot i_0$, où $i_0 \in I$ et $j_0 \in J$ sont tels que $i_0 + j_0 = 1_A$.

⊛ **Calcul de $\overline{x}^I$:**

$$a - x = a - a\cdot j_0 - a'\cdot i_0$$

$$= a\cdot(1_A - j_0) - a'\cdot i_0$$
$$= a\cdot i_0 - a'\cdot i_0 \qquad \text{car } 1_A - j_0 = i_0$$
$$= (a-a')\cdot i_0$$

Comme $i_0 \in I$ et I est un idéal, on a $(a-a')\cdot i_0 \in I$.

Donc $a - x \in I$, ce qui signifie que $\overline{x}^I = \overline{a}^I = u$.

⊛ **Calcul de $\overline{x}^J$:**

$$a' - x = a' - a\cdot j_0 - a'\cdot i_0$$
$$= a'\cdot(1_A - i_0) - a\cdot j_0$$
$$= a'\cdot j_0 - a\cdot j_0 \qquad \text{car } 1_A - i_0 = j_0$$
$$= (a'-a)\cdot j_0$$

Comme $j_0 \in J$ et J est un idéal, on a $(a'-a)\cdot j_0 \in J$.

Donc $a' - x \in J$, ce qui signifie que $\overline{x}^J = \overline{a'}^J = v$.

Ainsi :

$$\varphi(x) = \left(\overline{x}^I\,;\,\overline{x}^J\right) = (u\,;\,v)$$

Donc $(u,v) \in \mathrm{Im}(\varphi)$.

Finalement, $\mathrm{Im}(\varphi) = \dfrac{A}{I}\times\dfrac{A}{J}$, et φ est surjective.

D'après le premier théorème d'isomorphisme, on conclut que :

$$\frac{A}{I\cap J} \simeq \frac{A}{I}\times\frac{A}{J}$$

Exemple :

Cas particulier : $A = \mathbb{Z}$.

Soient $a \geqslant 1$ et $b \geqslant 1$ deux entiers premiers entre eux.

Posons $I = a\mathbb{Z}$ et $J = b\mathbb{Z}$.

Les idéaux I et J sont étrangers.

En effet, d'après le théorème de Bézout, il existe $(x,y) \in \mathbb{Z}^2$ tel que :

$$ax + by = 1$$

Or :

$$1 = \underbrace{ax}_{\in a\mathbb{Z}=I} + \underbrace{by}_{\in b\mathbb{Z}=J}$$

Donc $1 \in I + J$, ce qui implique $I + J = \mathbb{Z}$.

D'après le théorème des Restes Chinois (théorème 3.6) :

$$I\cap J = I\cdot J = a\mathbb{Z}\cdot b\mathbb{Z} = ab\mathbb{Z}$$

Donc :

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} = \frac{\mathbb{Z}}{I\cap J} \simeq \frac{\mathbb{Z}}{I}\times\frac{\mathbb{Z}}{J} = \frac{\mathbb{Z}}{a\mathbb{Z}}\times\frac{\mathbb{Z}}{b\mathbb{Z}}$$

$$a \geqslant 1,\ b \geqslant 1 \text{ premiers entre eux} \quad \Longrightarrow \quad \frac{\mathbb{Z}}{ab\mathbb{Z}} \simeq \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}} \text{ (isomorphisme d'anneaux)}$$

Corollaire 3.7 : (*Produit de groupes cycliques*)

Soient $a \geqslant 1$ et $b \geqslant 1$ deux entiers premiers entre eux.

Si A est un groupe cyclique d'ordre a et B est un groupe cyclique d'ordre b, alors $A \times B$ est cyclique d'ordre ab.

Preuve :

Puisque A est un groupe cyclique d'ordre a, on a l'isomorphisme de groupes :

$$A \underset{\text{(groupe)}}{\simeq} \left(\frac{\mathbb{Z}}{a\mathbb{Z}}\ ;\ +\right)$$

De même, puisque B est un groupe cyclique d'ordre b :

$$B \underset{\text{(groupe)}}{\simeq} \left(\frac{\mathbb{Z}}{b\mathbb{Z}}\ ;\ +\right)$$

Par produit cartésien :

$$A \times B \underset{\text{(groupe)}}{\simeq} \left(\frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}\ ;\ +\right)$$

D'après le théorème des Restes Chinois (théorème 3.6) :

$$\frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}} \simeq \frac{\mathbb{Z}}{ab\mathbb{Z}} \quad \text{(isomorphisme d'anneaux, donc de groupes)}$$

Finalement :

$$A \times B \underset{\text{(groupe)}}{\simeq} \left(\frac{\mathbb{Z}}{ab\mathbb{Z}}\ ;\ +\right)$$

qui est cyclique d'ordre ab.

Propriété 3.8 : (*Théorème des Restes Chinois généralisé*)

Soit A un anneau commutatif unitaire et $(I_i)_{i\in[\![1,m]\!]}$ une famille d'idéaux de A deux à deux étrangers (c'est-à-dire que pour tous $k \neq l$, on a $I_k + I_l = A$).

Alors :

$$\frac{A}{I_1 \cap \ldots \cap I_m} \simeq \frac{A}{I_1} \times \ldots \times \frac{A}{I_m}$$

Preuve :

Démontrons ce résultat par récurrence sur m.

Cas de base :

- Pour $m = 1$: le résultat est trivial.
- Pour $m = 2$: c'est exactement le théorème des Restes Chinois (théorème 3.6).

Hérédité : Supposons le résultat vrai pour un entier $m \geqslant 2$, et démontrons-le pour $m+1$.

Soit $(I_i)_{i\in[\![1,m+1]\!]}$ une famille d'idéaux de A deux à deux étrangers.

Par hypothèse de récurrence, on a :

$$\frac{A}{I_1 \cap \ldots \cap I_m} \simeq \frac{A}{I_1} \times \ldots \times \frac{A}{I_m}$$

Pour tout $k \in [\![1, m]\!]$, l'idéal I_{m+1} est étranger à I_k, c'est-à-dire :

$$I_k + I_{m+1} = A$$

Il existe donc $x_k \in I_k$ et $y_k \in I_{m+1}$ tels que :

$$1_A = x_k + y_k$$

Multiplions ces égalités pour $k = 1, \ldots, m$:

$$1_A = (x_1 + y_1) \cdot (x_2 + y_2) \cdots (x_m + y_m)$$

En développant ce produit, on obtient une somme de 2^m termes. Chaque terme est un produit de m facteurs, où chaque facteur est soit un x_k, soit un y_k.

Le seul terme qui ne contient aucun y_k est $x_1 \cdot x_2 \cdots x_m$.

Tous les autres termes contiennent au moins un facteur y_k pour un certain $k \in [\![1, m]\!]$. Comme $y_k \in I_{m+1}$ et I_{m+1} est un idéal, chacun de ces termes appartient à I_{m+1}.

On peut donc écrire :

$$1_A = \underbrace{x_1 \cdot x_2 \cdots x_m}_{\in I_1 \cap \ldots \cap I_m} + \underbrace{z}_{\in I_{m+1}}$$

où $z \in I_{m+1}$ est la somme de tous les termes contenant au moins un y_k.

De plus, pour tout $k \in [\![1, m]\!]$, on a $x_k \in I_k$, donc $x_1 \cdot x_2 \cdots x_m \in I_k$ (car I_k est un idéal). Ainsi :

$$x_1 \cdot x_2 \cdots x_m \in I_1 \cap \ldots \cap I_m$$

Par conséquent :

$$1_A \in (I_1 \cap \ldots \cap I_m) + I_{m+1}$$

ce qui implique :

$$A = (I_1 \cap \ldots \cap I_m) + I_{m+1}$$

Ainsi, les idéaux $I_1 \cap \ldots \cap I_m$ et I_{m+1} sont étrangers.

On peut alors appliquer le théorème des Restes Chinois (cas $m = 2$) aux deux idéaux $I_1 \cap \ldots \cap I_m$ et I_{m+1} :

$$\frac{A}{I_1 \cap \ldots \cap I_{m+1}} = \frac{A}{(I_1 \cap \ldots \cap I_m) \cap I_{m+1}} \simeq \frac{A}{I_1 \cap \ldots \cap I_m} \times \frac{A}{I_{m+1}}$$

Par hypothèse de récurrence :

$$\frac{A}{I_1 \cap \ldots \cap I_m} \simeq \frac{A}{I_1} \times \ldots \times \frac{A}{I_m}$$

Finalement :

$$\frac{A}{I_1 \cap \ldots \cap I_{m+1}} \simeq \frac{A}{I_1} \times \ldots \times \frac{A}{I_m} \times \frac{A}{I_{m+1}}$$

Ce qui achève la démonstration par récurrence.

Définition 3.9 : (*Groupe des unités d'un anneau*)

Soit A un anneau commutatif unitaire tel que $1_A \neq 0_A$.

On appelle ***groupe des unités*** de A (parfois noté $A^\times$) l'ensemble :

$$U(A) = \{a \in A \setminus \{0_A\} \mid \exists b \in A \setminus \{0_A\},\ a \cdot b = 1_A\}$$

Propriété 3.10 : (*Structure de groupe des unités*)

Soit A un anneau commutatif unitaire tel que $1_A \neq 0_A$.

$(U(A)\ ;\ \cdot)$ est un groupe d'élément neutre 1_A.

Preuve :

Vérifions les axiomes de groupe pour $(U(A)\ ;\ \cdot)$.

- *Loi de composition interne :*

  Soient $a, b \in U(A)$.

  Il existe $a', b' \in A \setminus \{0_A\}$ tels que $a \cdot a' = 1_A$ et $b \cdot b' = 1_A$.

  Alors :

$$\begin{aligned}(a \cdot b) \cdot (a' \cdot b') &= a \cdot (b \cdot a') \cdot b' \\ &= a \cdot (a' \cdot b) \cdot b' && \text{car } A \text{ est commutatif} \\ &= (a \cdot a') \cdot (b \cdot b') \\ &= 1_A \cdot 1_A \\ &= 1_A\end{aligned}$$

  De plus, $a' \cdot b' \neq 0_A$ (car A est commutatif et $a', b' \neq 0_A$... attention, cela suppose A intègre, sinon on utilise directement la définition).

  Donc $a \cdot b \in U(A)$.

- *Associativité :*

  L'associativité de $\cdot$ dans $U(A)$ est héritée de l'associativité de $\cdot$ dans A.

- *Élément neutre :*

  On a $1_A \cdot 1_A = 1_A$, donc $1_A \in U(A)$ (avec 1_A comme inverse de lui-même).

  De plus, pour tout $a \in U(A)$:

$$a \cdot 1_A = 1_A \cdot a = a$$

  Donc 1_A est l'élément neutre de $(U(A)\ ;\ \cdot)$.

- *Existence d'un inverse :*

  Soit $a \in U(A)$. Par définition, il existe $b \in A \setminus \{0_A\}$ tel que $a \cdot b = 1_A$.

  Comme A est commutatif, on a aussi $b \cdot a = 1_A$.

  Donc $b \in U(A)$ et b est l'inverse de a dans $(U(A)\ ;\ \cdot)$.

Finalement, $(U(A)\ ;\ \cdot)$ est un groupe d'élément neutre 1_A.

Exemple :

- Si A est un corps, alors $U(A) = A \setminus \{0\}$.
- $U(\mathbb{Z}) = \{-1; 1\}$.
- $U(K[x]) = K \setminus \{0\}$ (où K est un corps).

Propriété 3.11 : (*Groupe des unités d'un produit d'anneaux*)

Soient A et B deux anneaux commutatifs unitaires tels que $1_A \neq 0_A$ et $1_B \neq 0_B$.

On a :

$$U(A \times B) = U(A) \times U(B)$$

Preuve :

Soit $(a; b) \in A \times B$.

$(a; b) \in U(A \times B)$ si et seulement s'il existe $(a'; b') \in A \times B$ tel que :

$$(a; b) \cdot (a'; b') = (1_A; 1_B)$$

c'est-à-dire :

$$(a \cdot a'; b \cdot b') = (1_A; 1_B)$$

ce qui équivaut à :

$$a \cdot a' = 1_A \quad \text{et} \quad b \cdot b' = 1_B$$

Donc $a \in U(A)$ et $b \in U(B)$, soit $(a; b) \in U(A) \times U(B)$.

Propriété 3.12 : (*Isomorphisme des groupes des unités*)

Soient A et B deux anneaux commutatifs unitaires tels que $1_A \neq 0_A$ et $1_B \neq 0_B$.

Si $A \underset{\text{(anneau)}}{\simeq} B$, alors $U(A) \underset{\text{(groupe)}}{\simeq} U(B)$.

Preuve :

Soit $\varphi : A \longrightarrow B$ un isomorphisme d'anneaux.

- $\varphi(1_A) = 1_B$ **:**

  φ est bijectif, donc surjectif. Il existe $x \in A$ tel que $\varphi(x) = 1_B$.

  Alors :

$$\begin{aligned} \varphi(1_A) &= \varphi(1_A) \cdot 1_B \\ &= \varphi(1_A) \cdot \varphi(x) \\ &= \varphi(1_A \cdot x) \\ &= \varphi(x) \\ &= 1_B \end{aligned}$$

- φ **envoie** $U(A)$ **dans** $U(B)$ **:**

  Soit $a \in U(A)$. Il existe $a' \in A \setminus \{0_A\}$ tel que $a \cdot a' = 1_A$.

Alors :

$$\begin{aligned} 1_B &= \varphi(1_A) \\ &= \varphi\left(a \cdot a'\right) \\ &= \varphi(a) \cdot \varphi\left(a'\right) \end{aligned}$$

De plus, $\varphi\left(a'\right) \neq \varphi(0_A) = 0_B$ (car φ est injective).

Donc $\varphi(a) \in U(B)$.

Soit $\theta = \varphi|_{U(A)}$ la restriction de φ à $U(A)$:

$$\theta : U(A) \longrightarrow U(B)$$

θ est un morphisme de groupes.

Soit $\lambda = \varphi^{-1}|_{U(B)}$ la restriction de φ^{-1} à $U(B)$:

$$\lambda : U(B) \longrightarrow U(A)$$

λ est un morphisme de groupes.

Les morphismes λ et θ sont inverses l'un de l'autre.

Finalement, $U(A) \underset{\text{(groupe)}}{\simeq} U(B)$.

Définition 3.13 : (*Fonction indicatrice d'Euler*)

Soit $m \geqslant 1$ un entier.

On définit la ***fonction indicatrice d'Euler*** Φ par :

$$\Phi(m) = \left| U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right) \right|$$

Lemme 3.14 : (*Caractérisation de la fonction indicatrice d'Euler*)

Soit $m \geqslant 1$ un entier.

$\Phi(m)$ est le nombre d'entiers $k \in [\![1, m]\!]$ tels que $\text{PGCD}(k, m) = 1$.

Preuve :

On sait que :

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \{\overline{1} ; \ldots ; \overline{m}\}$$

Soit $k \in [\![1, m]\!]$.

$$\begin{aligned} \overline{k} \text{ est inversible dans } \frac{\mathbb{Z}}{m\mathbb{Z}} &\iff \exists x \in \mathbb{Z}, \quad \overline{k} \cdot \overline{x} = \overline{1} \\ &\iff \exists x \in \mathbb{Z}, \quad \overline{k \cdot x} = \overline{1} \\ &\iff \exists x \in \mathbb{Z}, \quad m \text{ divise } 1 - k \cdot x \\ &\iff \exists (x, y) \in \mathbb{Z}^2, \quad 1 - k \cdot x = m \cdot y \\ &\iff \exists (x, y) \in \mathbb{Z}^2, \quad k \cdot x + m \cdot y = 1 \\ &\iff \text{PGCD}(k, m) = 1 \end{aligned}$$

Pour la dernière équivalence :

- ⊛ Sens direct $\Rightarrow$: Si $k \cdot x + m \cdot y = 1$, alors tout diviseur commun à k et m divise également $k \cdot x + m \cdot y = 1$. Le seul diviseur

commun positif possible est donc 1, ce qui signifie que $\text{PGCD}(k,m)=1$.

⊛ Réciproque $\Leftarrow$: D'après le théorème de Bachet-Bézout, si $\text{PGCD}(k,m)=1$, alors il existe $(x,y)\in\mathbb{Z}^2$ tel que $k\cdot x+m\cdot y=1$.

Ainsi, $\overline{k}\in U\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$ si et seulement si $\text{PGCD}(k,m)=1$.

Par définition de $\Phi(m)=\left|U\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)\right|$, on en déduit que $\Phi(m)$ est bien le nombre d'entiers $k\in[\![1,m]\!]$ tels que $\text{PGCD}(k,m)=1$.

Exemple :

Calculons $\Phi(m)$ pour les premières valeurs de m en utilisant le lemme précédent :

$\Phi(m)$ est le nombre d'entiers $k\in[\![1,m]\!]$ tels que $\text{PGCD}(k,m)=1$.

$$\Phi(1)=1 \quad ; \quad \Phi(2)=1 \quad ; \quad \Phi(3)=2$$

$$\Phi(4)=2 \quad ; \quad \Phi(5)=4 \quad ; \quad \Phi(6)=2$$

$$\Phi(7)=6 \quad ; \quad \Phi(8)=4 \quad ; \quad \Phi(9)=6 \quad ; \quad \Phi(10)=4$$

⊛ $\Phi(1)=1$ **:**

Le seul entier dans $[\![1,1]\!]$ est 1.

$\text{PGCD}(1,1)=1$, donc 1 est premier avec 1.

Ainsi, $\Phi(1)=1$.

⊛ $\Phi(2)=1$ **:**

Les entiers dans $[\![1,2]\!]$ sont 1 et 2.

$\text{PGCD}(1,2)=1$ (premier avec 2) et $\text{PGCD}(2,2)=2\neq 1$.

Seul 1 est premier avec 2.

Ainsi, $\Phi(2)=1$.

⊛ $\Phi(3)=2$ **:**

Les entiers dans $[\![1,3]\!]$ sont 1, 2 et 3.

$\text{PGCD}(1,3)=1$, $\text{PGCD}(2,3)=1$ et $\text{PGCD}(3,3)=3\neq 1$.

Les entiers premiers avec 3 sont 1 et 2.

Ainsi, $\Phi(3)=2$.

⊛ $\Phi(4)=2$ **:**

Les entiers dans $[\![1,4]\!]$ sont 1, 2, 3 et 4.

$\text{PGCD}(1,4)=1$, $\text{PGCD}(2,4)=2\neq 1$, $\text{PGCD}(3,4)=1$ et $\text{PGCD}(4,4)=4\neq 1$.

Les entiers premiers avec 4 sont 1 et 3.

Ainsi, $\Phi(4)=2$.

⊛ $\Phi(5)=4$ **:**

Les entiers dans $[\![1,5]\!]$ sont 1, 2, 3, 4 et 5.

$\text{PGCD}(1,5)=1$, $\text{PGCD}(2,5)=1$, $\text{PGCD}(3,5)=1$, $\text{PGCD}(4,5)=1$ et $\text{PGCD}(5,5)=5\neq 1$.

Les entiers premiers avec 5 sont 1, 2, 3 et 4.

Ainsi, $\Phi(5)=4$.

⊛ $\Phi(6)=2$ **:**

Les entiers dans $[\![1,6]\!]$ sont 1, 2, 3, 4, 5 et 6.

PGCD(1,6) = 1, PGCD(2,6) = 2 ≠ 1, PGCD(3,6) = 3 ≠ 1, PGCD(4,6) = 2 ≠ 1, PGCD(5,6) = 1 et PGCD(6,6) = 6 ≠ 1.

Les entiers premiers avec 6 sont 1 et 5.

Ainsi, $\Phi(6) = 2$.

⊛ $\Phi(7) = 6$ **:**

7 est premier, donc tous les entiers de 1 à 6 sont premiers avec 7.

Ainsi, $\Phi(7) = 6$.

⊛ $\Phi(8) = 4$ **:**

Les entiers dans $[\![1,8]\!]$ premiers avec 8 (c'est-à-dire impairs) sont 1, 3, 5 et 7.

Ainsi, $\Phi(8) = 4$.

⊛ $\Phi(9) = 6$ **:**

Les entiers dans $[\![1,9]\!]$ premiers avec 9 (c'est-à-dire non multiples de 3) sont 1, 2, 4, 5, 7 et 8.

Ainsi, $\Phi(9) = 6$.

⊛ $\Phi(10) = 4$ **:**

Les entiers dans $[\![1,10]\!]$ premiers avec 10 (c'est-à-dire non multiples de 2 ni de 5) sont 1, 3, 7 et 9.

Ainsi, $\Phi(10) = 4$.

Théorème 3.15 : (*Multiplicativité de la fonction indicatrice d'Euler*)

Soient $n \geqslant 1$ et $m \geqslant 1$ deux entiers premiers entre eux.

Alors :

$$\Phi(nm) = \Phi(n) \cdot \Phi(m)$$

Preuve :

D'après le théorème des Restes Chinois (théorème 3.6), comme n et m sont premiers entre eux, on a l'isomorphisme d'anneaux :

$$\frac{\mathbb{Z}}{nm\mathbb{Z}} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

En appliquant le foncteur groupe des unités $U(\cdot)$ et d'après la propriété $U(A \times B) = U(A) \times U(B)$ (proposition 3.11) :

$$U\left(\frac{\mathbb{Z}}{nm\mathbb{Z}}\right) \simeq U\left(\frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}\right) = U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \times U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)$$

En prenant les cardinaux de ces ensembles finis :

$$\begin{aligned}
\Phi(nm) &= \left|U\left(\frac{\mathbb{Z}}{nm\mathbb{Z}}\right)\right| \\
&= \left|U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \times U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)\right| \\
&= \left|U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right| \cdot \left|U\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)\right| \\
&= \Phi(n)\Phi(m)
\end{aligned}$$

Lemme 3.16 : (*Fonction indicatrice d'Euler pour les puissances de nombres premiers*)

Soit p un nombre premier et $k \geqslant 1$ un entier.

Alors :

$$\Phi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Preuve :

D'après le lemme 3.14, on a :

$$\Phi\left(p^k\right) = \left|\left\{\ell \in [\![1, p^k]\!] \;\middle|\; \ell \text{ et } p^k \text{ premiers entre eux}\right\}\right|$$

Par complémentarité, on compte d'abord les entiers qui ne sont pas premiers avec p^k :

$$p^k - \Phi\left(p^k\right) = \left|\left\{\ell \in [\![1, p^k]\!] \;\middle|\; \ell \text{ et } p^k \text{ non premiers entre eux}\right\}\right|$$

Or, ℓ et p^k ne sont pas premiers entre eux si et seulement si $\text{PGCD}(\ell, p^k) > 1$.

Comme p est premier, les seuls diviseurs de p^k sont les puissances de p. Donc $\text{PGCD}(\ell, p^k) > 1$ si et seulement si p divise ℓ.

Ainsi :

$$p^k - \Phi\left(p^k\right) = \left|\left\{\ell \in [\![1, p^k]\!] \;\middle|\; p \text{ divise } \ell\right\}\right|$$

Les multiples de p dans $[\![1, p^k]\!]$ sont :

$$p \cdot 1,\ p \cdot 2,\ \ldots,\ p \cdot p^{k-1}$$

Il y en a exactement p^{k-1}.

Donc :

$$p^k - \Phi\left(p^k\right) = p^{k-1}$$

Finalement :

$$\Phi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Corollaire 3.17 : (*Formule explicite de la fonction indicatrice d'Euler*)

Soit $m \geqslant 1$ un entier de décomposition en facteurs premiers :

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

où les p_i sont des nombres premiers deux à deux distincts et les $\alpha_i \geqslant 1$.

Alors :

$$\begin{aligned}
\Phi(m) &= \prod_{i=1}^{m} p_i^{\alpha_i - 1}(p_i - 1) \\
&= \prod_{i=1}^{m} \left(p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\right) \\
&= m \prod_{\substack{p \mid m \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

Remarque :

① **Si $m \geqslant 3$, alors $\Phi(m)$ est pair.**

En effet, soit m possède au moins un facteur premier impair p, alors $2 \mid (p-1)$ et $(p-1) \mid \Phi(m)$, donc $2 \mid \Phi(m)$.

Soit $m = 2^k$ avec $k \geqslant 2$, alors :

$$\Phi(m) = 2^{k-1}(2-1) = 2^{k-1}$$

qui est pair car $k \geqslant 2$ implique $k-1 \geqslant 1$.

② **Pour tout $\ell \geqslant 1$, l'ensemble $\mathscr{E}_\ell = \{m \geqslant 1 \mid \Phi(m) = \ell\}$ est fini.**

Soit $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ avec $m \in \mathscr{E}_\ell$.

On a :

$$\Phi(m) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}\left(p_i - 1\right) = \ell$$

Pour tout i, on a $(p_i - 1) \mid \Phi(m) = \ell$ et $p_i^{\alpha_i - 1} \mid \Phi(m) = \ell$.

Donc pour chaque i, il y a un nombre fini de possibilités pour α_i (car $p_i^{\alpha_i - 1} \leqslant \ell$) et pour p_i (car $p_i - 1 \leqslant \ell$).

Ainsi, $\mathscr{E}_\ell$ est fini.

- ⊛ Si $\ell \geqslant 3$ et ℓ est impair, alors $\mathscr{E}_\ell = \varnothing$ (d'après le point 1).
- ⊛ **Calcul de $\mathscr{E}_1$:**

  $\Phi(m) = 1$.

  Les seules solutions sont $m = 1$ et $m = 2$.

  Donc $\mathscr{E}_1 = \{1;2\}$.
- ⊛ **Calcul de $\mathscr{E}_2$:**

  $\Phi(m) = 2$.

  Si p est un facteur premier de m, alors $(p-1) \mid 2$, donc $p - 1 \in \{1;2\}$, ce qui donne $p \in \{2;3\}$.

  Les cas possibles sont :

  - ★ $m = 1 : \Phi(1) = 1 \neq 2$.
  - ★ $m = 2^\alpha : \Phi(m) = 2^{\alpha-1} = 2$, donc $\alpha = 2$, soit $m = 4$.
  - ★ $m = 3^\beta : \Phi(m) = 3^{\beta-1}(3-1) = 2 \cdot 3^{\beta-1} = 2$, donc $\beta = 1$, soit $m = 3$.
  - ★ $m = 2^\alpha \cdot 3^\beta : \Phi(m) = 2^{\alpha-1}(2-1) \cdot 3^{\beta-1}(3-1) = 2^\alpha \cdot 3^{\beta-1} = 2$, donc $\alpha = 1$ et $\beta = 1$, soit $m = 6$.

  Finalement, $\mathscr{E}_2 = \{3;4;6\}$.

③ **$\mathscr{E}_{14} = \varnothing$ et $\mathscr{E}_{26} = \varnothing$.**

Supposons qu'il existe m tel que $\Phi(m) = 14$.

Si p est un facteur premier de m, alors $(p-1) \mid 14$, donc $p - 1 \in \{1;2;7;14\}$, ce qui donne $p \in \{2;3;8;15\}$.

Comme p doit être premier, on a $p \in \{2;3\}$.

Les cas possibles sont :

- ⊛ $m = 1 : \Phi(1) = 1 \neq 14$.
- ⊛ $m = 2^\alpha : \Phi(m) = 2^{\alpha-1} = 14$, impossible car 14 n'est pas une puissance de 2.
- ⊛ $m = 3^\beta : \Phi(m) = 2 \cdot 3^{\beta-1} = 14$, donc $3^{\beta-1} = 7$, impossible.
- ⊛ $m = 2^\alpha \cdot 3^\beta : \Phi(m) = 2^\alpha \cdot 3^{\beta-1} = 14 = 2 \cdot 7$, impossible car 7 n'est pas une puissance de 3.

Donc $\mathscr{E}_{14} = \emptyset$.

De même, pour $\Phi(m) = 26$, on a $(p-1) \mid 26$, donc $p-1 \in \{1;2;13;26\}$, ce qui donne $p \in \{2;3;14;27\}$.

Les seuls premiers possibles sont $p \in \{2;3\}$, et aucun cas ne donne $\Phi(m) = 26$.

Donc $\mathscr{E}_{26} = \emptyset$.

Conjecture 3.18 : (*Conjecture de Carmichael*)

Soit $\ell \geqslant 1$ un entier et $\mathscr{E}_\ell = \{m \geqslant 1 \mid \Phi(m) = \ell\}$ l'ensemble des entiers dont l'indicatrice d'Euler vaut ℓ.

Pour tout $\ell \geqslant 2$, on a $|\mathscr{E}_\ell| \neq 1$.

Autrement dit, pour tout $m \geqslant 1$, il existe $n \neq m$ tel que $\Phi(n) = \Phi(m)$.

Exemple :

On a :

$$\mathscr{E}_8 = \{15;16;20;24;30\}$$

qui contient 5 éléments, confirmant la conjecture pour $\ell = 8$.

Chapitre 4

Idéaux premiers, idéaux maximaux

Définition 4.1 : (*Idéal premier*)

Soit A un anneau commutatif unitaire et I un idéal de A.

On dit que I est un ***idéal premier*** si $I \neq A$ et :

$$\forall (a,b) \in A^2, \quad a \cdot b \in I \quad \Longrightarrow \quad a \in I \quad \text{ou} \quad b \in I$$

Définition 4.2 : (*Idéal maximal*)

Soit A un anneau commutatif unitaire et I un idéal de A.

On dit que I est un ***idéal maximal*** si $I \neq A$ et :

$$\forall J \text{ idéal de } A, \quad I \subset J \quad \Longrightarrow \quad J = I \quad \text{ou} \quad J = A$$

Théorème 4.3 : (*Tout idéal maximal est premier*)

Soit A un anneau commutatif unitaire et I un idéal de A.

Si I est un idéal maximal, alors I est un idéal premier.

Preuve :

Soit $\mathscr{M}$ un idéal maximal de A.

Par définition d'un idéal maximal, on a $\mathscr{M} \neq A$.

Montrons que $\mathscr{M}$ est premier.

Soient $a, b \in A$ tels que $a \cdot b \in \mathscr{M}$.

Définissons l'ensemble :

$$\mathscr{N} = \{m + \lambda \cdot a \mid m \in \mathscr{M},\ \lambda \in A\}$$

⊛ $\mathscr{N}$ **est un idéal de** A**.**

★ *$\mathscr{N}$ est non vide :*

On a $0_A = 0_A + 0_A \cdot a \in \mathscr{N}$ (car $0_A \in \mathscr{M}$).

Donc $\mathscr{N} \neq \emptyset$.

★ *Stabilité par soustraction :*

Soient $x, y \in \mathscr{N}$. Il existe $m_1, m_2 \in \mathscr{M}$ et $\lambda_1, \lambda_2 \in A$ tels que :

$$x = m_1 + \lambda_1 \cdot a$$

$$y = m_2 + \lambda_2 \cdot a$$

Alors :

$$\begin{aligned} x - y &= (m_1 + \lambda_1 \cdot a) - (m_2 + \lambda_2 \cdot a) \\ &= \underbrace{(m_1 - m_2)}_{\in \mathscr{M}} + \underbrace{(\lambda_1 - \lambda_2)}_{\in A} \cdot a \in \mathscr{N} \end{aligned}$$

★ *Stabilité par multiplication par un élément de A :*

Soit $x \in \mathscr{N}$ et $r \in A$. Il existe $m \in \mathscr{M}$ et $\lambda \in A$ tels que $x = m + \lambda \cdot a$.

Alors :

$$\begin{aligned} r \cdot x &= r \cdot (m + \lambda \cdot a) \\ &= \underbrace{r \cdot m}_{\in \mathscr{M}} + \underbrace{(r \cdot \lambda)}_{\in A} \cdot a \in \mathscr{N} \end{aligned}$$

Finalement, $\mathscr{N}$ est un idéal de A.

⊛ **Inclusion $\mathscr{M} \subset \mathscr{N}$.**

Soit $m \in \mathscr{M}$. On peut écrire :

$$m = m + 0_A \cdot a \in \mathscr{N}$$

Donc $\mathscr{M} \subset \mathscr{N}$.

⊛ **Utilisation de la maximalité de $\mathscr{M}$.**

Puisque $\mathscr{M}$ est maximal et $\mathscr{M} \subset \mathscr{N}$, on a :

$$\mathscr{N} = \mathscr{M} \quad \text{ou} \quad \mathscr{N} = A$$

★ **Cas 1 : $\mathscr{N} = \mathscr{M}$.**

On a $a = 0_A + 1_A \cdot a \in \mathscr{N} = \mathscr{M}$.

Donc $a \in \mathscr{M}$.

★ **Cas 2 : $\mathscr{N} = A$.**

Puisque $1_A \in A = \mathscr{N}$, il existe $m \in \mathscr{M}$ et $\lambda \in A$ tels que :

$$1_A = m + \lambda \cdot a$$

Multiplions par b :

$$\begin{aligned} b &= b \cdot 1_A \\ &= b \cdot (m + \lambda \cdot a) \\ &= \underbrace{b \cdot m}_{\in \mathscr{M}} + \lambda \cdot \underbrace{(a \cdot b)}_{\in \mathscr{M}} \end{aligned}$$

Comme $\mathscr{M}$ est un idéal, $b \cdot m \in \mathscr{M}$ et $\lambda \cdot (a \cdot b) \in \mathscr{M}$.

Donc $b \in \mathscr{M}$.

Dans les deux cas, on a $a \in \mathscr{M}$ ou $b \in \mathscr{M}$.

Finalement, $\mathscr{M}$ est un idéal premier de A.

Exemple :

Soit $A = \mathbb{Z}$.

Les idéaux de $\mathbb{Z}$ sont les $a\mathbb{Z}$ pour $a \in \mathbb{N}$.

① $a\mathbb{Z}$ est premier $\iff$ $a = 0$ ou a est premier.

② $a\mathbb{Z}$ est maximal $\iff$ a est premier.

En particulier, $\{0\}$ est premier et non maximal, ce qui montre que la réciproque du théorème 4.3 est fausse.

Preuve :

① **Démontrons que $a\mathbb{Z}$ est premier $\iff$ $a = 0$ ou a est premier.**

⊛ **Sens direct ($\Rightarrow$) :**

Supposons que $a\mathbb{Z}$ est premier. Raisonnons par l'absurde en supposant que $a \neq 0$ et que a n'est pas premier.

★ Si $a = 1$, alors $a\mathbb{Z} = \mathbb{Z}$, ce qui contredit le fait que $a\mathbb{Z}$ est premier (car un idéal premier doit être différent de A).

★ Si $a \neq 1$, alors a n'étant pas premier, il existe $b \geqslant 2$ et $c \geqslant 2$ tels que $a = b \cdot c$.

On a :

$$b \cdot c = a \cdot 1 \in a\mathbb{Z}$$

Cependant, $b \notin a\mathbb{Z}$ (car $b < a$ et $b \neq 0$) et $c \notin a\mathbb{Z}$ (car $c < a$ et $c \neq 0$).

Cela contredit le fait que $a\mathbb{Z}$ est premier.

Donc $a = 0$ ou a est premier.

⊛ **Sens réciproque ($\Leftarrow$) :**

★ **Cas $a = 0$:**

On a $a\mathbb{Z} = \{0\}$.

Montrons que $\{0\}$ est premier :

♣ $\{0\} \neq \mathbb{Z}$ (car $1 \notin \{0\}$).

♣ Soient $b, c \in \mathbb{Z}$ tels que $b \cdot c \in \{0\}$, c'est-à-dire $b \cdot c = 0$.

Comme $\mathbb{Z}$ est un anneau intègre, on a $b = 0$ ou $c = 0$, donc $b \in \{0\}$ ou $c \in \{0\}$.

Ainsi, $\{0\}$ est un idéal premier de $\mathbb{Z}$.

★ **Cas $a = p$ premier :**

On a $p\mathbb{Z} \neq \mathbb{Z}$ (car $1 \notin p\mathbb{Z}$).

Soient $b, c \in \mathbb{Z}$ tels que $b \cdot c \in p\mathbb{Z}$.

Alors il existe $\lambda \in \mathbb{Z}$ tel que $b \cdot c = p \cdot \lambda$, c'est-à-dire $p \mid b \cdot c$.

Comme p est premier, on a $p \mid b$ ou $p \mid c$.

Donc $b \in p\mathbb{Z}$ ou $c \in p\mathbb{Z}$.

Ainsi, $p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.

② **Démontrons que $a\mathbb{Z}$ est maximal $\iff$ a est premier.**

⊛ **Sens direct ($\Rightarrow$) :**

Supposons que $a\mathbb{Z}$ est maximal.

D'après le théorème 4.3, $a\mathbb{Z}$ est premier.

Donc a est premier ou $a = 0$.

Or, $0 \cdot \mathbb{Z} = \{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Donc $a\mathbb{Z} = \{0\}$ n'est pas maximal, ce qui implique $a \neq 0$.

Ainsi, a est premier.

⊛ **Sens réciproque ($\Leftarrow$) :**

Supposons que $a = p$ est premier.

On a $p\mathbb{Z} \neq \mathbb{Z}$ (car $1 \notin p\mathbb{Z}$).

Soit J un idéal de $\mathbb{Z}$ tel que $p\mathbb{Z} \subset J$.

Comme tout idéal de $\mathbb{Z}$ est de la forme $b\mathbb{Z}$ avec $b \in \mathbb{N}$, il existe $b \in \mathbb{N}$ tel que $J = b\mathbb{Z}$.

On a $p = p \cdot 1 \in p\mathbb{Z} \subset J = b\mathbb{Z}$.

Donc $p \in b\mathbb{Z}$, ce qui signifie qu'il existe $x \in \mathbb{Z}$ tel que $p = b \cdot x$.

Ainsi, $b \mid p$.

Comme p est premier, on a $b = 1$ ou $b = p$.

- Si $b = 1$, alors $J = b\mathbb{Z} = 1 \cdot \mathbb{Z} = \mathbb{Z}$.
- Si $b = p$, alors $J = b\mathbb{Z} = p\mathbb{Z}$.

Dans les deux cas, $J = p\mathbb{Z}$ ou $J = \mathbb{Z}$.

Ainsi, $p\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$.

Définition 4.4 : (*Idéal principal*)

Soit A un anneau commutatif unitaire et I un idéal de A.

On dit que I est un ***idéal principal*** s'il existe $x \in A$ tel que :

$$I = Ax = \{a \cdot x \mid a \in A\}$$

Définition 4.5 : (*Anneau principal*)

Soit A un anneau commutatif unitaire.

On dit que A est un ***anneau principal*** si :

- A est intègre, c'est-à-dire $A \neq \{0\}$ et :

$$\forall (a,b) \in A^2, \quad a \cdot b = 0 \Longrightarrow a = 0 \quad \text{ou} \quad b = 0$$

- Tout idéal de A est principal.

Exemple :

- $\mathbb{Z}$ est un anneau principal.
- $K[x]$ est un anneau principal (où K est un corps).

Théorème 4.6 : (*Idéal premier dans un anneau principal*)

Soit A un anneau principal.

Tout idéal premier de A différent de $\{0\}$ est maximal.

Preuve :

Soit $\mathscr{P}$ un idéal premier de A tel que $\mathscr{P} \neq \{0\}$ et $\mathscr{P} \neq A$.

Comme A est un anneau principal, $\mathscr{P}$ est principal. Il existe donc $x \in A$, $x \neq 0$ (car $\mathscr{P} \neq \{0\}$), tel que :

$$\mathscr{P} = Ax$$

Soit J un idéal de A tel que $\mathscr{P} \subset J$.

Comme A est principal, il existe $y \in A$ tel que :

$$J = Ay$$

On a $x = 1_A \cdot x \in Ax = \mathscr{P} \subset J = Ay$.

Donc $x \in Ay$, ce qui signifie qu'il existe $\alpha \in A$ tel que :

$$x = \alpha \cdot y$$

Or $\alpha \cdot y = 1_A \cdot x \in Ax = \mathscr{P}$, donc $\alpha \cdot y \in \mathscr{P}$.

Comme $\mathscr{P}$ est un idéal premier, on en déduit que :

$$\alpha \in \mathscr{P} \quad \text{ou} \quad y \in \mathscr{P}$$

⊛ **Cas 1 : $\alpha \in \mathscr{P}$.**

Comme $\alpha \in \mathscr{P} = Ax$, il existe $\beta \in A$ tel que :

$$\alpha = \beta \cdot x$$

Alors :

$$\begin{aligned} x &= \alpha \cdot y \\ &= (\beta \cdot x) \cdot y \\ &= \beta \cdot x \cdot y \\ &= x \cdot \beta \cdot y \qquad \text{car } A \text{ est commutatif} \end{aligned}$$

Donc :

$$x - x \cdot \beta \cdot y = 0_A$$
$$x \cdot (1_A - \beta \cdot y) = 0_A$$

Comme A est intègre et $x \neq 0_A$, on en déduit que :

$$1_A - \beta \cdot y = 0_A$$

Donc :

$$\beta \cdot y = 1_A$$

Ainsi, $1_A = \beta \cdot y \in Ay = J$, donc $1_A \in J$.

Finalement, $J = A$.

⊛ **Cas 2 : $y \in \mathscr{P}$.**

Soit $t \in J = Ay$.

Il existe $\alpha \in A$ tel que $t = \alpha \cdot y$.

Comme $y \in \mathscr{P}$ et $\mathscr{P}$ est un idéal, on a $\alpha \cdot y \in \mathscr{P}$.

Donc $t \in \mathscr{P}$.

Ainsi, $J \subset \mathscr{P}$.

Comme on a déjà $\mathscr{P} \subset J$, on en déduit que $J = \mathscr{P}$.

Dans les deux cas, $J = \mathscr{P}$ ou $J = A$.

Finalement, $\mathscr{P}$ est un idéal maximal de A.

Remarque :

Soit A un anneau commutatif unitaire et I un idéal de A.

① I est premier $\iff \dfrac{A}{I}$ est intègre.

② I est maximal $\iff \dfrac{A}{I}$ est un corps.

On retrouve que (I maximal $\implies I$ premier), car tout corps est intègre.

Preuve :

Preuve de 1) : I est premier $\iff \dfrac{A}{I}$ est intègre.

⊛ **Sens direct ($\Rightarrow$) :**

Supposons que I est premier. Alors $I \neq A$, donc :

$$\frac{A}{I} \neq \left\{0_{\frac{A}{I}}\right\} \quad \text{avec} \quad 0_{\frac{A}{I}} = \overline{0_A}$$

Soient $(x,y) \in \left(\dfrac{A}{I}\right)^2$ tels que $x \cdot y = 0_{\frac{A}{I}}$.

Il existe $a, b \in A$ tels que $x = \overline{a}$ et $y = \overline{b}$.

Alors :

$$x \cdot y = \overline{a} \cdot \overline{b} = \overline{a \cdot b} = 0_{\frac{A}{I}} = \overline{0_A}$$

Donc $a \cdot b \in I$.

Comme I est premier, on a $a \in I$ ou $b \in I$.

★ Si $a \in I$, alors $x = \overline{a} = 0_{\frac{A}{I}}$.

★ Si $b \in I$, alors $y = \overline{b} = 0_{\frac{A}{I}}$.

Ainsi, $\dfrac{A}{I}$ est intègre.

⊛ **Sens réciproque ($\Leftarrow$) :**

Supposons que $\dfrac{A}{I}$ est intègre.

Alors $\dfrac{A}{I} \neq \left\{0_{\frac{A}{I}}\right\}$, donc $I \neq A$.

Soient $a, b \in A$ tels que $a \cdot b \in I$.

Alors $\overline{a \cdot b} = \overline{0_A} = 0_{\frac{A}{I}}$, c'est-à-dire $\overline{a} \cdot \overline{b} = 0_{\frac{A}{I}}$.

Comme $\dfrac{A}{I}$ est intègre, on a $\overline{a} = 0_{\frac{A}{I}}$ ou $\overline{b} = 0_{\frac{A}{I}}$.

Donc $a \in I$ ou $b \in I$.

Ainsi, I est premier.

Preuve de 2) : I est maximal $\iff \dfrac{A}{I}$ est un corps.

D'après le théorème de correspondance des idéaux, les idéaux de $\dfrac{A}{I}$ sont les $\dfrac{J}{I}$, où J est un idéal de A contenant I.

$$\begin{aligned} I \text{ est maximal} &\iff I \neq A \text{ et les seuls idéaux de } A \text{ contenant } I \text{ sont } I \text{ et } A \\ &\iff \frac{A}{I} \neq \left\{0_{\frac{A}{I}}\right\} \text{ et les seuls idéaux de } \frac{A}{I} \text{ sont } \left\{0_{\frac{A}{I}}\right\} \text{ et } \frac{A}{I} \end{aligned}$$

Il suffit donc d'appliquer à $B = \dfrac{A}{I}$ le lemme suivant.

Lemme 4.7 : (*Caractérisation d'un corps par ses idéaux*)

Soit B un anneau commutatif unitaire tel que $B \neq \{0_B\}$.

Alors B est un corps si et seulement si les seuls idéaux de B sont $\{0_B\}$ et B.

Preuve :

⊛ **Sens direct ($\Rightarrow$) :**

Supposons que B est un corps.

Soit I un idéal de B tel que $I \neq \{0_B\}$.

Il existe $x \in I$ tel que $x \neq 0_B$.

Comme B est un corps, x admet un inverse x^{-1} dans B.

Soit $y \in B$. Alors :

$$y = \underbrace{\left(y \cdot x^{-1}\right)}_{\in B} \cdot \underbrace{x}_{\in I} \in I$$

Donc $B \subset I$, ce qui implique $B = I$.

Ainsi, les seuls idéaux de B sont $\{0_B\}$ et B.

⊛ **Sens réciproque ($\Leftarrow$) :**

Supposons que les seuls idéaux de B sont $\{0_B\}$ et B.

Soit $x \in B$ tel que $x \neq 0_B$.

Considérons l'ensemble :

$$I = Bx = \{b \cdot x \mid b \in B\}$$

I est un idéal de B (idéal principal engendré par x).

On a $0_B \neq x = 1_B \cdot x \in I$, donc $I \neq \{0_B\}$.

Par hypothèse, $I = B$.

En particulier, $1_B \in I$, donc il existe $y \in B$ tel que $1_B = y \cdot x$.

Comme B est commutatif, on a $x \cdot y = y \cdot x = 1_B$.

Ainsi, tout élément non nul de B est inversible, donc B est un corps.

Chapitre 5

Anneaux euclidiens, principaux, factoriels

Remarque :

Les implications entre ces trois types d'anneaux sont les suivantes :

$$\text{Euclidien} \Longrightarrow \text{Principal} \Longrightarrow \text{Factoriel}$$

Les réciproques sont fausses en général.

Définition 5.1 : (*Anneau euclidien*)

Soit A un anneau commutatif unitaire intègre.

On dit que A est un ***anneau euclidien*** s'il existe une application $d : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que :

① Pour tous $x, y \in A \setminus \{0\}$:

$$x \mid y \Longrightarrow d(x) \leqslant d(y)$$

② Pour tous $a \in A$ et $b \in A \setminus \{0\}$, il existe $(q, r) \in A^2$ tels que :

$$a = b \cdot q + r$$

$$\text{et} \quad (r = 0 \quad \text{ou} \quad d(r) < d(b))$$

Dans ce cas on dit que d est un ***stathme euclidien***.

Exemple :

① $A = \mathbb{Z}$ avec $d(x) = |x|$.

② $A = K[x]$ (où K est un corps commutatif) avec $d(P) = \deg(P)$.

③ $A = \mathbb{Z}[i] = \left\{a + i \cdot b \;\middle|\; (a, b) \in \mathbb{Z}^2\right\}$ avec $d(a + i \cdot b) = a^2 + b^2$.

Théorème 5.2 : (*Un anneau euclidien est principal*)

Soit A un anneau euclidien.

Alors A est un anneau principal.

Preuve :

Soit I un idéal de A.

Si $I = \{0_A\}$, alors $I = A \cdot 0_A$ est principal.

Si $I \neq \{0_A\}$, il existe $x \in I$ tel que $x \neq 0_A$.

L'ensemble :

$$\{d(x) \mid x \in I,\ x \neq 0_A\}$$

est une partie non vide de $\mathbb{N}$, donc elle possède un plus petit élément n_0.

Il existe donc $i_0 \in I$, $i_0 \neq 0_A$, tel que $n_0 = d(i_0)$.

On a $A \cdot i_0 \subset I$ (car $i_0 \in I$ et I est un idéal).

Soit $i \in I$. D'après la définition d'un anneau euclidien, il existe $(q, r) \in A^2$ tels que :

$$i = q \cdot i_0 + r \quad \text{et} \quad (r = 0 \quad \text{ou} \quad d(r) < d(i_0))$$

On a :

$$r = i - q \cdot i_0 = \underbrace{i}_{\in I} + \underbrace{(-q)}_{\in A} \cdot \underbrace{i_0}_{\in I} \in I$$

Si $r \neq 0_A$, alors $r \in I$ et $r \neq 0_A$, donc $d(r) \in \{d(x) \mid x \in I,\ x \neq 0_A\}$.

Mais $d(r) < d(i_0) = n_0$, ce qui contredit la minimalité de n_0.

Donc $r = 0_A$, et :

$$i = q \cdot i_0 \in A \cdot i_0$$

Ainsi, $I \subset A \cdot i_0$.

Finalement, $I = A \cdot i_0$, donc I est principal.

Tout idéal de A est principal, donc A est un anneau principal.

Définition 5.3 : (*Relation de divisibilité*)

Soit A un anneau commutatif unitaire intègre.

Sur $A \setminus \{0_A\}$, on définit la ***relation de divisibilité*** par :

$$a \mid b \iff (\exists c \in A \setminus \{0_A\}), \quad b = a \cdot c$$

Cette relation est réflexive et transitive.

Définition 5.4 : (*Relation d'association*)

Soit A un anneau commutatif unitaire intègre.

On définit la ***relation d'association*** $\sim$ sur $A \setminus \{0_A\}$ par :

$$a \sim b \iff a \mid b \quad \text{et} \quad b \mid a$$

Propriété 5.5 : ($\sim$ *est une relation d'équivalence*)

Soit A un anneau commutatif unitaire intègre.

La relation $\sim$ est une relation d'équivalence sur $A \setminus \{0_A\}$.

Preuve :

- **Réflexivité :**

  Soit $a \in A \setminus \{0_A\}$.

  On a $a = 1_A \cdot a$, donc $a \mid a$.

  Ainsi, $a \sim a$.

- **Symétrie :**

  Soient $a, b \in A \setminus \{0_A\}$ tels que $a \sim b$.

  Alors $a \mid b$ et $b \mid a$, donc $b \mid a$ et $a \mid b$.

  Ainsi, $b \sim a$.

- **Transitivité :**

  Soient $a, b, c \in A \setminus \{0_A\}$ tels que $a \sim b$ et $b \sim c$.

  Alors $a \mid b$ et $b \mid c$, donc il existe $x, y \in A$ tels que $b = a \cdot x$ et $c = b \cdot y$.

  Ainsi, $c = (a \cdot x) \cdot y = a \cdot (x \cdot y)$, donc $a \mid c$.

De même, $c \mid b$ et $b \mid a$, donc $c \mid a$.

Finalement, $a \sim c$.

La relation $\sim$ est donc une relation d'équivalence sur $A \setminus \{0_A\}$.

Propriété 5.6 : (*Caractérisation de l'association par les unités*)

Soit A un anneau commutatif unitaire intègre.

Pour tous $a, b \in A \setminus \{0_A\}$:

$$a \sim b \iff (\exists u \in U(A)), \quad a = u \cdot b$$

Preuve :

⊛ **Sens direct ($\Rightarrow$) :**

Supposons que $a \sim b$, c'est-à-dire $a \mid b$ et $b \mid a$.

Il existe $c, c' \in A$ tels que :

$$b = a \cdot c \quad \text{et} \quad a = b \cdot c'$$

Alors :

$$\begin{aligned} a &= b \cdot c' \\ &= (a \cdot c) \cdot c' \\ &= a \cdot \left(c \cdot c'\right) \end{aligned}$$

Donc :

$$a \cdot \left(1_A - c \cdot c'\right) = 0_A$$

Comme A est intègre et $a \neq 0_A$, on en déduit que :

$$1_A - c \cdot c' = 0_A$$

c'est-à-dire $c \cdot c' = 1_A$.

Ainsi, c' est inversible et $a = c' \cdot b$ avec $c' \in U(A)$.

⊛ **Sens réciproque ($\Leftarrow$) :**

Supposons qu'il existe $u \in U(A)$ tel que $a = u \cdot b$.

Alors $a \mid b$ (car $a = u \cdot b$).

De plus, $b = u^{-1} \cdot a$, donc $b \mid a$.

Ainsi, $a \sim b$.

Finalement, $a \sim b \iff \exists u \in U(A),\ a = u \cdot b$.

Définition 5.7 : (*Élément irréductible*)

Soit A un anneau commutatif unitaire intègre.

Un élément $a \in A \setminus \{0_A\}$ est dit ***irréductible*** si :

⊛ a n'est pas inversible,

⊛ Pour tous $b, c \in A$:

$$a = b \cdot c \quad \Longrightarrow \quad b \in U(A) \quad \text{ou} \quad c \in U(A)$$

Propriété 5.8 : (*Invariance de l'irréductibilité par association*)

Soit A un anneau commutatif unitaire intègre.

Soient a et a' deux éléments de A tels que a est irréductible et $a \sim a'$.

Alors a' est irréductible.

Preuve :

Puisque $a \sim a'$, il existe $u \in U(A)$ tel que $a' = u \cdot a$.

- a' **n'est pas inversible :**

  Si a' était inversible, alors $a = u^{-1} \cdot a'$ serait inversible (comme produit d'éléments inversibles), ce qui contredit l'hypothèse que a est irréductible.

  Donc a' n'est pas inversible.

- **Propriété de factorisation :**

  Soient $b, c \in A$ tels que $a' = b \cdot c$.

  Alors $u \cdot a = b \cdot c$, donc :

  $$a = u^{-1} \cdot b \cdot c$$

  Comme a est irréductible, on a $u^{-1} \cdot b \in U(A)$ ou $c \in U(A)$.

  - Si $c \in U(A)$, alors c est inversible.
  - Si $u^{-1} \cdot b \in U(A)$, alors $b = u \cdot \left(u^{-1} \cdot b\right)$ est inversible (comme produit d'éléments inversibles).

  Dans les deux cas, b ou c est inversible.

Finalement, a' est un élément irréductible de A.

Définition 5.9 : (*Anneau factoriel*)

Soit A un anneau commutatif unitaire intègre.

On dit que A est un ***anneau factoriel*** (ou ***anneau factoriel unique*** - UFD) si chaque élément $a \in A \setminus \{0_A\}$ possède une décomposition essentiellement unique :

$$a = u \cdot p_1 \cdots p_m$$

où :

- $u \in U(A)$ est inversible,
- $m \geqslant 0$,
- $p_1, \ldots, p_m$ sont irréductibles.

Définition 5.10 : (*Décomposition essentiellement unique*)

La décomposition est dite ***essentiellement unique*** si :

Pour toutes décompositions :

$$a = u \cdot p_1 \cdots p_m = v \cdot q_1 \cdots q_n$$

où $u, v \in U(A)$ et les p_i, q_j sont irréductibles, alors :

- $n = m$,
- Il existe une permutation σ de $\{1;\dots;m\}$ telle que pour tout $i \in \{1;\dots;m\}$:

$$q_i \sim p_{\sigma(i)}$$

Théorème 5.11 : (*Théorème de Bachet-Bézout*)

Soit A un anneau principal.

Soient $a \in A$ et $b \in A$.

Il existe $d \in A$ tel que :

- $d \mid a$, $d \mid b$,
- Pour tout $d' \in A$:

$$\left[d' \mid a \quad \text{et} \quad d' \mid b \Longrightarrow d' \mid d\right]$$

d est un PGCD de a et b.

De plus, il existe $(x, y) \in A^2$ tel que :

$$d = a \cdot x + b \cdot y$$

Preuve :

Considérons l'idéal :

$$I = A \cdot a + A \cdot b = \left\{\lambda \cdot a + \mu \cdot b \;\middle|\; (\lambda, \mu) \in A^2\right\}$$

I est un idéal de A.

Comme A est principal, il existe $d \in A$ tel que :

$$I = A \cdot d = \{z \cdot d \mid z \in A\}$$

- d **divise** a **et** b **:**

  On a $a = 1_A \cdot a + 0_A \cdot b \in I = A \cdot d$.

  Il existe $c \in A$ tel que $a = c \cdot d$, donc $d \mid a$.

  De même, $b = 0_A \cdot a + 1_A \cdot b \in I = A \cdot d$.

  Il existe $c' \in A$ tel que $b = c' \cdot d$, donc $d \mid b$.

- **Relation de Bézout :**

  On a $d = 1_A \cdot d \in A \cdot d = I$.

  Il existe $(x, y) \in A^2$ tel que :

$$d = x \cdot a + y \cdot b$$

- d **est un PGCD de** a **et** b **:**

  Supposons que $d' \mid a$ et $d' \mid b$.

  Il existe $a', b' \in A$ tels que :

$$a = d' \cdot a' \quad \text{et} \quad b = d' \cdot b'$$

Alors :

$$\begin{aligned} d &= x \cdot a + y \cdot b \\ &= x \cdot \left(d' \cdot a'\right) + y \cdot \left(d' \cdot b'\right) \\ &= d' \cdot \left(x \cdot a' + y \cdot b'\right) \end{aligned}$$

Donc $d' \mid d$.

Finalement, d est un PGCD de a et b et vérifie la relation de Bézout.

Lemme 5.12 : (*Lemme de Gauss*)

Soit A un anneau principal.

Soit $p \in A$ un élément irréductible et soient $a, b \in A$.

Si $p \mid a \cdot b$, alors $p \mid a$ ou $p \mid b$.

Preuve :

D'après le théorème de Bachet-Bézout (théorème 5.11), il existe $d \in A$ tel que $d \mid a$, $d \mid p$ et il existe $\left(x, y\right) \in A^2$ tel que :

$$d = a \cdot x + p \cdot y$$

Comme $d \mid p$, il existe $e \in A$ tel que $p = d \cdot e$.

Puisque p est irréductible, on en déduit que d ou e est inversible.

- **Cas 1 : d est inversible.**

  On a :

  $$\begin{aligned} 1_A &= d^{-1} \cdot d \\ &= d^{-1} \cdot a \cdot x + d^{-1} \cdot p \cdot y \end{aligned}$$

  Multiplions par b :

  $$\begin{aligned} b &= b \cdot 1_A \\ &= b \cdot \left(d^{-1} \cdot a \cdot x + d^{-1} \cdot p \cdot y\right) \\ &= d^{-1} \cdot x \cdot (a \cdot b) + p \cdot \left(b \cdot d^{-1} \cdot y\right) \end{aligned}$$

  Comme $p \mid a \cdot b$, il existe $f \in A$ tel que $a \cdot b = p \cdot f$.

  Donc :

  $$\begin{aligned} b &= d^{-1} \cdot x \cdot \left(p \cdot f\right) + p \cdot \left(b \cdot d^{-1} \cdot y\right) \\ &= p \cdot \left(d^{-1} \cdot x \cdot f + b \cdot d^{-1} \cdot y\right) \end{aligned}$$

  Ainsi, $p \mid b$.

- **Cas 2 : e est inversible.**

  Comme $d \mid a$, il existe $h \in A$ tel que $a = d \cdot h$.

  Alors :

  $$\begin{aligned} a &= d \cdot h \\ &= p \cdot e^{-1} \cdot h \end{aligned}$$

$$= p \cdot \left(e^{-1} \cdot h\right)$$

Ainsi, $p \mid a$.

Dans les deux cas, on a $p \mid a$ ou $p \mid b$.

Lemme 5.13 : (*Absence de suite infinie strictement décroissante pour la divisibilité*)

Soit A un anneau principal.

Il n'existe pas de suite $a_0, \ldots, a_m, \ldots$ d'éléments de $A \setminus \{0_A\}$ telle que pour tout $n \in \mathbb{N}$:

$$a_{n+1} \mid a_n \quad \text{et} \quad a_n \not\sim a_{n+1}$$

Preuve :

Raisonnons par l'absurde en supposant qu'une telle suite existe.

Considérons l'ensemble :

$$I = \left\{ \lambda_1 \cdot a_1 + \cdots + \lambda_m \cdot a_m \;\middle|\; m \in \mathbb{N},\ (\lambda_1, \ldots, \lambda_m) \in A^m \right\}$$

I est un idéal de A.

Comme A est principal, il existe $d \in A$ tel que $I = A \cdot d$.

On a $d = 1_A \cdot d \in I$, donc il existe $m \in \mathbb{N}$ et $\lambda_1, \ldots, \lambda_m \in A$ tels que :

$$d = \lambda_1 \cdot a_1 + \cdots + \lambda_m \cdot a_m$$

Comme $a_{m+1} \mid a_m$ et $a_m \mid a_{m-1}$, etc., on a $a_{m+1} \mid a_k$ pour tout $k \leqslant m$.

Donc $a_{m+1} \mid d$, ce qui signifie qu'il existe $c \in A$ tel que $a_{m+1} = c \cdot d$.

Ainsi, $a_{m+1} \in A \cdot d = I$.

Mais par hypothèse, $a_m \not\sim a_{m+1}$ et $a_{m+1} \mid a_m$, donc $a_m \mid a_{m+1}$ est faux.

Contradiction.

Une telle suite n'existe donc pas.

Théorème 5.14 : (*Principal implique factoriel*)

Soit A un anneau principal.

Alors A est un anneau factoriel.

Preuve :

Supposons que A est principal.

① **Existence de la décomposition :**

Soit $a \in A \setminus \{0_A\}$.

Si a est irréductible, la décomposition est triviale.

Sinon, $a = a_1 \cdot b_1$ avec a_1, b_1 non inversibles.

Si a_1 ou b_1 n'est pas irréductible, on recommence.

D'après le lemme 5.13, ce processus doit s'arrêter.

Donc a admet une décomposition en irréductibles.

② **Unicité de la décomposition :**

Soient deux décompositions :

$$a = u \cdot p_1 \cdots p_n = v \cdot q_1 \cdots q_m$$

où $u, v \in U(A)$ et les p_i, q_j sont irréductibles.

Par récurrence sur n :

- Si $n = 0$, alors $a = u$ est inversible, donc $m = 0$.
- Si $n \geqslant 1$, alors $p_1 \mid v \cdot q_1 \cdots q_m$.

  D'après le lemme de Gauss (lemme 5.12), $p_1 \mid q_j$ pour un certain j.

  Comme q_j est irréductible, $p_1 \sim q_j$.

  En simplifiant, on obtient une décomposition avec $n-1$ facteurs, et on conclut par récurrence.

Ainsi, la décomposition est essentiellement unique.

Finalement, A est un anneau factoriel.

Propriété 5.15 : (*Unités de l'anneau des polynômes*)

Soit A un anneau commutatif unitaire intègre.

Les éléments inversibles de $A[x]$ sont les éléments inversibles de A (considérés comme polynômes de degré 0).

Autrement dit :

$$U(A[x]) = U(A)$$

Preuve :

Soit $P \in U(A[x])$.

Il existe $Q \in A[x]$ tel que $P \cdot Q = 1_{A[x]}$.

Écrivons $P = \sum_{k=0}^{n} a_k \cdot x^k$ avec $a_n \neq 0_A$ et $Q = \sum_{k=0}^{m} b_k \cdot x^k$ avec $b_m \neq 0_A$.

Alors :

$$1_A = P \cdot Q = \underbrace{a_n \cdot b_m}_{\neq 0_A} \cdot x^{n+m} + \cdots$$

car A est intègre, donc $a_n \cdot b_m \neq 0_A$.

En identifiant les degrés, on obtient $n + m = 0$, donc $n = 0$ (car $n, m \geqslant 0$).

Ainsi, $P = a_0 \in A$ et $a_0 \cdot b_0 = 1_A$, donc $P \in U(A)$.

Réciproquement, tout élément de $U(A)$ est inversible dans $A[x]$.

Finalement, $U(A[x]) = U(A)$.

Remarque :

L'hypothèse "A intègre" est essentielle.

Par exemple, dans $\frac{\mathbb{Z}}{4\mathbb{Z}}[x]$:

$$\left(\overline{1} + \overline{2} \cdot x\right) \cdot \left(\overline{1} - \overline{2} \cdot x\right) = \overline{1}$$

donc $\overline{1} + \overline{2} \cdot x \in U\left(\frac{\mathbb{Z}}{4\mathbb{Z}}[x]\right)$ mais $\overline{1} + \overline{2} \cdot x \notin U\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)$.

Définition 5.16 : (*Contenu d'un polynôme*)

Soit A un anneau factoriel et $P = a_n \cdot x^n + \cdots + a_0 \in A[x]$ un polynôme non nul.

On appelle ***contenu*** de P et on note $c(P)$ le PGCD des coefficients de P :

$$c(P) = \text{PGCD}(a_0, \ldots, a_n)$$

Le contenu est défini à multiplication près par un élément de $U(A)$.

Lemme 5.17 : (*Lemme de Gauss (version polynômes)*)

Soit A un anneau factoriel.

Pour tous $P, Q \in A[x]$:

$$c(P \cdot Q) \sim c(P) \cdot c(Q)$$

Preuve :

Soient $P = a_n \cdot x^n + \cdots + a_0$ et $Q \in A[x]$.

On peut écrire $P = c(P) \cdot R$ où $R = a'_n \cdot x^n + \cdots + a'_0$ avec $a_k = c(P) \cdot a'_k$.

Alors :

$$\begin{aligned} c(R) &= \text{PGCD}(a'_0, \ldots, a'_n) \\ &= \text{PGCD}\left(\frac{a_0}{c(P)}, \ldots, \frac{a_n}{c(P)}\right) \\ &\sim \frac{\text{PGCD}(a_0, \ldots, a_n)}{c(P)} \\ &= \frac{c(P)}{c(P)} = 1 \end{aligned}$$

De même, on écrit $Q = c(Q) \cdot S$ avec $c(S) = 1$.

Alors :

$$P \cdot Q = (c(P) \cdot R) \cdot (c(Q) \cdot S) = c(P) \cdot c(Q) \cdot R \cdot S$$

Donc :

$$c(P \cdot Q) = c\left(c(P) \cdot c(Q) \cdot R \cdot S\right) = c(P) \cdot c(Q) \cdot c(R \cdot S)$$

Il suffit donc de démontrer que $c(R \cdot S) = 1$.

Raisonnons par l'absurde en supposant que $c(R \cdot S)$ est divisible par un irréductible p de A.

Écrivons $R = d_s \cdot x^s + \cdots + d_0$ et $S = e_t \cdot x^t + \cdots + e_0$.

On a $c(R) = 1 = \text{PGCD}(d_0, \ldots, d_s)$, donc il existe un plus petit indice u tel que $p \nmid d_u$.

De même, il existe un plus petit indice v tel que $p \nmid e_v$.

Le coefficient de degré $u + v$ de $R \cdot S$ est :

$$(R \cdot S)_{u+v} = \sum_{k=0}^{u+v} d_k \cdot e_{u+v-k}$$

Dans cette somme :

- Pour $k < u$: $p \mid d_k$ par minimalité de u, donc $p \mid d_k \cdot e_{u+v-k}$.
- Pour $k > u$: alors $u + v - k < v$, donc $p \mid e_{u+v-k}$ par minimalité de v, donc $p \mid d_k \cdot e_{u+v-k}$.
- Pour $k = u$: le terme est $d_u \cdot e_v$, et $p \nmid d_u$, $p \nmid e_v$.

Comme p est irréductible dans un anneau factoriel (donc premier d'après le lemme de Gauss), $p \nmid d_u \cdot e_v$.

Ainsi, $p \nmid (R \cdot S)_{u+v}$, ce qui contredit $p \mid c(R \cdot S)$.

Finalement, $c(R \cdot S) = 1$, et donc $c(P \cdot Q) \sim c(P) \cdot c(Q)$.

Propriété 5.18 : (*Caractérisation des irréductibles des polynômes*)

Soit A un anneau factoriel et $K = \text{Frac}(A)$ son corps des fractions.

Les irréductibles de $A[x]$ sont :

① Les irréductibles de A (considérés comme polynômes constants).

② Les polynômes $P \in A[x]$ tels que $c(P) = 1$ et P est irréductible dans $K[x]$.

Preuve :

⊛ **Sens direct (⇒) :**

Soit $P \in A[x]$ irréductible.

★ **Si** $\deg(P) = 0$ **:**

Alors $P \in A$, et P est irréductible dans A (car sinon $P = a \cdot b$ avec a, b non inversibles dans A, donc dans $A[x]$ aussi, ce qui contredirait l'irréductibilité de P dans $A[x]$).

On est dans le cas i).

★ **Si** $\deg(P) \geqslant 1$ **:**

On écrit $P = c(P) \cdot R$ avec $R \in A[x]$.

On a $\deg(R) = \deg(P) \geqslant 1$.

Comme P est irréductible dans $A[x]$, soit $c(P)$ est inversible dans $A[x]$, soit R est inversible dans $A[x]$.

Mais R ne peut pas être inversible car $\deg(R) \geqslant 1$ (d'après la proposition 5.15).

Donc $c(P)$ est inversible dans A, ce qui signifie $c(P) \sim 1$, c'est-à-dire $c(P) = 1$ (à unité près).

Montrons que P est irréductible dans $K[x]$.

Supposons $P = S \cdot T$ avec $S, T \in K[x]$.

On peut écrire $S = \dfrac{1}{N} \cdot U$ et $T = \dfrac{1}{N'} \cdot V$ avec $N, N' \in A$ et $U, V \in A[x]$.

Alors :

$$N \cdot N' \cdot P = U \cdot V \quad \text{dans } A[x]$$

En prenant les contenus :

$$c(N \cdot N' \cdot P) = c(U \cdot V)$$

$$N \cdot N' \cdot c(P) = c(U) \cdot c(V)$$

$$N \cdot N' = c(U) \cdot c(V)$$

Donc :

$$P = \frac{1}{N \cdot N'} \cdot U \cdot V = \frac{1}{c(U) \cdot c(V)} \cdot U \cdot V = \left(\frac{U}{c(U)}\right) \cdot \left(\frac{V}{c(V)}\right)$$

où $\dfrac{U}{c(U)}$ et $\dfrac{V}{c(V)}$ sont dans $A[x]$ (car leurs coefficients sont dans A après division par le contenu).

Comme P est irréductible dans $A[x]$, soit $\dfrac{U}{c(U)}$ soit $\dfrac{V}{c(V)}$ est inversible dans $A[x]$.

Donc $\deg(U) = 0$ ou $\deg(V) = 0$, ce qui implique $\deg(S) = 0$ ou $\deg(T) = 0$.

Ainsi, S ou T est inversible dans $K[x]$.

Finalement, P est irréductible dans $K[x]$.

⊛ **Sens réciproque ($\Leftarrow$) :**

★ **Cas ① :**

Soit $P = a \in A$ avec a irréductible dans A.

Montrons que P est irréductible dans $A[x]$.

D'après la proposition 5.15, a n'est pas inversible dans $A[x]$ (car a n'est pas inversible dans A).

Soient $Q, R \in A[x]$ tels que $a = Q \cdot R$.

En prenant les degrés, on obtient :

$$\deg(Q) + \deg(R) = \deg(a) = 0$$

Comme les degrés sont des entiers positifs ou nuls, on a nécessairement :

$$\deg(Q) = 0 \quad \text{et} \quad \deg(R) = 0$$

Ainsi, Q et R sont des polynômes constants, c'est-à-dire $Q, R \in A$.

Comme $a = Q \cdot R$ dans A et que a est irréductible dans A, l'un des deux éléments, Q ou R, est inversible dans A.

D'après la proposition 5.15, Q ou R est donc inversible dans $A[x]$.

Finalement, a est irréductible dans $A[x]$.

★ **Cas ② :**

Soit $P \in A[x]$ tel que $c(P) = 1$ et P irréductible dans $K[x]$.

Comme $\deg(P) \geqslant 1$, P n'est pas inversible dans $A[x]$ (d'après la proposition 5.15).

Soit $P = Q \cdot R$ avec $Q, R \in A[x]$.

Comme P est irréductible dans $K[x]$, soit Q soit R (par exemple Q) est inversible dans $K[x]$.

Donc $\deg(Q) = 0$, c'est-à-dire $Q \in A$, disons $Q = b$.

Alors $P = b \cdot R$, donc $b \mid c(P) = 1$.

Ainsi, b est inversible dans A, donc Q est inversible dans $A[x]$.

Finalement, P est irréductible dans $A[x]$.

Théorème 5.19 : (*Factorialité de l'anneau des polynômes*)

Soit A un anneau commutatif unitaire intègre.

Si A est factoriel, alors $A[x]$ est factoriel.

Preuve :

Supposons que A est factoriel. Soit $K = \mathrm{Frac}(A)$ son corps des fractions.

① **Existence de la décomposition :**

Soit $P \in A[x]$, $P \neq 0$.

On écrit $P = c(P) \cdot R$ avec $R \in A[x]$ et $c(R) = 1$.

Comme A est factoriel, on peut décomposer le contenu :

$$c(P) = u \cdot p_1 \cdots p_k$$

où $u \in U(A)$ et les p_i sont irréductibles dans A.

Comme $c(R) = 1$, on a $R \in K[x]$ (en fait $R \in A[x]$ mais on le voit dans $K[x]$).

Or K est un corps, donc $K[x]$ est principal, donc factoriel.

On peut donc décomposer R dans $K[x]$:

$$R = \lambda \cdot R_1 \cdots R_m$$

où $\lambda \in K$ et les R_i sont irréductibles dans $K[x]$.

Écrivons $\lambda = \dfrac{a}{b}$ avec $a, b \in A$.

Pour chaque R_i, on peut écrire $R_i = \dfrac{1}{N_i} \cdot S_i$ avec $N_i \in A$ et $S_i \in A[x]$.

Alors :

$$R = \frac{a}{b} \cdot \frac{1}{N_1} \cdot S_1 \cdots \frac{1}{N_m} \cdot S_m$$

donc :

$$b \cdot N_1 \cdots N_m \cdot R = a \cdot S_1 \cdots S_m$$

En prenant les contenus :

$$b \cdot N_1 \cdots N_m \cdot c(R) = a \cdot c(S_1) \cdots c(S_m)$$

Comme $c(R) = 1$:

$$b \cdot N_1 \cdots N_m = a \cdot c(S_1) \cdots c(S_m)$$

Donc :

$$\begin{aligned} R &= \frac{a}{b \cdot N_1 \cdots N_m} \cdot S_1 \cdots S_m \\ &= \frac{1}{c(S_1) \cdots c(S_m)} \cdot S_1 \cdots S_m \\ &= \left(\frac{S_1}{c(S_1)}\right) \cdots \left(\frac{S_m}{c(S_m)}\right) \end{aligned}$$

Chaque $\dfrac{S_i}{c(S_i)}$ est un polynôme de $A[x]$ de contenu 1, irréductible dans $K[x]$, donc irréductible dans $A[x]$ (d'après la proposition 5.18, cas ii)).

Finalement :

$$P = c(P) \cdot R = \underbrace{u}_{\text{inversible}} \cdot \underbrace{p_1 \cdots p_k}_{\text{irréductibles de type ①}} \cdot \underbrace{\left(\frac{S_1}{c(S_1)}\right) \cdots \left(\frac{S_m}{c(S_m)}\right)}_{\text{irréductibles de type ②}}$$

Ainsi, P admet une décomposition en irréductibles dans $A[x]$.

② **Unicité de la décomposition :**

Soit $P \in A[x]$, $P \neq 0$, avec deux décompositions :

$$P = u \cdot P_1 \cdots P_m \cdot P_{m+1} \cdots P_n = v \cdot Q_1 \cdots Q_{m'} \cdot Q_{m'+1} \cdots Q_{n'}$$

où $u, v \in U(A)$, les $P_1, \ldots, P_m$ et $Q_1, \ldots, Q_{m'}$ sont des irréductibles de type ① (dans A), et les $P_{m+1}, \ldots, P_n$ et $Q_{m'+1}, \ldots, Q_{n'}$ sont des irréductibles de type ②.

En prenant les contenus :

$$\begin{aligned} c(P) &= c\left(u \cdot P_1 \cdots P_m \cdot P_{m+1} \cdots P_n\right) \\ &= u \cdot P_1 \cdots P_m \cdot c\left(P_{m+1} \cdots P_n\right) \\ &= u \cdot P_1 \cdots P_m \cdot c(P_{m+1}) \cdots c(P_n) \\ &= u \cdot P_1 \cdots P_m \end{aligned}$$

car $c(P_i) = 1$ pour $i > m$.

De même, $c(P) = v \cdot Q_1 \cdots Q_{m'}$.

Comme A est factoriel, la décomposition de $c(P)$ dans A est essentiellement unique :

$$m' = m \quad \text{et} \quad Q_i \sim P_{\sigma(i)} \quad \text{pour } i \in \{1, \ldots, m\}$$

Il reste à montrer l'unicité pour les facteurs de type ②.

On a :

$$\frac{1}{c(P)} \cdot P = P_{m+1} \cdots P_n = Q_{m+1} \cdots Q_{n'}$$

où ces polynômes sont irréductibles dans $K[x]$.

Or $K[x]$ est principal, donc factoriel.

La décomposition dans $K[x]$ est donc essentiellement unique :

$$n - m = n' - m' \quad \text{donc} \quad n = n'$$

À permutation près, $Q_i = k_i \cdot P_i$ avec $k_i = \dfrac{a_i}{b_i} \in K$.

Donc $b_i \cdot Q_i = a_i \cdot P_i$.

En prenant les contenus :

$$b_i = b_i \cdot c(Q_i) = c(b_i \cdot Q_i) = c(a_i \cdot P_i) = a_i \cdot c(P_i) = a_i$$

Donc $a_i = b_i$, ce qui implique $k_i = 1$.

Ainsi, $Q_i = P_i$ pour tout $i > m$.

Finalement, la décomposition de P dans $A[x]$ est essentiellement unique.

Donc $A[x]$ est factoriel.

Corollaire 5.20 : (*Factorialité de l'anneau des polynômes à plusieurs indéterminées*)

Soit A un anneau factoriel.

Alors $A[x_1, \ldots, x_m]$ est factoriel.

Preuve :

Par récurrence sur m.

On utilise l'isomorphisme :

$$A[x_1, \ldots, x_{m+1}] = (A[x_1, \ldots, x_m])[x_{m+1}]$$

Corollaire 5.21 : (*Exemples d'anneaux factoriels*)

Les anneaux suivants sont factoriels :

- $\mathbb{Z}[x_1,\ldots,x_m]$,
- $K[x_1,\ldots,x_m]$ où K est un corps commutatif.

Remarque :

- $\mathbb{Z}[x]$ n'est pas principal.
- $K[x_1,\ldots,x_m]$ n'est pas principal pour $m \geqslant 2$.

Chapitre 6

Localisation

La localisation est un procédé algébrique qui permet de construire un nouvel anneau à partir d'un anneau A et d'un sous-monoïde multiplicatif S, en rendant inversibles tous les éléments de S.
Cette construction généralise la formation du corps des fractions d'un anneau intègre et joue un rôle fondamental en géométrie algébrique pour étudier les propriétés locales des anneaux.

Définition 6.1 : (*Sous-monoïde multiplicatif*)

Soit A un anneau commutatif unitaire.

On dit qu'une partie S de A est un ***sous-monoïde multiplicatif*** de A si elle vérifie les propriétés suivantes :

- $1_A \in S$,
- Pour tous $(s, s') \in S^2$, on a $s \cdot s' \in S$ (stabilité par multiplication),
- $0_A \notin S$.

Lemme 6.2 : (*Relation d'équivalence pour la localisation*)

Soit A un anneau commutatif unitaire et S un sous-monoïde multiplicatif de A.

On définit sur $A \times S$ la relation $\mathcal{R}$ par :

$$(a, s)\,\mathcal{R}\,(a', s') \iff (\exists s'' \in S), \quad s'' \cdot a \cdot s' = s'' \cdot a' \cdot s$$

Alors $\mathcal{R}$ est une relation d'équivalence sur $A \times S$.

Preuve :

Montrons que $\mathcal{R}$ est une relation d'équivalence en vérifiant les trois propriétés : réflexivité, symétrie et transitivité.

- **Réflexivité :**

  Soit $(a, s) \in A \times S$.

  Comme $1_A \in S$, on a :

  $$1_A \cdot a \cdot s = 1_A \cdot a \cdot s$$

  donc

  $$(a, s)\mathcal{R}\,(a, s)$$

  La relation $\mathcal{R}$ est donc réflexive.

- **Symétrie :**

  Soient $(a, s), (a', s') \in A \times S$ tels que $(a, s)\,\mathcal{R}\,(a', s')$.

  Il existe $s'' \in S$ tel que :

  $$s'' \cdot a \cdot s' = s'' \cdot a' \cdot s$$

  Par commutativité de A, on a également :

  $$s'' \cdot a' \cdot s = s'' \cdot a \cdot s'$$

Donc

$$(a', s') \mathcal{R} (a, s)$$

La relation $\mathcal{R}$ est donc symétrique.

⊛ **Transitivité :**

Soient $(a, s), (b, t), (c, u) \in A \times S$ tels que $(a, s) \mathcal{R} (b, t)$ et $(b, t) \mathcal{R} (c, u)$.

Il existe $s_1 \in S$ et $s_2 \in S$ tels que :

$$s_1 \cdot a \cdot t = s_1 \cdot b \cdot s$$

$$s_2 \cdot b \cdot u = s_2 \cdot c \cdot t$$

Posons $s_3 = s_1 \cdot s_2 \cdot t$.

Comme S est stable par multiplication et que $s_1, s_2, t \in S$, on a $s_3 \in S$.

Calculons $s_3 \cdot a \cdot u$:

$$\begin{aligned} s_3 \cdot a \cdot u &= s_1 \cdot s_2 \cdot t \cdot a \cdot u \\ &= s_1 \cdot s_2 \cdot a \cdot t \cdot u \\ &= s_2 \cdot \underbrace{(s_1 \cdot a \cdot t)}_{= s_1 \cdot b \cdot s} \cdot u \\ &= s_2 \cdot s_1 \cdot b \cdot s \cdot u \\ &= s_1 \cdot s \cdot \underbrace{(s_2 \cdot b \cdot u)}_{= s_2 \cdot c \cdot t} \\ &= s_1 \cdot s \cdot s_2 \cdot c \cdot t \\ &= (s_1 \cdot s_2 \cdot t) \cdot c \cdot s \\ &= s_3 \cdot c \cdot s \end{aligned}$$

Ainsi, $s_3 \cdot a \cdot u = s_3 \cdot c \cdot s$ avec $s_3 \in S$.

Donc

$$(a, s) \mathcal{R} (c, u)$$

La relation $\mathcal{R}$ est donc transitive.

Finalement, $\mathcal{R}$ est une relation d'équivalence sur $A \times S$.

Définition 6.3 : (*Localisation d'un anneau en une partie*)

Soit A un anneau commutatif unitaire et S un sous-monoïde multiplicatif de A.

On note $S^{-1}A$ l'ensemble quotient de $A \times S$ par la relation d'équivalence $\mathcal{R}$:

$$S^{-1}A = (A \times S) / \mathcal{R} = \left\{ \overline{(a, s)} \;\middle|\; a \in A,\ s \in S \right\}$$

L'ensemble $S^{-1}A$ est appelé ***localisé de*** A ***en*** S ou encore la ***localisation de*** A ***en*** S.

Théorème 6.4 : (*Structure d'anneau du localisé*)

Soit A un anneau commutatif unitaire et S un sous-monoïde multiplicatif de A.

On définit sur $S^{-1}A$ les opérations suivantes :

$$\overline{(a,s)} + \overline{(a',s')} = \overline{(a\cdot s' + a'\cdot s,\ s\cdot s')}$$

$$\overline{(a,s)} \cdot \overline{(a',s')} = \overline{(a\cdot a',\ s\cdot s')}$$

Ces opérations sont bien définies et font de $S^{-1}A$ un anneau commutatif unitaire.

L'application $i_{S,A} : A \longrightarrow S^{-1}A$ définie par :

$$a \longmapsto \overline{(a,1)}$$

est un morphisme d'anneaux unitaires appelé ***morphisme de localisation***.

Preuve :

① **L'addition est bien définie :**

Soient $\overline{(a,s)} = \overline{(b,t)}$ et $\overline{(a',s')} = \overline{(c,u)}$.

On veut montrer que $\overline{(a\cdot s' + a'\cdot s, s\cdot s')} = \overline{(b\cdot u + c\cdot t, t\cdot u)}$.

Il existe $s_1 \in S$ et $s_2 \in S$ tels que :

$$s_1 \cdot a \cdot t = s_1 \cdot b \cdot s$$

$$s_2 \cdot a' \cdot u = s_2 \cdot c \cdot s'$$

Posons $s_3 = s_1 \cdot s_2 \in S$.

Calculons :

$$\begin{aligned}
s_3 \cdot \left(a\cdot s' + a'\cdot s\right)\cdot t\cdot u &= s_3\cdot a\cdot s'\cdot t\cdot u + s_3\cdot a'\cdot s\cdot t\cdot u \\
&= s_1\cdot s_2\cdot a\cdot s'\cdot t\cdot u + s_1\cdot s_2\cdot a'\cdot s\cdot t\cdot u \\
&= (s_1\cdot a\cdot t)\cdot s_2\cdot s'\cdot u + s_1\cdot\left(s_2\cdot a'\cdot u\right)\cdot s\cdot t \\
&= (s_1\cdot b\cdot s)\cdot s_2\cdot s'\cdot u + s_1\cdot\left(s_2\cdot c\cdot s'\right)\cdot s\cdot t \\
&= s_1\cdot s_2\cdot b\cdot s\cdot s'\cdot u + s_1\cdot s_2\cdot c\cdot s'\cdot s\cdot t \\
&= s_1\cdot s_2\cdot (b\cdot u + c\cdot t)\cdot s\cdot s' \\
&= s_3\cdot (b\cdot u + c\cdot t)\cdot s\cdot s'
\end{aligned}$$

Donc $\left(a\cdot s' + a'\cdot s, s\cdot s'\right)\mathcal{R}\,(b\cdot u + c\cdot t, t\cdot u)$.

Ainsi :

$$\overline{(a\cdot s' + a'\cdot s, s\cdot s')} = \overline{(b\cdot u + c\cdot t, t\cdot u)}$$

② **La multiplication est bien définie :**

On a :

$$\begin{aligned}
s_3\cdot\left(a\cdot a'\right)\cdot t\cdot u &= s_1\cdot s_2\cdot a\cdot a'\cdot t\cdot u \\
&= (s_1\cdot a\cdot t)\cdot\left(s_2\cdot a'\cdot u\right) \\
&= (s_1\cdot b\cdot s)\cdot\left(s_2\cdot c\cdot s'\right) \\
&= s_1\cdot s_2\cdot b\cdot c\cdot s\cdot s'
\end{aligned}$$

$$= s_3 \cdot (b \cdot c) \cdot s \cdot s'$$

Donc $(a \cdot a', s \cdot s') \mathcal{R} (b \cdot c, t \cdot u)$.

Ainsi :

$$\overline{(a \cdot a', s \cdot s')} = \overline{(b \cdot c, t \cdot u)}$$

③ **L'addition est associative :**

$$\begin{aligned}
\left(\overline{(a,s)} + \overline{(b,t)}\right) + \overline{(c,u)} &= \overline{(a \cdot t + b \cdot s, s \cdot t)} + \overline{(c,u)} \\
&= \overline{((a \cdot t + b \cdot s) \cdot u + c \cdot s \cdot t, s \cdot t \cdot u)} \\
&= \overline{(a \cdot t \cdot u + b \cdot s \cdot u + c \cdot s \cdot t, s \cdot t \cdot u)} \\
&= \overline{(a \cdot t \cdot u + (b \cdot u + c \cdot t) \cdot s, s \cdot (t \cdot u))} \\
&= \overline{(a,s)} + \overline{(b \cdot u + c \cdot t, t \cdot u)} \\
&= \overline{(a,s)} + \left(\overline{(b,t)} + \overline{(c,u)}\right)
\end{aligned}$$

④ **L'addition est commutative :**

$$\begin{aligned}
\overline{(a,s)} + \overline{(b,t)} &= \overline{(a \cdot t + b \cdot s, s \cdot t)} \\
&= \overline{(b \cdot s + a \cdot t, t \cdot s)} \\
&= \overline{(b,t)} + \overline{(a,s)}
\end{aligned}$$

⑤ **Élément neutre pour l'addition :**

$$\begin{aligned}
\overline{(0,1)} + \overline{(a,s)} &= \overline{(a,s)} + \overline{(0,1)} \\
&= \overline{(a \cdot 1 + 0 \cdot s, s \cdot 1)} \\
&= \overline{(a,s)}
\end{aligned}$$

Donc il existe $0_{S^{-1}A} = \overline{(0_A, 1_A)}$.

⑥ **Symétrique pour l'addition :**

$$\begin{aligned}
\overline{(-a,s)} + \overline{(a,s)} &= \overline{(a,s)} + \overline{(-a,s)} \\
&= \overline{(a \cdot s + (-a) \cdot s, s \cdot s)} \\
&= \overline{(0, s^2)} \\
&= \overline{(0,1)}
\end{aligned}$$

car $(0, s^2) \mathcal{R} (0,1)$ puisque $1 \cdot 0 \cdot 1 = 1 \cdot s^2 \cdot 0$.

Ainsi, $\overline{(-a,s)}$ est l'opposé de $\overline{(a,s)}$.

Donc $\left(S^{-1}A, +\right)$ est un groupe abélien.

⑦ **La multiplication est associative :**

$$\begin{aligned}
\left(\overline{(a,s)} \cdot \overline{(b,t)}\right) \cdot \overline{(c,u)} &= \overline{(a \cdot b, s \cdot t)} \cdot \overline{(c,u)} \\
&= \overline{((a \cdot b) \cdot c, (s \cdot t) \cdot u)} \\
&= \overline{(a \cdot (b \cdot c), s \cdot (t \cdot u))}
\end{aligned}$$

$$= \overline{(a,s)} \cdot \overline{(b \cdot c, t \cdot u)}$$
$$= \overline{(a,s)} \cdot \left(\overline{(b,t)} \cdot \overline{(c,u)}\right)$$

⑧ **La multiplication est commutative :**

$$\overline{(a,s)} \cdot \overline{(b,t)} = \overline{(a \cdot b, s \cdot t)}$$
$$= \overline{(b \cdot a, t \cdot s)}$$
$$= \overline{(b,t)} \cdot \overline{(a,s)}$$

⑨ **Élément neutre pour la multiplication :**

$$\overline{(1,1)} \cdot \overline{(a,s)} = \overline{(a,s)} \cdot \overline{(1,1)}$$
$$= \overline{(a \cdot 1, s \cdot 1)}$$
$$= \overline{(a,s)}$$

Donc il existe $1_{S^{-1}A} = \overline{(1_A, 1_A)}$.

⑩ **Distributivité :**

$$\overline{(a,s)} \cdot \left(\overline{(b,t)} + \overline{(c,u)}\right) = \overline{(a,s)} \cdot \overline{(b \cdot u + c \cdot t, t \cdot u)}$$
$$= \overline{(a \cdot b \cdot u + a \cdot c \cdot t, s \cdot t \cdot u)}$$

et :

$$\overline{(a,s)} \cdot \overline{(b,t)} + \overline{(a,s)} \cdot \overline{(c,u)} = \overline{(a \cdot b, s \cdot t)} + \overline{(a \cdot c, s \cdot u)}$$
$$= \overline{\left(a \cdot b \cdot s \cdot u + a \cdot c \cdot s \cdot t, s^2 \cdot t \cdot u\right)}$$

Il suffit de démontrer que :

$$(a \cdot b \cdot u + a \cdot c \cdot t, s \cdot t \cdot u) \mathcal{R} \left(a \cdot b \cdot s \cdot u + a \cdot c \cdot s \cdot t, s^2 \cdot t \cdot u\right)$$

c'est-à-dire qu'il existe $s'' \in S$ tel que :

$$s'' \cdot (a \cdot b \cdot u + a \cdot c \cdot t) \cdot s^2 \cdot t \cdot u = s'' \cdot (a \cdot b \cdot s \cdot u + a \cdot c \cdot s \cdot t) \cdot (s \cdot t \cdot u)$$

$s'' = 1$ convient.

Donc $\left(S^{-1}A, +, \cdot\right)$ est un anneau commutatif unitaire.

⑪ $i_{S,A}$ **est un morphisme d'anneaux unitaires :**

Soit $i = i_{S,A} : A \longrightarrow S^{-1}A$ définie par $i(a) = \overline{(a,1)}$.

⊛ Pour tous $a, b \in A$:

$$i(a) + i(b) = \overline{(a,1)} + \overline{(b,1)}$$
$$= \overline{(a \cdot 1 + b \cdot 1, 1 \cdot 1)}$$
$$= \overline{(a+b,1)}$$
$$= i(a+b)$$

⊛ Pour tous $a, b \in A$:

$$\begin{aligned} i(a) \cdot i(b) &= \overline{(a,1)} \cdot \overline{(b,1)} \\ &= \overline{(a \cdot b, 1 \cdot 1)} \\ &= \overline{(a \cdot b, 1)} \\ &= i(a \cdot b) \end{aligned}$$

⊛ $i(1_A) = \overline{(1_A, 1_A)} = 1_{S^{-1}A}$.

Donc i est un morphisme d'anneaux unitaires.

Propriété 6.5 : (*Propriétés du morphisme de localisation*)

Soit A un anneau commutatif unitaire et S un sous-monoïde multiplicatif de A.

① Chaque élément de $i_{S,A}(S)$ est inversible dans $S^{-1}A$.

② Le noyau de $i_{S,A}$ est donné par :

$$\operatorname{Ker}\left(i_{S,A}\right) = \{a \in A \mid (\exists s \in S),\ s \cdot a = 0_A\}$$

③ Si A est intègre, alors $i_{S,A}$ est injectif.

Preuve :

① Soit $s \in S$.

On a $i_{S,A}(s) = \overline{(s,1)}$.

Considérons $\overline{(1,s)} \in S^{-1}A$.

Alors :

$$\begin{aligned} \overline{(s,1)} \cdot \overline{(1,s)} &= \overline{(s \cdot 1, 1 \cdot s)} \\ &= \overline{(s,s)} \end{aligned}$$

Or

$$\overline{(s,s)} = \overline{(1,1)} = 1_{S^{-1}A} \qquad \text{car } 1 \cdot s \cdot 1 = 1 \cdot 1 \cdot s.$$

Donc $\overline{(s,1)}$ est inversible d'inverse $\overline{(1,s)}$.

② On a :

$$\begin{aligned} a \in \operatorname{Ker}\left(i_{S,A}\right) &\iff i_{S,A}(a) = \overline{(0_A,1)} \\ &\iff \overline{(a,1)} = \overline{(0_A,1)} \\ &\iff (\exists s \in S),\ s \cdot a \cdot 1 = s \cdot 0_A \cdot 1 \\ &\iff (\exists s \in S),\ s \cdot a = 0_A \end{aligned}$$

③ Supposons que A est intègre.

Soit $a \in \operatorname{Ker}\left(i_{S,A}\right)$.

Il existe $s \in S$ tel que $s \cdot a = 0_A$.

Comme A est intègre et $s \in S$ (donc $s \neq 0_A$ car $0_A \notin S$), on a nécessairement $a = 0_A$.

Ainsi, $\operatorname{Ker}\left(i_{S,A}\right) = \{0_A\}$, donc $i_{S,A}$ est injectif.

Exemple :

① **Corps des fractions d'un anneau intègre :**

Soit A un anneau commutatif intègre.

On prend $S = A \setminus \{0_A\}$.

Le localisé $S^{-1}A$ est noté $\mathrm{Frac}(A)$ et appelé corps des fractions de A.

C'est un corps.

Cas particulier : $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

② **Localisation en un idéal premier :**

Soit P un idéal premier de A.

On prend $S = A \setminus P$.

Le localisé $S^{-1}A$ est noté A_P et appelé localisé de A en P.

③ **Anneau des nombres décimaux :**

Soit $A = \mathbb{Z}$.

On prend $S = \{10^n \mid n \in \mathbb{N}\}$.

Le localisé $S^{-1}A$ est l'anneau $\mathbb{D}$ des nombres décimaux :

$$S^{-1}A = \mathbb{D} = \left\{ \frac{a}{10^n} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N} \right\}$$

Lemme 6.6 : (*Intégrité du localisé*)

Soit A un anneau commutatif unitaire intègre et S un sous-monoïde multiplicatif de A.

Alors $S^{-1}A$ est un anneau intègre.

Preuve :

Soient $(x, y) \in (S^{-1}A)^2$ tels que $x \cdot y = 0_{S^{-1}A}$.

On écrit $x = \overline{(a, s)}$ avec $a \in A$, $s \in S$.

Et $y = \overline{(b, t)}$ avec $b \in A$, $t \in S$.

On a $x \cdot y = 0_{S^{-1}A}$, donc :

$$\overline{(a \cdot b, s \cdot t)} = \overline{(0_A, 1_A)}$$

Il existe $s' \in S$ tel que :

$$s' \cdot a \cdot b \cdot 1_A = s' \cdot 0_A \cdot s \cdot t = 0_A$$

Donc :

$$\underbrace{s'}_{\in S} \cdot a \cdot b = 0_A$$

Or $s' \neq 0$ (car $0_A \notin S$) et A est intègre, donc $a \cdot b = 0_A$.

Ainsi $a = 0_A$ ou $b = 0_A$.

⊛ Si $a = 0_A$, alors $x = \overline{(0_A, s)} = \overline{(0_A, 1_A)} = 0_{S^{-1}A}$.

⊛ De même, si $b = 0_A$, alors $y = 0_{S^{-1}A}$.

Reste à montrer que $1_{S^{-1}A} \neq 0_{S^{-1}A}$ (ce qui est vrai car $0_A \notin S$).

Théorème 6.7 : (*Localisation d'un anneau principal*)

Soit A un anneau commutatif unitaire principal et S un sous-monoïde multiplicatif de A.

Alors $S^{-1}A$ est un anneau principal.

Preuve :

A est principal, donc A est intègre, donc (d'après le lemme 6.6) $S^{-1}A$ est intègre.

Soit $\mathcal{J}$ un idéal de $S^{-1}A$.

$i^{-1}(\mathcal{J})$ est un idéal de A.

A est principal, donc il existe $a \in A$ tel que :

$$i^{-1}(\mathcal{J}) = A \cdot a$$

On a $a = 1_A \cdot a \in A \cdot a = i^{-1}(\mathcal{J})$.

Donc $i(a) \in \mathcal{J}$.

Ainsi $\left(S^{-1}A\right) \cdot i(a) \subset \mathcal{J}$.

Soit $x \in \mathcal{J}$, avec $x = \overline{(a', s)}$, $a' \in A$, $s \in S$.

Comme $\mathcal{J}$ est un idéal de $S^{-1}A$ et que $\overline{(s, 1_A)} \in S^{-1}A$, on a :

$$x \cdot \overline{(s, 1_A)} \in \mathcal{J}$$

Calculons ce produit :

$$\begin{aligned} x \cdot \overline{(s, 1_A)} &= \overline{(a', s)} \cdot \overline{(s, 1_A)} \\ &= \overline{(a' \cdot s, s \cdot 1_A)} \\ &= \overline{(a' \cdot s, s)} \\ &= \overline{(a', 1_A)} \\ &= i(a') \end{aligned}$$

Donc $i(a') \in \mathcal{J}$, ce qui implique $a' \in i^{-1}(\mathcal{J}) = A \cdot a$.

Il existe $b \in A$ tel que $a' = b \cdot a$.

Alors :

$$\begin{aligned} x &= \overline{(a', s)} \\ &= \overline{(b \cdot a, s)} \\ &= \overline{(b, s)} \cdot \overline{(a, 1_A)} \\ &= \overline{(b, s)} \cdot i(a) \\ &\in \left(S^{-1}A\right) \cdot i(a) \end{aligned}$$

Donc $\mathcal{J} \subset \left(S^{-1}A\right) \cdot i(a)$.

Finalement :

$$\mathcal{J} = \left(S^{-1}A\right) \cdot i(a)$$

Donc tout idéal de $S^{-1}A$ est principal.

Ainsi $S^{-1}A$ est principal.

Théorème 6.8 : (*Corps des fractions*)

Soit A un anneau commutatif unitaire intègre.

On pose $S = A \setminus \{0_A\}$ et $K = \mathrm{Frac}(A) = S^{-1}A$.

Alors K est un corps, appelé ***corps des fractions*** de A.

De plus, le morphisme de localisation $i = i_{S,A}$ défini par :

$$\begin{array}{rccc} i_{S,A}: & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & \overline{(a,1)} \end{array}$$

est injectif (car A est intègre).

Et on a l'identification :

$$K = \left\{ \frac{a}{b} \;\middle|\; a \in A,\ b \in A,\ b \neq 0_A \right\}$$

Preuve :

La preuve se déroule en plusieurs étapes.

① **Montrons que K est un corps :**

Soit $x \in K$ tel que $x \neq 0_K$.

On peut écrire $x = \overline{(a,s)}$ avec $a \in A$ et $s \in S$.

Comme $x \neq 0_K = \overline{(0_A,1)}$, on a $a \neq 0_A$.

Donc $a \in S$ (car $S = A \setminus \{0_A\}$).

Soit $y = \overline{(s,a)} \in K$.

Alors :

$$\begin{aligned} y \cdot x = x \cdot y &= \overline{(a,s)} \cdot \overline{(s,a)} \\ &= \overline{(a \cdot s, s \cdot a)} \end{aligned}$$

donc

$$y \cdot x = \overline{(1_A, 1_A)} = 1_K$$

Donc x est inversible dans K.

② **Expression des éléments de K sous forme de fraction :**

Soient $a \in A$ et $b \in A \setminus \{0_A\}$.

Dans K :

$$\frac{i(a)}{i(b)} = i(a) \cdot i(b)^{-1} = \overline{(a,1_A)} \cdot \left(\overline{(b,1_A)}\right)^{-1}$$

Donc :

$$K = \left\{ \frac{i(a)}{i(b)} \;\middle|\; a \in A,\ b \in A,\ b \neq 0_A \right\}$$

③ **Identification de A avec $i(A)$:**

Maintenant on identifie chaque $x \in A$ avec $i(x)$ (c'est permis car i est injectif).

Et on a :

$$K = \left\{ \frac{a}{b} \;\middle|\; a \in A,\ b \in A,\ b \neq 0_A \right\}$$

Exemple :

Anneau des nombres décimaux — suite

Reprenons l'exemple précédent sur l'**anneau des nombres décimaux** :

Soit $A = \mathbb{Z}$.

On prend $S = \{10^n \mid n \in \mathbb{N}\}$.

Le localisé $S^{-1}A$ est l'anneau $\mathbb{D}$ des nombres décimaux :

$$S^{-1}A = \mathbb{D} = \left\{ \frac{a}{10^n} \;\middle|\; a \in \mathbb{Z},\ n \in \mathbb{N} \right\}$$

$S^{-1}A \simeq \mathbb{D}$ (anneau des nombres décimaux) via l'isomorphisme :

$$\overline{(a, 10^n)} \longmapsto \frac{a}{10^n}$$

D'après le théorème 6.7, $S^{-1}A$ est principal, donc $\mathbb{D}$ est principal.

Théorème 6.9 : (*Propriétés du localisé en un idéal premier*)

Soit A un anneau commutatif unitaire et P un idéal premier de A.

On pose $S = A \setminus P$ et $A_P = S^{-1}A$.

On définit :

$$\mathfrak{m}_P = \left\{ \overline{(a, s)} \;\middle|\; a \in P,\ s \in S \right\}$$

Alors :

① $\mathfrak{m}_P$ est un idéal strict de A_P (c'est-à-dire $\mathfrak{m}_P \neq A_P$).

② Tout idéal strict de A_P est contenu dans $\mathfrak{m}_P$. En particulier, $\mathfrak{m}_P$ est l'unique idéal maximal de A_P.

③ On a l'isomorphisme :

$$\frac{A_P}{\mathfrak{m}_P} \simeq \mathrm{Frac}\,(A/P)$$

Preuve :

La preuve se déroule en trois parties correspondant aux trois assertions.

① **$\mathfrak{m}_P$ est un idéal strict de A_P :**

⊛ **$\mathfrak{m}_P$ est non vide :**

On a $0_{A_P} = \overline{(0_A, 1_A)} \in \mathfrak{m}_P$ car $0_A \in P$ et $1_A \in S$.

⊛ **Stabilité par soustraction :**

Soient $x, y \in \mathfrak{m}_P$.

On écrit $x = \overline{(a, s)}$ et $y = \overline{(a', s')}$ avec $a, a' \in P$ et $s, s' \in S$.

Alors :

$$\begin{aligned} x - y &= \overline{(a, s)} - \overline{(a', s')} \\ &= \overline{(a \cdot s' - a' \cdot s,\ s \cdot s')} \end{aligned}$$

Comme P est un idéal et $a, a' \in P$, on a $a \cdot s' - a' \cdot s \in P$.

Donc $x - y \in \mathfrak{m}_P$.

⊛ **Stabilité par multiplication par un élément de A_P :**

Soit $x = \overline{(a,s)} \in \mathfrak{m}_P$ avec $a \in P$ et $s \in S$.

Soit $z = \overline{(b,t)} \in A_P$ avec $b \in A$ et $t \in S$.

Alors :

$$x \cdot z = \overline{(a \cdot b, s \cdot t)}$$

Comme $a \in P$ et P est un idéal, on a $a \cdot b \in P$.

Donc $x \cdot z \in \mathfrak{m}_P$.

⊛ $\mathfrak{m}_P$ **est strict :**

Raisonnons par l'absurde en supposant que $\mathfrak{m}_P = A_P$.

Alors $1_{A_P} = \overline{(1_A, 1_A)} \in \mathfrak{m}_P$.

Il existe $a \in P$ et $s \in S$ tels que $\overline{(1_A, 1_A)} = \overline{(a,s)}$.

Il existe $s' \in S$ tel que :

$$s' \cdot 1_A \cdot s = s' \cdot a \cdot 1_A$$

donc

$$s' \cdot s = s' \cdot a$$

Or $s' \cdot s \in S$ (car S est stable par multiplication) et $s' \cdot a \in P$ (car $a \in P$ et P est un idéal).

Donc $s' \cdot s \in S \cap P = \emptyset$, contradiction.

Ainsi $\mathfrak{m}_P \neq A_P$.

② **Tout idéal strict de A_P est contenu dans $\mathfrak{m}_P$:**

Soit $\mathcal{J}$ un idéal strict de A_P et soit $x \in \mathcal{J}$.

On écrit $x = \overline{(a,s)}$ avec $a \in A$ et $s \in S$.

⊛ **Si $a \notin P$:**

Alors $a \in A \setminus P = S$.

Considérons $\overline{(s,a)} \in A_P$.

Comme $\mathcal{J}$ est un idéal et $x \in \mathcal{J}$, on a :

$$\begin{aligned} \overline{(s,a)} \cdot x &= \overline{(s,a)} \cdot \overline{(a,s)} \\ &= \overline{(s \cdot a, a \cdot s)} \\ &= \overline{(1_A, 1_A)} \\ &= 1_{A_P} \end{aligned}$$

Donc $1_{A_P} \in \mathcal{J}$, ce qui implique $\mathcal{J} = A_P$.

Contradiction avec l'hypothèse que $\mathcal{J}$ est strict.

⊛ **Donc $a \in P$:**

Ainsi $x = \overline{(a,s)} \in \mathfrak{m}_P$.

On a montré que $\mathcal{J} \subset \mathfrak{m}_P$.

⊛ **Unicité de l'idéal maximal :**

Supposons que $\mathfrak{m}_P \subset K$ où K est un idéal de A_P.

Si $K \neq A_P$, alors K est un idéal strict de A_P, donc $K \subset \mathfrak{m}_P$ d'après ce qui précède.

Ainsi $K = \mathfrak{m}_P$.

Donc $\mathfrak{m}_P$ est un idéal maximal de A_P.

Soit $\mathfrak{m}'$ un idéal maximal de A_P.

Comme $\mathfrak{m}'$ est maximal, $\mathfrak{m}' \neq A_P$, donc $\mathfrak{m}' \subset \mathfrak{m}_P$.

Par maximalité de $\mathfrak{m}'$, on a $\mathfrak{m}' = \mathfrak{m}_P$.

Ainsi $\mathfrak{m}_P$ est l'unique idéal maximal de A_P.

③ **Isomorphisme $\dfrac{A_P}{\mathfrak{m}_P} \simeq \mathrm{Frac}\,(A/P)$:**

Comme P est un idéal premier, A/P est un anneau intègre.

On note $j : A/P \longrightarrow \mathrm{Frac}\,(A/P)$ le morphisme de localisation canonique défini par $x \longmapsto x$.

On note $\pi : A_P \longrightarrow \dfrac{A_P}{\mathfrak{m}_P}$ la projection canonique définie par $y \longmapsto \overline{y}$.

On note $i = i_{S,A} : A \longrightarrow S^{-1}A = A_P$ le morphisme de localisation.

On définit $\theta = \pi \circ i : A \longrightarrow \dfrac{A_P}{\mathfrak{m}_P}$.

⊛ **Calcul du noyau de θ :**

Soit $y \in P$.

Alors $i(y) = \overline{(y, 1_A)} \in \mathfrak{m}_P$.

Donc $\theta(y) = \pi(i(y)) = 0_{\frac{A_P}{\mathfrak{m}_P}}$.

Ainsi $y \in \mathrm{Ker}(\theta)$, donc $P \subset \mathrm{Ker}(\theta)$.

Réciproquement, soit $a \in \mathrm{Ker}(\theta)$.

Alors $\theta(a) = 0_{\frac{A_P}{\mathfrak{m}_P}}$, donc $\pi(i(a)) = 0_{\frac{A_P}{\mathfrak{m}_P}}$.

Ainsi $i(a) = \overline{(a, 1_A)} \in \mathfrak{m}_P$.

Il existe $b \in P$ et $s \in S$ tels que $\overline{(a, 1_A)} = \overline{(b, s)}$.

Il existe $s' \in S$ tel que :

$$s' \cdot a \cdot s = s' \cdot b \cdot 1_A = s' \cdot b$$

Or $s' \cdot b \in P$ (car $b \in P$ et P est un idéal).

Donc $s \cdot s' \cdot a \in P$.

Comme $s \cdot s' \in S = A \setminus P$ et P est premier, on a $a \in P$.

Ainsi $\mathrm{Ker}(\theta) \subset P$.

Finalement :

$$\mathrm{Ker}(\theta) = P$$

⊛ **Factorisation par le noyau :**

D'après le premier théorème d'isomorphisme :

$$\frac{A}{P} = \frac{A}{\mathrm{Ker}(\theta)} \simeq \mathrm{Im}(\theta) \subset \frac{A_P}{\mathfrak{m}_P}$$

⊛ **Construction de l'isomorphisme λ :**

Soit $\lambda : \mathrm{Frac}(A/P) \longrightarrow \dfrac{A_P}{\mathfrak{m}_P}$ définie par :

$$\frac{\tilde{a}}{\tilde{b}} \longmapsto \frac{\theta(a)}{\theta(b)}$$

où $\tilde{a}$ et $\tilde{b}$ désignent les classes de a et b dans A/P.

★ **λ est bien définie :**

Montrons d'abord que $\theta(b) \neq 0_{\frac{A_P}{\mathfrak{m}_P}}$ dès que $b \notin P$.

Soit $b \in A$ tel que $b \notin P$.

Supposons par l'absurde que $\theta(b) = 0_{\frac{A_P}{\mathfrak{m}_P}}$.

Alors $\pi(i(b)) = 0_{\frac{A_P}{\mathfrak{m}_P}}$, donc $i(b) = \overline{(b, 1_A)} \in \mathfrak{m}_P$.

Par définition de $\mathfrak{m}_P$, il existe $a \in P$ et $s \in S$ tels que $\overline{(b, 1_A)} = \overline{(a, s)}$.

Il existe $s' \in S$ tel que :

$$s' \cdot b \cdot s = s' \cdot a \cdot 1_A = s' \cdot a$$

Or $s' \cdot a \in P$ (car $a \in P$ et P est un idéal).

Donc $s' \cdot s \cdot b \in P$.

Comme $s' \cdot s \in S = A \setminus P$ et P est un idéal premier, on en déduit que $b \in P$.

Contradiction avec $b \notin P$.

Ainsi $\theta(b) \neq 0_{\frac{A_P}{\mathfrak{m}_P}}$, et l'expression $\dfrac{\theta(a)}{\theta(b)}$ a bien un sens dans $\dfrac{A_P}{\mathfrak{m}_P}$ (qui est un corps car $\mathfrak{m}_P$ est maximal).

Montrons maintenant que λ ne dépend pas du choix des représentants.

Soient $\tilde{a}, \tilde{c} \in A/P$ et $\tilde{b}, \tilde{d} \in A/P \setminus \{0\}$ tels que :

$$\frac{\tilde{a}}{\tilde{b}} = \frac{\tilde{c}}{\tilde{d}}$$

dans $\mathrm{Frac}(A/P)$.

Cela signifie que $\tilde{a} \cdot \tilde{d} = \tilde{b} \cdot \tilde{c}$ dans A/P, c'est-à-dire :

$$a \cdot d - b \cdot c \in P$$

Donc $\theta(a \cdot d - b \cdot c) = 0_{\frac{A_P}{\mathfrak{m}_P}}$.

Comme θ est un morphisme d'anneaux :

$$\theta(a) \cdot \theta(d) - \theta(b) \cdot \theta(c) = 0_{\frac{A_P}{\mathfrak{m}_P}}$$

donc

$$\theta(a) \cdot \theta(d) = \theta(b) \cdot \theta(c)$$

En multipliant par $\theta(b)^{-1} \cdot \theta(d)^{-1}$ (qui existent car $\theta(b) \neq 0$ et $\theta(d) \neq 0$) :

$$\frac{\theta(a)}{\theta(b)} = \frac{\theta(c)}{\theta(d)}$$

Ainsi $\lambda\left(\frac{\tilde{a}}{\tilde{b}}\right) = \lambda\left(\frac{\tilde{c}}{\tilde{d}}\right)$.

Donc λ est bien définie.

★ **λ est un morphisme d'anneaux :**

Soient $\frac{\tilde{a}}{\tilde{b}}$ et $\frac{\tilde{c}}{\tilde{d}}$ deux éléments de $\mathrm{Frac}(A/P)$.

♣ **Additivité :**

$$\begin{aligned}\lambda\left(\frac{\tilde{a}}{\tilde{b}} + \frac{\tilde{c}}{\tilde{d}}\right) &= \lambda\left(\frac{\widetilde{a\cdot d + b\cdot c}}{\widetilde{b\cdot d}}\right)\\ &= \frac{\theta(a\cdot d + b\cdot c)}{\theta(b\cdot d)}\end{aligned}$$

Comme θ est un morphisme :

$$\begin{aligned}\lambda\left(\frac{\tilde{a}}{\tilde{b}} + \frac{\tilde{c}}{\tilde{d}}\right) &= \frac{\theta(a)\cdot\theta(d) + \theta(b)\cdot\theta(c)}{\theta(b)\cdot\theta(d)}\\ &= \frac{\theta(a)}{\theta(b)} + \frac{\theta(c)}{\theta(d)}\\ &= \lambda\left(\frac{\tilde{a}}{\tilde{b}}\right) + \lambda\left(\frac{\tilde{c}}{\tilde{d}}\right)\end{aligned}$$

♣ **Multiplicativité :**

$$\begin{aligned}\lambda\left(\frac{\tilde{a}}{\tilde{b}}\cdot\frac{\tilde{c}}{\tilde{d}}\right) &= \lambda\left(\frac{\widetilde{a\cdot c}}{\widetilde{b\cdot d}}\right)\\ &= \frac{\theta(a\cdot c)}{\theta(b\cdot d)}\end{aligned}$$

Comme θ est un morphisme :

$$\begin{aligned}\lambda\left(\frac{\tilde{a}}{\tilde{b}}\cdot\frac{\tilde{c}}{\tilde{d}}\right) &= \frac{\theta(a)\cdot\theta(c)}{\theta(b)\cdot\theta(d)}\\ &= \frac{\theta(a)}{\theta(b)}\cdot\frac{\theta(c)}{\theta(d)}\\ &= \lambda\left(\frac{\tilde{a}}{\tilde{b}}\right)\cdot\lambda\left(\frac{\tilde{c}}{\tilde{d}}\right)\end{aligned}$$

♣ **Unité :**

$$\lambda\left(\frac{\tilde{1}_A}{\tilde{1}_A}\right) = \frac{\theta(1_A)}{\theta(1_A)} = \frac{1_{\frac{A_P}{\mathfrak{m}_P}}}{1_{\frac{A_P}{\mathfrak{m}_P}}} = 1_{\frac{A_P}{\mathfrak{m}_P}}$$

Donc λ est un morphisme d'anneaux.

★ **λ est injectif :**

Soit $\frac{\tilde{a}}{\tilde{b}} \in \mathrm{Frac}(A/P)$ tel que $\lambda\left(\frac{\tilde{a}}{\tilde{b}}\right) = 0_{\frac{A_P}{\mathfrak{m}_P}}$.

Alors :

$$\frac{\theta(a)}{\theta(b)} = 0_{\frac{A_P}{\mathfrak{m}_P}}$$

donc

$$\theta(a) = 0_{\frac{A_P}{\mathfrak{m}_P}}$$

Ainsi $a \in \mathrm{Ker}(\theta) = P$.

Donc $\tilde{a} = 0$ dans A/P, ce qui implique :

$$\frac{\tilde{a}}{\tilde{b}} = 0$$

dans $\mathrm{Frac}(A/P)$.

Ainsi $\mathrm{Ker}(\lambda) = \{0\}$, donc λ est injectif.

⊛ **Surjectivité de λ :**

Soit $\alpha \in \dfrac{A_P}{\mathfrak{m}_P}$.

Il existe $u \in A_P$ tel que $\alpha = \pi(u)$.

On écrit $u = \overline{(a,s)}$ avec $a \in A$ et $s \in S$.

Alors :

$$\begin{aligned} u \cdot \overline{(s,1_A)} &= \overline{(a,s)} \cdot \overline{(s,1_A)} \\ &= \overline{(a \cdot s, s \cdot 1_A)} \\ &= \overline{(a \cdot s, s)} \\ &= \overline{(a,1_A)} \\ &= i(a) \end{aligned}$$

Donc :

$$u \cdot i(s) = i(a)$$

En appliquant π :

$$\pi(u) \cdot \pi(i(s)) = \pi(i(a))$$

$$\alpha \cdot \theta(s) = \theta(a)$$

Donc :

$$\begin{aligned} \alpha &= \frac{\theta(a)}{\theta(s)} \\ &= \lambda\left(\frac{\tilde{a}}{\tilde{s}}\right) \end{aligned}$$

Ainsi λ est surjective.

Finalement, λ est un isomorphisme et donc :

$$\frac{A_P}{\mathfrak{m}_P} \simeq \mathrm{Frac}\,(A/P)$$

Exemple :

Localisé de $\mathbb{Z}$ en un nombre premier p

Soit p un nombre premier.

L'idéal $P = p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$.

On pose $S = \mathbb{Z} \setminus p\mathbb{Z}$ et on note $\mathbb{Z}_{(p)} = \mathbb{Z}_{p\mathbb{Z}} = S^{-1}\mathbb{Z}$.

Soit $i = i_{S,\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}_{(p)}$ le morphisme de localisation.

D'après le théorème 6.9, on a :

⊛ $\mathbb{Z}_{(p)}$ admet un unique idéal maximal : $\mathfrak{m}_p = i(p)\mathbb{Z}_{(p)}$.

⊛ On a l'isomorphisme :

$$\frac{\mathbb{Z}_{(p)}}{\mathfrak{m}_p} \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$$

Propriété 6.10 : (*Sous-anneaux de Frac(B)*)

Soit B un anneau principal.

Si A est un anneau tel que $B \subset A \subset \mathrm{Frac}(B)$, alors A est principal.

Propriété 6.11 : (*Sous-anneaux unitaires de $\mathbb{Q}$*)

Tout sous-anneau unitaire de $\mathbb{Q}$ est principal.

Preuve :

On propose deux preuves de ce résultat.

① **Première preuve (via localisation) :**

Soit A un sous-anneau unitaire de $\mathbb{Q}$.

Alors A contient forcément $\mathbb{Z}$ (car $1_{\mathbb{Q}} \in A$, donc $\mathbb{Z} \subset A$).

On définit :

$$S = \left\{ n \geqslant 1 \;\middle|\; \frac{1}{n} \in A \right\}$$

On vérifie que S est un sous-monoïde multiplicatif :

⊛ $0 \notin S$,

⊛ $1 \in S$,

⊛ Si $(s, s') \in S^2$, alors $s \cdot s' \in S$.

Supposons que $\dfrac{a}{b} \in A$ avec $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \geqslant 1$ et $\mathrm{PGCD}(a,b) = 1$.

D'après le théorème de Bézout, il existe $(\lambda, \mu) \in \mathbb{Z}^2$ tels que :

$$\lambda \cdot a + \mu \cdot b = 1$$

Donc :

$$\lambda \cdot \frac{a}{b} + \mu = \frac{1}{b}$$

Or $\lambda \in \mathbb{Z} \subset A$, $\dfrac{a}{b} \in A$ et $\mu \in \mathbb{Z} \subset A$.

Donc $\dfrac{1}{b} \in A$, ce qui signifie que $b \in S$.

Soit ψ définie par :

$$\begin{array}{rccc} \psi : & S^{-1}\mathbb{Z} & \longrightarrow & A \\ & \overline{(a,b)} & \longmapsto & \frac{a}{b} \end{array}$$

⊛ **ψ est bien définie :**

Soient $\overline{(a,b)} = \overline{(a',b')}$ dans $S^{-1}\mathbb{Z}$.

Il existe $s'' \in S$ tel que :

$$s'' \cdot a \cdot b' = s'' \cdot a' \cdot b$$

Donc :

$$\frac{s'' \cdot a \cdot b'}{s'' \cdot b \cdot b'} = \frac{s'' \cdot a' \cdot b}{s'' \cdot b \cdot b'}$$

c'est-à-dire :

$$\frac{a}{b} = \frac{a'}{b'}$$

⊛ **ψ est un morphisme d'anneaux unitaires :**

Soient $x = \overline{(a,b)}$ et $y = \overline{(a',b')}$ dans $S^{-1}\mathbb{Z}$.

⊛ **Additivité :**

$$\begin{aligned} x + y &= \overline{(a \cdot b' + a' \cdot b, b \cdot b')} \\ \psi(x+y) &= \frac{a \cdot b' + a' \cdot b}{b \cdot b'} \\ &= \frac{a}{b} + \frac{a'}{b'} \\ &= \psi(x) + \psi(y) \end{aligned}$$

⊛ **Multiplicativité :**

$$\begin{aligned} x \cdot y &= \overline{(a \cdot a', b \cdot b')} \\ \psi(x \cdot y) &= \frac{a \cdot a'}{b \cdot b'} \\ &= \frac{a}{b} \cdot \frac{a'}{b'} \\ &= \psi(x) \cdot \psi(y) \end{aligned}$$

⊛ **Unité :**

$$\psi\left(1_{S^{-1}\mathbb{Z}}\right) = \psi\left(\overline{(1,1)}\right) = \frac{1}{1} = 1 = 1_A$$

⊛ **ψ est injective :**

Soit $x \in \mathrm{Ker}(\psi)$.

On écrit $x = \overline{(a,b)}$.

Alors :

$$\psi\left(\overline{(a,b)}\right) = 0$$

donc

$$\frac{a}{b} = 0$$

ce qui implique $a = 0$.

Ainsi :

$$x = \overline{(0,b)} = \overline{(0,1)} = 0_{S^{-1}\mathbb{Z}}$$

⊛ **ψ est surjective :**

Soit $x \in A$.

On peut écrire $x = \frac{a}{b}$ avec $(a,b) \in \mathbb{Z}^2$, $b \geqslant 1$ et $\mathrm{PGCD}(a,b) = 1$.

Comme $\frac{a}{b} = x \in A$ et PGCD$(a,b) = 1$, on a montré précédemment que $b \in S$.

Alors :

$$x = \frac{a}{b} = \psi\left(\overline{(a,b)}\right)$$

avec $\overline{(a,b)} \in S^{-1}\mathbb{Z}$.

Donc ψ est un isomorphisme d'anneaux, et :

$$A \simeq S^{-1}\mathbb{Z}$$

Or $\mathbb{Z}$ est principal, donc $S^{-1}\mathbb{Z}$ est principal (d'après le théorème 6.7).

Ainsi A est principal.

② **Deuxième preuve (alternative) :**

Soit I un idéal de A.

Alors $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Comme $\mathbb{Z}$ est principal, il existe $m \in \mathbb{N}$ tel que :

$$I \cap \mathbb{Z} = m \cdot \mathbb{Z}$$

On a $m = m \cdot 1 \in m \cdot \mathbb{Z} = I \cap \mathbb{Z} \subset I$.

Donc $m \in I$, et ainsi $m \cdot A \subset I$.

Soit $x \in I$.

On peut écrire $x = \frac{a}{b}$ avec $(a,b) \in \mathbb{Z}^2$ et $b \neq 0$.

On suppose PGCD$(a,b) = 1$.

D'après le théorème de Bézout, il existe $(\lambda, \mu) \in \mathbb{Z}^2$ tels que :

$$\lambda \cdot a + \mu \cdot b = 1$$

Alors :

$$a = x \cdot b \in I$$

car $x \in I$ et $b \in \mathbb{Z} \subset A$.

Donc $a \in I \cap \mathbb{Z} = m \cdot \mathbb{Z}$.

Il existe $c \in \mathbb{Z}$ tel que $a = m \cdot c$.

De l'égalité de Bézout, on déduit :

$$\frac{1}{b} = \lambda \cdot \frac{a}{b} + \mu = \lambda \cdot x + \mu$$

Or $\lambda \in \mathbb{Z} \subset A$, $x \in I \subset A$ et $\mu \in \mathbb{Z} \subset A$.

Donc $\frac{1}{b} \in A$.

Finalement :

$$x = \frac{a}{b} = \frac{m \cdot c}{b} = m \cdot \left(c \cdot \frac{1}{b}\right) \in m \cdot A$$

Ainsi $I \subset m \cdot A$.

On a montré que $I = m \cdot A$.

Donc tout idéal de A est principal.

Finalement, A est principal.

Propriété 6.12 : (*Intersection des puissances de l'idéal maximal de $\mathbb{Z}_{(p)}$*)

On a :

$$\bigcap_{n\in\mathbb{N}} i(p)^n\mathbb{Z}_{(p)} = \{0\}$$

Preuve :

Soit $x = \overline{(a,s)} \in \bigcap_{n\in\mathbb{N}} i(p)^n\mathbb{Z}_{(p)}$.

Pour tout $n \in \mathbb{N}$, on a :

$$\begin{aligned}\overline{(a,s)} &= i(p)^n \cdot \overline{(b_n,s_n)}\\ &= \overline{(p,s)}^n \cdot \overline{(b_n,s_n)}\\ &= \overline{(p^n,1)} \cdot \overline{(b_n,s_n)}\\ &= \overline{(p^n\cdot b_n, s_n)}\end{aligned}$$

Il existe $s'_n \in S$ tel que :

$$s'_n \cdot a \cdot s_n = s'_n \cdot p^n \cdot b_n \cdot s$$

Donc :

$$\underbrace{s_n \cdot s'_n}_{\in S=\mathbb{Z}\setminus p\mathbb{Z}} \cdot a = p^n \cdot \left(s'_n \cdot b_n \cdot s\right)$$

On a $p^n \mid s_n \cdot s'_n \cdot a$ et $p^n \nmid s_n \cdot s'_n$.

Donc $p^n \mid a$.

Ainsi, pour tout $n \in \mathbb{N}$, $p^n \mid a$, ce qui implique $a = 0$.

Finalement :

$$x = \overline{(a,s)} = 0_{\mathbb{Z}_{(p)}}$$

Définition 6.13 : (*Valuation p-adique*)

Soit $x \in \mathbb{Z}_{(p)}$ tel que $x \neq 0_{\mathbb{Z}_{(p)}}$.

On définit la ***valuation p-adique*** de x par :

$$v_p(x) = \max\left\{k \in \mathbb{N} \;\middle|\; x \in i(p)^k\mathbb{Z}_{(p)}\right\}$$

Propriété 6.14 : (*La valuation p-adique est bien définie*)

La valuation v_p est bien définie.

Preuve :

La suite $\left(i(p)^n\mathbb{Z}_{(p)}\right)_{n\in\mathbb{N}}$ est décroissante car :

$$i(p)^{n+1}\mathbb{Z}_{(p)} \subset i(p)^n\mathbb{Z}_{(p)}$$

pour tout $n \in \mathbb{N}$.

De plus, d'après la propriété 6.12, on a :

$$\bigcap_{n\in\mathbb{N}} i(p)^n\mathbb{Z}_{(p)} = \{0\}$$

Donc pour tout $x \in \mathbb{Z}_{(p)}$ non nul, l'ensemble $\left\{k \in \mathbb{N} \;\middle|\; x \in i(p)^k\mathbb{Z}_{(p)}\right\}$ est fini (car x n'appartient pas à l'intersection de tous les $i(p)^n\mathbb{Z}_{(p)}$).

Ainsi, le maximum existe et $v_p(x)$ est bien défini.

Définition 6.15 : (*Distance p-adique*)

On définit la ***distance p-adique*** sur $\mathbb{Z}_{(p)}$ par :

$$d_p(x,y) = \begin{cases} 0 & \text{si } x = y \\ p^{-v_p(x-y)} & \text{si } x \neq y \end{cases}$$

Propriété 6.16 : (*Propriétés de la distance p-adique*)

La fonction d_p vérifie les propriétés suivantes :

① Pour tous $(x,y) \in \mathbb{Z}_{(p)}^2$, $d_p(x,y) \geqslant 0$.

② Pour tous $(x,y) \in \mathbb{Z}_{(p)}^2$, $d_p(x,y) = 0 \iff x = y$.

③ Pour tous $(x,y) \in \mathbb{Z}_{(p)}^2$, $d_p(x,y) = d_p(y,x)$.

Théorème 6.17 : (*Inégalité ultramétrique*)

Pour tous $(x,y,z) \in \mathbb{Z}_{(p)}^3$:

$$d_p(x,z) \leqslant \max\left(d_p(x,y), d_p(y,z)\right)$$

d_p est dite une ***distance ultramétrique*** sur $\mathbb{Z}_{(p)}$.

Preuve :

Si $x = y$ ou $x = z$ ou $y = z$, alors l'inégalité est évidente.

Donc on peut supposer que $x \neq y$, $x \neq z$ et $y \neq z$.

Soient $m = v_p(x-y)$ et $n = v_p(y-z)$.

On peut supposer que $m \leqslant n$.

Donc $x - y \in i(p)^m \cdot \mathbb{Z}_{(p)}$ et $y - z \in i(p)^n\mathbb{Z}_{(p)}$.

Comme $m \leqslant n$, on a $i(p)^n\mathbb{Z}_{(p)} \subset i(p)^m\mathbb{Z}_{(p)}$, donc $y - z \in i(p)^m\mathbb{Z}_{(p)}$.

On a :

$$x - z = x - y + y - z = i(p)^m \cdot \alpha + i(p)^n \cdot \beta$$

donc

$$x - z = i(p)^m \cdot \left(\alpha + i(p)^{n-m} \cdot \beta\right) \in i(p)^m\mathbb{Z}_{(p)}$$

Ainsi $v_p(x-z) \geqslant m$.

Donc $d_p(x,z) = p^{-v_p(x-z)} \leqslant p^{-m}$.

Or :

$$\max\left(d_p(x,y), d_p(y,z)\right) = \max\left(p^{-m}, p^{-n}\right) = p^{-m}$$

car $m \leqslant n$.

Finalement :

$$p^{-m} \geqslant d_p(x,z)$$

Définition 6.18 : (*Anneau des entiers p-adiques*)

On note $\mathbb{Z}_p$ le complété de $\left(\mathbb{Z}_{(p)}, d_p\right)$.

$\mathbb{Z}_p$ est appelé ***anneau des entiers p-adiques***.

Propriété 6.19 : (*Prolongement des opérations de $\mathbb{Z}_{(p)}$ à $\mathbb{Z}_p$*)

Les opérations de $\mathbb{Z}_{(p)}$ se prolongent par continuité à $\mathbb{Z}_p$.

Preuve :

Soit $x \in \mathbb{Z}_p$.

Il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{Z}_{(p)}$ telle que :

$$x = \lim_{n\to+\infty} x_n$$

De même, pour $y \in \mathbb{Z}_p$, on écrit $y = \lim\limits_{n\to+\infty} y_n$ avec $y_n \in \mathbb{Z}_{(p)}$.

On définit les opérations par passage à la limite :

$$x + y = \lim_{n\to+\infty} \left(x_n + y_n\right)$$

et

$$x \cdot y = \lim_{n\to+\infty} \left(x_n \cdot y_n\right)$$

Ces opérations sont bien définies car pour toutes suites (x'_n) et (y'_n) convergeant vers x et y respectivement, on a :

$$v_p\left(x_n + y_n - \left(x'_n + y'_n\right)\right) \geqslant \min\left(v_p\left(x_n - x'_n\right), v_p\left(y_n - y'_n\right)\right)$$

donc par l'inégalité ultramétrique :

$$d_p\left(x_n + y_n, x'_n + y'_n\right) \leqslant \max\left(d_p\left(x_n, x'_n\right), d_p\left(y_n, y'_n\right)\right)$$

Ce qui assure que la limite ne dépend pas du choix des suites.

Propriété 6.20 : (*Densité de $\mathbb{Z}$ dans $\mathbb{Z}_p$*)

$i(\mathbb{Z})$ est dense dans $\left(\mathbb{Z}_p, d_p\right)$.

On a les inclusions denses :

$$i(\mathbb{Z}) \subset \mathbb{Z}_{(p)} \subset \mathbb{Z}_p$$

Preuve :

Il suffit de démontrer que $i(\mathbb{Z})$ est dense dans $\mathbb{Z}_{(p)}$.

Soit $x \in \mathbb{Z}_{(p)}$ et $\varepsilon > 0$.

Il existe $n \in \mathbb{N}$ tel que $p^{-n} < \varepsilon$.

On écrit $x = \overline{(a,s)}$ avec $s \in S = \mathbb{Z} \setminus p\mathbb{Z}$.

Donc $p \nmid s$, donc $\text{PGCD}(p,s) = 1$ et $\text{PGCD}\left(p^n, s\right) = 1$.

D'après le théorème de Bézout, il existe $(\lambda, \mu) \in \mathbb{Z}^2$ tels que :

$$\lambda \cdot p^n + \mu \cdot s = 1$$

Posons $a_\mu = a \cdot \mu \in \mathbb{Z}$.

Alors :

$$\begin{aligned} x - i(a_\mu) &= \overline{(a,s)} - \overline{\left(a \cdot \mu, 1\right)} \\ &= \overline{(a,s)} + \overline{\left(-a \cdot \mu, 1\right)} \\ &= \overline{\left(a - a \cdot \mu \cdot s, s\right)} \\ &= \overline{\left(a \cdot \left(1 - s \cdot \mu\right), s\right)} \\ &= \overline{\left(a \cdot \lambda \cdot p^n, s\right)} \\ &= \overline{\left(p^n, 1\right)} \cdot \overline{(\lambda \cdot a, s)} \\ &= i(p)^n \cdot \overline{(\lambda \cdot a, s)} \end{aligned}$$

Donc $x - i(a_\mu) \in i(p)^n \mathbb{Z}_{(p)}$.

Ainsi $x - i(a_\mu) = 0$ ou $v_p\left(x - i(a_\mu)\right) \geqslant n$.

Donc $d_p\left(x, i(a_\mu)\right) = 0$ ou $d_p\left(x, i(a_\mu)\right) \leqslant p^{-n} < \varepsilon$.

Finalement :

$$d_p\left(x, i(a_\mu)\right) < \varepsilon$$

avec $i(a_\mu) \in i(\mathbb{Z})$.

Donc $i(\mathbb{Z})$ est dense dans $\mathbb{Z}_{(p)}$, et par transitivité dense dans $\mathbb{Z}_p$.

Propriété 6.21 : (*Structure d'anneau de $\mathbb{Z}_p$*)

$\mathbb{Z}_p$ est un anneau intègre local principal.

Preuve :

⊛ **Anneau intègre :**

$\mathbb{Z}_p$ est un anneau commutatif unitaire car il est le complété d'un anneau commutatif unitaire $\mathbb{Z}_{(p)}$.

De plus, $\mathbb{Z}_p$ est intègre car si $x, y \in \mathbb{Z}_p$ sont non nuls, alors $v_p(x) < +\infty$ et $v_p(y) < +\infty$, donc $v_p(xy) = v_p(x) + v_p(y) < +\infty$, ce qui implique $xy \neq 0$.

⊛ **Anneau local :**

L'idéal maximal de $\mathbb{Z}_p$ est $p\mathbb{Z}_p$.

En effet, tout élément $x \in \mathbb{Z}_p$ tel que $v_p(x) = 0$ est inversible dans $\mathbb{Z}_p$.

Donc les éléments non inversibles de $\mathbb{Z}_p$ sont exactement ceux de valuation $v_p(x) \geqslant 1$, c'est-à-dire $p\mathbb{Z}_p$.

⊛ **Anneau principal :**

Tout idéal de $\mathbb{Z}_p$ est de la forme $p^n\mathbb{Z}_p$ pour un certain $n \in \mathbb{N}$.

En effet, soit I un idéal non nul de $\mathbb{Z}_p$.

On pose $n = \min\{v_p(x) \mid x \in I, x \neq 0\}$.

Alors $I = p^n\mathbb{Z}_p$.

Définition 6.22 : (*Corps des nombres p-adiques*)

On note $\mathbb{Q}_p = \text{Frac}(\mathbb{Z}_p)$.

$\mathbb{Q}_p$ est appelé ***corps des nombres p-adiques***.

Propriété 6.23 : (*Inclusions des corps p-adiques*)

On a les inclusions :

$$\mathbb{Q} = \text{Frac}(\mathbb{Z}) \simeq \text{Frac}(i(\mathbb{Z})) \subset \text{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$$

Chapitre 7

Corps

Définition 7.1 : (*Morphisme canonique de $\mathbb{Z}$ dans un corps*)

Soit K un corps (pour le moment, éventuellement non commutatif).

On appelle ***morphisme canonique*** de $\mathbb{Z}$ dans K l'application $\varphi : \mathbb{Z} \longrightarrow K$ définie par :

$$\varphi(n) = \begin{cases} \sum_{k=1}^{n} 1_K = \underbrace{1_K + \cdots + 1_K}_{n \text{ fois}} & \text{si } n \geqslant 1 \\ 0_K & \text{si } n = 0 \\ -\varphi(-n) = -\sum_{k=1}^{-n} 1_K & \text{si } n \leqslant -1 \end{cases}$$

Propriété 7.2 : (*Propriété du morphisme canonique*)

L'application φ est un morphisme d'anneaux unitaire.

Propriété 7.3 : (*Noyau du morphisme canonique*)

Le noyau $\mathrm{Ker}(\varphi)$ est un idéal de $\mathbb{Z}$.

Il existe donc $a \in \mathbb{N}$ tel que $\mathrm{Ker}(\varphi) = a\mathbb{Z}$.

De plus, comme $\varphi(1) = 1_K \neq 0_K$, on a $1 \notin \mathrm{Ker}(\varphi)$, donc $a \neq 1$.

Propriété 7.4 : (*Structure du quotient*)

On a l'isomorphisme :

$$\frac{\mathbb{Z}}{a\mathbb{Z}} = \frac{\mathbb{Z}}{\mathrm{Ker}(\varphi)} \simeq \mathrm{Im}(\varphi) \subset K$$

L'image $\mathrm{Im}(\varphi)$ est un anneau intègre contenu dans tout sous-corps de K.

Les seules possibilités sont :

$$a = 0 \quad \text{ou} \quad a = p \text{ avec } p \text{ premier}$$

Définition 7.5 : (*Corps de caractéristique nulle*)

Si $a = 0$, alors $\mathrm{Ker}(\varphi) = \{0\}$.

Le morphisme $\varphi : \mathbb{Z} \to K$ est injectif et $\mathrm{Im}(\varphi) \simeq \mathbb{Z}$.

On définit le sous-corps :

$$K_0 = \left\{ \frac{\varphi(a)}{\varphi(b)} \;\middle|\; (a,b) \in \mathbb{Z}^2,\ b \neq 0 \right\}$$

Alors K_0 est un sous-corps de K isomorphe à $\mathbb{Q}$.

K_0 est le plus petit sous-corps de K.

On dit que K est de ***caractéristique nulle*** et on note :

$$\mathrm{Char}(K) = 0$$

Définition 7.6 : (*Corps de caractéristique p*)

Si $a = p$ est premier, alors :

$$K_0 = \mathrm{Im}(\varphi) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$$

est un corps (car $\mathbb{Z}/p\mathbb{Z}$ est un corps).

K_0 est le plus petit sous-corps de K (et K_0 est commutatif).

On dit que K est de ***caractéristique*** p et on note :

$$\mathrm{Char}(K) = p$$

Propriété 7.7 : (*Caractéristique et sous-corps*)

Soit K un corps.

- Si $\mathrm{Char}(K) = 0$, alors K contient un sous-corps isomorphe à $\mathbb{Q}$.
- Si $\mathrm{Char}(K) = p$ (premier), alors K contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Propriété 7.8 : (*Caractéristique d'une extension de corps*)

Soit L un corps et K un sous-corps de L.

Alors $\mathrm{Char}(K) = \mathrm{Char}(L)$.

Preuve :

On a les inclusions :

$$K_0 \subset K \subset L$$

et

$$L_0 \subset K_0 \subset K_0$$

donc $L_0 = K_0$.

Ainsi, K et L ont le même sous-corps premier, donc la même caractéristique.

Exemple :

Le corps $\mathbb{Q}_p$ des nombres p-adiques est de caractéristique nulle :

$$\mathrm{Char}(\mathbb{Q}_p) = 0$$

Chapitre 8

Polynômes cyclotomiques

Définition 8.1 : (*Corps algébriquement clos*)

Soit K un corps.

On dit que K est ***algébriquement clos*** si et seulement si tout polynôme de $K[X]$ de degré $\geqslant 1$ admet au moins une racine dans K.

Cela équivaut à dire que tout polynôme de $K[X]$ de degré $\geqslant 1$ se factorise en :

$$\lambda(X-\alpha_1)\cdots(X-\alpha_n)$$

avec $\lambda \in K$ et $\alpha_1,\ldots,\alpha_n \in K$.

Exemple :

- $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert-Gauss).
- Pour tout corps K, on a $K \subset \overline{K}$ où $\overline{K}$ est la clôture algébrique de K.
- $\overline{\mathbb{R}} = \mathbb{C}$.

Propriété 8.2 : (*Racine multiple d'un polynôme*)

Soit $P \in K[X]$ et $\alpha \in K$.

α est une racine au moins double de P si et seulement si :

$$P(\alpha) = P'(\alpha) = 0$$

Si P et P' n'ont pas de racine commune, alors toutes les racines de P sont simples.

Définition 8.3 : (*Polynômes cyclotomiques*)

Soit $n \geqslant 1$.

On appelle ***n-ième polynôme cyclotomique*** le polynôme $\Phi_n(X)$ défini par :

$$\Phi_n(X) = \prod_{\substack{\zeta \text{ racine} \\ \text{primitive} \\ n\text{-ième de 1}}} (X-\zeta)$$

On a $\Phi_n(X) \in \mathbb{C}[X]$ et :

$$\Phi_n(X) = \prod_{\substack{k=1 \\ \text{PGCD}(k,n)=1}}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

Exemple :

$$\Phi_1(X) = X-1 \qquad \Phi_2(X) = X+1$$

$$\Phi_3(X) = (X-j)(X-j^2) = X^2+X+1 \qquad \Phi_4(X) = X^2+1$$

$$\Phi_5(X) = X^4+X^3+X^2+X+1 \qquad \Phi_6(X) = X^2-X+1$$

Théorème 8.4 : (*Polynômes cyclotomiques à coefficients entiers*)

Pour tout $n \geqslant 1$, on a

$$\Phi_n(X) \in \mathbb{Z}[X]$$

Preuve :

On procède par récurrence forte sur n.

Initialisation : Pour $n = 1$, on a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

Hérédité : Supposons que pour tout $k < n$, on a $\Phi_k(X) \in \mathbb{Z}[X]$.

On a la relation :

$$\prod_{d|n} \Phi_d(X) = \prod_{d|n} \prod_{\substack{\zeta \text{ racine} \\ \text{primitive} \\ n\text{-ième de 1}}} (X - \zeta) = \prod_{\zeta \text{ tq } \zeta^n = 1} (X - \zeta) = X^n - 1$$

car les racines n-ièmes de l'unité sont simples.

Donc :

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \left(\prod_{\substack{d|n \\ d<n}} \Phi_d(X) \right) \cdot \Phi_n(X)$$

Or $X^n - 1 \in \mathbb{Z}[X]$ et $\prod_{\substack{d|n \\ d<n}} \Phi_d(X) \in \mathbb{Z}[X]$ par hypothèse de récurrence, et ce polynôme est unitaire.

Donc $\Phi_n(X) \in \mathbb{Z}[X]$.

Théorème 8.5 : (*Théorème de Wedderburn*)

Tout corps fini est commutatif.

Preuve :

Soit K un corps fini.

① **Structure du centre de K :**

Le sous-corps premier K_0 de K est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

On note $|K| = p^m$.

On définit le **centre** de K par :

$$Z(K) = \left\{ x \in K \;\middle|\; \left(\forall y \in K\right),\ x \cdot y = y \cdot x \right\}$$

$Z(K)$ est un sous-corps commutatif de K contenant K_0.

On note $|Z(K)| = q = p^r$ avec $r \geqslant 1$.

② **Centralisateurs :**

Pour tout $x \in K$, on définit le **centralisateur** de x dans K par :

$$C_K(x) = \left\{ y \in K \;\middle|\; x \cdot y = y \cdot x \right\}$$

$C_K(x)$ est un sous-corps de K contenant $Z(K)$.

③ **Structure d'espace vectoriel :**

K est un espace vectoriel à gauche sur $Z(K)$.

Si on note $n = \dim_{Z(K)}(K)$, alors :

$$|K| = |Z(K)|^n = q^n$$

De même, K est un espace vectoriel à gauche sur $C_K(x)$.

Si on note $m_x = \dim_{C_K(x)}(K)$, alors :

$$|K| = |C_K(x)|^{m_x}$$

Et $C_K(x)$ est un espace vectoriel à gauche sur $Z(K)$.

Si on note $d_x = \dim_{Z(K)}(C_K(x))$, alors :

$$|C_K(x)| = |Z(K)|^{d_x} = q^{d_x}$$

On en déduit que :

$$q^n = \left(q^{d_x}\right)^{m_x} = q^{d_x \cdot m_x}$$

donc

$$d_x \cdot m_x = n$$

④ **Formule des classes :**

On suppose $n > 1$ (sinon $K = Z(K)$ est commutatif).

On considère l'action de $K^* = K \setminus \{0\}$ sur lui-même par conjugaison : $y \cdot x = y \cdot x \cdot y^{-1}$.

Les classes de conjugaison sont les orbites de cette action.

Soit $\{x_1, \ldots, x_{q-1}, x_q, \ldots, x_s\}$ un système de représentants des classes de conjugaison de K^*.

Les éléments de $Z(K)^* = Z(K) \setminus \{0\}$ forment des classes de conjugaison à un élément.

On a $Z(K)^* = \{x_1, \ldots, x_{q-1}\}$.

Pour $\ell \geqslant q$, la classe de conjugaison de x_ℓ a pour cardinal :

$$\frac{|K^*|}{|C_{K^*}(x_\ell)|} = \frac{|K \setminus \{0\}|}{|C_K(x_\ell) \setminus \{0\}|} = \frac{q^n - 1}{q^{d_{x_\ell}} - 1}$$

La formule des classes donne :

$$q^n - 1 = (q-1) + \sum_{\ell=q}^{s} \frac{q^n - 1}{q^{d_{x_\ell}} - 1}$$

Or d_{x_ℓ} divise n et $d_{x_\ell} < n$ (car $x_\ell \notin Z(K)$).

⑤ **Utilisation des polynômes cyclotomiques :**

On a la factorisation :

$$q^n - 1 = \prod_{d|n} \Phi_d(q)$$

Et pour chaque ℓ :

$$\frac{q^n - 1}{q^{d_{x_\ell}} - 1} = \prod_{\substack{d|n \\ d \nmid d_{x_\ell}}} \Phi_d(q)$$

Donc $\Phi_n(q)$ divise chaque terme $\dfrac{q^n - 1}{q^{d_{x_\ell}} - 1}$ et divise donc $q^n - 1 - \displaystyle\sum_{\ell=q}^{s} \frac{q^n - 1}{q^{d_{x_\ell}} - 1} = q - 1$.

Ainsi $\Phi_n(q)$ divise $q - 1$.

⑥ **Contradiction :**

Or :

$$\left|\Phi_n(q)\right| = \prod_{\substack{\zeta \text{ racine} \\ \text{primitive} \\ n\text{-ième de 1}}} \left|q-\zeta\right|$$

Pour chaque racine primitive ζ, on a $|\zeta| = 1$, donc :

$$\left|q-\zeta\right| \geqslant q - |\zeta| = q-1$$

De plus, $\deg(\Phi_n) = \varphi(n) \geqslant 1$ (où φ est la fonction indicatrice d'Euler).

Si $n > 1$, alors $\varphi(n) \geqslant 1$ et il existe au moins une racine primitive $\zeta \neq 1$, donc $\left|q-\zeta\right| > q-1$.

Ainsi :

$$\left|\Phi_n(q)\right| > q-1$$

Ceci contredit le fait que $\Phi_n(q)$ divise $q-1$ (car $\left|\Phi_n(q)\right| > q-1 \geqslant 1$).

Donc l'hypothèse $n > 1$ est fausse.

Ainsi $n = 1$, ce qui signifie $K = Z(K)$, donc K est commutatif.