Université des Sciences et Technologies de Lille
U.F.R. de Mathématiques Pures et Appliquées

M301 : Algèbre commutative

Notes de cours par Clément Boulonne

L3 Mathématiques **2008 - 2009**

Table des matières

Chapitre 1

Anneaux, anneaux intégres, corps

1.1 Anneaux

Définition 1.1.1. Soit A un ensemble non vide muni de deux opérations notés "+" et ".". $(A, +, .)$ est un anneau si :

(i) $(A, +)$ est un groupe commutatif :
- $\forall x, y \in A$, $x + y \in A$
- $\forall x, y, z \in A$, $(x + y) + z = x + (y + z)$
- $\forall x, y \in A$, $x + y = y + x$
- $\exists x \in A$, $\forall x \in A$, $x + e = x$, e sera noté 0_A.
- $\forall x \in A$, $\exists x' \in A$, $x + x' = 0_A$. x' sera noté $-x$.

(ii)
- $\forall x, y \in A$, $x.y \in A$
- $\forall x, y, z \in A$, $(x.y).z = x.(y.z)$
- $\forall x, y, z \in A$, $x.(y + z) = x.y + x.z$ et $(y + z).x = y.x + z.x$
- $\exists e \in A$, $\forall x \in A$, $x.e = e.x = x$. e sera noté 1_A (élément unité).

Définition 1.1.2. $(A, +, .)$ est un anneau commutatif si $\forall x, y \in A$, $x.y = y.x$.

Exemple 1.1.1. $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ sont des anneaux commutatifs.

Exemple 1.1.2. Soit $n \in \mathbb{N}\backslash\{0\}$. $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif :

$$0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0} = n\mathbb{Z},\ 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1} = 1 + n\mathbb{Z}$$

Propriété 1.1.1. *Soit A un anneau non nécessairement commutatif. Alors :*

(i) $\forall a \in A$, $a.0 = 0.a = 0$

(ii) $\forall a, b \in A$, $(-a).b = a.(-b) = -(a.b)$

(iii) $0_A = 1_A \Leftrightarrow A = \{0_A\}$

Démonstration. (i) Soit $a \in A$:

$$a.0 = a(0+0) = a.0+a.0 \Rightarrow \underbrace{-(a.0) + a.0}_{0} = -(a.0)+(a.0+a.0) = \underbrace{(-(a.0) + a.0)}_{0} + a.0 = 0$$

$$\Rightarrow 0 = a.0$$

(ii) Soit $a, b \in A$:

$$(-a).b + a.b = (-a + a).b = 0.b = 0$$

$$a.(-b) + a.b = a.(-b + b) = 0.a = 0$$

(iii) ($\Rightarrow$) Soit $a \in A$ alors :

$$a = a.1 = a.0 = 0$$

($\Leftarrow$) évident.

□

Proposition 1.1.2 (Formule du binôme)**.** *Soit A un anneau commutatif. Soit $a, b \in A$, $n \in \mathbb{N}\backslash\{0\}$. Alors :*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Démonstration. Voir **M101** et **M103**. □

1.2 Sous-anneaux

Définition 1.2.1. Soit $(A, +, .)$ est un anneau et B un sous-ensemble de A, B est un sous-anneau de A si $(B, +, .)$ est un anneau. Ceci revient à :

(i) $(B, +)$ est un sous-groupe de $(A, +)$, c'est-à-dire $0_A \in B$ et $\forall x, y \in B$, $x - y \in B$, où $x - y = x + (-y)$.

(ii) B stable pour la multiplication : $\forall x, y \in B$, $x.y = B$.

(iii) $1_A \in B$.

Exemple 1.2.1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

Exemple 1.2.2. $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{C}, +, .)$.

1.3 Anneaux intégres

Définition 1.3.1. Soit A un anneau non nul. A est un anneau intégre si :

$$\forall x, y \in A,\ x.y = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Exemple 1.3.1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intégres.

Exemple 1.3.2. $\mathbb{Z}/6\mathbb{Z}$ est un anneau non intégre car :

$$\overline{2}.\overline{3} = 0 \text{ mais } \overline{2} \neq \overline{0} \text{ et } \overline{3} \neq \overline{0}$$

On peut montrer que $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ est intégre si et seulement si n un nombre premier.

Définition 1.3.2 (Diviseurs de zéro)**.** Soit A un anneau non nul et $a \in A\backslash\{0\}$, a est un diviseur de zéro s'il existe $b \in A\backslash\{0\}$ tel que $a.b = 0$.

1.4 Corps

Définition 1.4.1. Soit $(A, +, .)$ un anneau non nul commutatif et $a \in A$, a est inversible pour la multiplication "." s'il existe a' tel que $a'.a = 1$.

Si a' existe, il est unique et sera noté a^{-1}. On note $A^\times$ l'ensemble des éléments de A inversibles pour la multiplication.

$$1 \in A^\times \Rightarrow A^\times \neq \emptyset$$

Exemple 1.4.1. $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$.

Exemple 1.4.2. Soit $n \in \mathbb{N}\backslash\{0\}$.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z},\ \mathrm{PGCD}(a, n) = 1\}$$

Proposition 1.4.1. *Soit A un anneau non nul commutatif. Alors $(A^\times, .)$ est un groupe commutatif.*

Démonstration. (i) Soit $a, b \in A^\times$. On doit montrer que $a, b \in A^\times$. On a :

$$(a.b).(b^{-1}.a) = a.(b.b^{-1}).a^{-1} = a.1.a^{-1} = a.a^{-1} = 1$$

(ii) La multiplication est associative et commutative.

(iii) $1 \in A^\times$

(iv) Par définition de $A^\times$, tous les élements de $A^\times$ sont inversibles.

□

Définition 1.4.2. Soit A un anneau commutatif non nul, A est un corps si $A^\times = A\backslash\{0\}$.

Exemple 1.4.3. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

Exemple 1.4.4. Soit $n \in \mathbb{N}\backslash\{0, 1\}$, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Démonstration. ($\Rightarrow$) On suppose que n n'est pas premier alros n s'écrit $n = ab$ avec $a > 1$ et $b > 1$. on a : $\overline{a}.\overline{b} = \overline{0}$. On montre que $\overline{a}$ n'est pas inversible. Supposons qu'il existe $\overline{a}^{-1} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a}.\overline{a}^{-1} = 1$. alors :

$$\underbrace{\overline{a}^{-1}.\overline{a}}_{\overline{1}}.\overline{b} = \overline{a}^{-1}.\overline{0} = \overline{0} \Rightarrow \overline{b} = \overline{0}$$

Ce qui est absurde puisuqe $1 < b < n$. Puisque $\overline{a}$ n'est pas inversible, ceci contredit le fait que $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$.

($\Leftarrow$)

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z},\ \mathrm{PGCD}(a, n) = 1\}$$

Si n premier, alors pour $a = 1, 2, ..., n-1$, $\mathrm{PGCD}(a, n) = 1$ donc :

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$$

□

Proposition 1.4.2. *Si A est un anneau intégre fini alors A est un corps.*

Démonstration. Soit $a \in A\backslash\{0\}$ (fixé). On considère l'application :

$$\begin{array}{rccc} \varphi & : & A & \to & A \\ & & x & \mapsto & a.x \end{array}$$

On montre que φ est injective. Soit $x, x' \in A$ tels que $a.x = a.x'$:

$$\begin{array}{rcl} a.x = a.x' & \Rightarrow & a.x - a.x' = 0 \\ & \Rightarrow & a(x - x') = 0 \\ & \overset{(*)}{\Rightarrow} & x - x' = 0 \\ & \Rightarrow & x = x' \end{array}$$

Condition $(*)$: $a \neq 0$ et A intégre. Comme A est fini, φ est surjective donc il existe $x \in A$ tel que $a.x = 1$. □

Chapitre 2

Idéaux

2.1 Introduction

Définition 2.1.1. Soit $(G, *)$ un groupe commutatif et H un sous-groupe de G. Soit $a, b \in G$. On dit que a est congru à b modulo H si $a * b^{-1} \in H$. Ceci revient à dire qu'il existe $h \in H$ tel que $a * b^{-1} = h$ ou encore $a = h * b = b * h$. Soit $a \in H$. On note $a * H$ l'ensemble :

$$a * H = \{a * h,\, h \in H\}$$

On note $a \equiv b[H]$ si $a \in b * H$. On démontre que la relation "congru mod H" est une relation d'équivalence. La classe d'un élément $a \in G$ sera notée $a * H$. L'ensemble des classes sera noté G/H :

$$G/H = \{a * H,\, a \in G\}$$

Exemple 2.1.1. $G = \mathbb{Z}$, $* = +$ et $H = n\mathbb{Z}$:

$$G/H = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z},\, a \in \mathbb{Z}\}$$

Définition 2.1.2. On définit dans G/H l'opération qui sera notée "$\circledast$" :

$$(a * H) \circledast (b * H) = (a * b) * H$$

Démonstration. On vérifie que cette opération a un sens. Soit $a, b, a', b' \in G$ tels que :

$$a * H = a' * H \text{ et } b * H = b' * H$$

On montre que :

$$(a * b) * h = (a' * b') * H$$

$$a * H = a' * H \Rightarrow \exists h \in H \text{ tel que } a = a' * h$$

$$b * H = b' * H \Rightarrow \exists h' \in H \text{ tel que } b = b' * h'$$

Donc :

$$a * b = (a' * h) * (b' * h') = a' * b' * h * h' \text{ (loi commutatif)}$$

Donc : $a * b \in (a' * b') * H$ et donc $(a * b) * H \subset (a' * b') * H$. De même on peut montrer que $(a' * b') * H \subset (a * b) * H$. □

Proposition 2.1.1. *$(G/H, \circledast)$ est un groupe commutatif. Soit e l'élément neutre de G, l'élément neutre de G/H est $e * H$.*

Exemple 2.1.2. $G = \mathbb{Z}$, $* = +$, $H = n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ est un sous-groupe commutatif.

Définition 2.1.3. Soit $(A, +, .)$ un anneau commutatif donc $(A, +)$ est un groupe commutatif. Soit I un sous-groupe de $(A, +)$ et :

$$A/I = \{a + I,\ a \in A\}$$

On définit dans A/I l'opération :

$$(a + I) \oplus (b + I) = (a + b) + I$$

On a : $(A/I, \oplus)$ est un groupe commutatif. Soit l'opération $\odot$:

$$(a + I) \odot (b + I) = (a.b) + I$$

On veut que cette opération ait un sens. Soit $a, b, a', b' \in A$ tels que :

$$a + I = a' + I \text{ et } b + I = b' + I$$

On veut que $a.b + I = a'b' + I$:

$$a + I = a' + I \Rightarrow \exists i \in I \text{ tel que } a = a' + i$$

$$b + I = b' + I \Rightarrow \exists i' \in I \text{ tel que } b = b' + i'$$

Donc :

$$(a.b) = (a' + i).(b' + i') = a'.b' + i.b' + a'.i' + i.i'$$

On veut que $i.b' + a'.i + i.i' \in I$. En particulier, il faut que pour tout $a \in A$:

$$(a + I) \odot (0 + I) = a.0 + I = 0.I$$

Pour cela, il faut que :

$$\forall a \in A,\ \forall i \in I,\ a.i \in I \qquad (*)$$

Réciproquement, si on a la propriété $(*)$ alors la multiplication $\odot$ a un sens.

Résumé. Soit $(A, +, .)$ un anneau commutatif, I est un sous-groupe de $(A, +)$ et $A/I = \{a + I, a \in A\}$.

- $(A/I, \oplus)$ est un groupe commutatif.
- On définit dans A/I l'opération $\odot$:

$$(a + I) \odot (b + I) = (a.b) + I$$

- Cette opération a un sens si et seulement si I vérifie en plus la propriété suivante :

$$\forall a \in A,\ \forall i \in I,\ a.i \in I$$

On dit alors que I absorbe par la multiplication tous les éléments de A.

2.2 Idéal

Définition 2.2.1. Soit $(A, +, .)$ un anneau commutatif et I est un sous-ensemble de A. I est un idéal de A si :

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

(ii) $\forall a \in A$, $\forall i \in I$, $a.i \in I$.

Proposition 2.2.1. *Soit $(A, +, .)$ un anneau commutatif et I un idéal de A. Alors $(A/I, \oplus, \odot)$ est un anneau commutatif. On a ainsi :*

$$0_{A/I} = 0_A + I = I \text{ et } 1_{A/I} = 1_A + I$$

Exemple 2.2.1. $(\mathbb{Z}/n\mathbb{Z}, \oplus, \odot)$ est un anneau commutatif.

Exemple 2.2.2. Les idéaux de $\mathbb{Z}$ sont $n\mathbb{Z}$, $n \in \mathbb{N}$. En effet :
- Les sous-groupes de $(\mathbb{Z}, +)$ sont $n\mathbb{Z}$, $n \in \mathbb{N}$.
- On vérifie que ces ensembles $n\mathbb{Z}$ absorbent les éléments de $\mathbb{Z}$.

Exemple 2.2.3. Si A est un anneau, $\{0\}$ et A sont des idéeaux de A.

Exemple 2.2.4. Les idéaux de :

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} \\ &= \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\} \end{aligned}$$

- $\{0\}$ et $\mathbb{Z}/6\mathbb{Z}$ sont des idéaux.
- Soit I un idéal de $\mathbb{Z}/6\mathbb{Z}$ tel que $I \neq \{\overline{0}\}$ et $I \neq \mathbb{Z}/6\mathbb{Z}$. Alors $\overline{0} \in I$.
- Si $\overline{1} \in I$, comme $\underbrace{\overline{a}.\overline{1}}_{\overline{a}} \in I$, $\forall a \in \mathbb{Z}/6\mathbb{Z}$ alors $I = \mathbb{Z}/6\mathbb{Z}$.
- Si $\overline{2} \in I$ alors $\{\overline{0}, \overline{2}, \overline{4}\} \subset I$, $\{\overline{0}, \overline{2}, \overline{4}\}$ est un sous-groupe de $(\mathbb{Z}/6\mathbb{Z}, +)$ et $\forall \overline{a} \in \mathbb{Z}/6\mathbb{Z}$ et $\overline{b} \in \{\overline{0}, \overline{2}, \overline{4}\}$:
$$\overline{a}\overline{b} = \overline{ab} = \{\overline{0}, \overline{2}, \overline{4}\}$$
$\{\overline{0}, \overline{2}, \overline{4}\}$ est un idéal de $\mathbb{Z}/6\mathbb{Z}$.
- On vérifie que $\{\overline{0}, \overline{3}\}$ est un idéal de $\mathbb{Z}/6\mathbb{Z}$.
- Si $\overline{5} \in I$, on vérifie que $I = \mathbb{Z}/6\mathbb{Z}$.

Propriété 2.2.2. *Soit A un anneau et I un idéal de A. Alors les propositions suivantes sont équivalents :*

(i) $I = A$

(ii) $1 \in I$

(iii) $\exists u \in A^\times$, $u \in I$

Démonstration. $(i) \Rightarrow (ii)$ évident

$(ii) \Rightarrow (iii)$ évident

$(iii) \Rightarrow (ii)$ On doit montrer qu'il existe $u \in A^\times$ tel que $u \in I$, alors $I = A$. Soit $a \in A$, montrer que $a \in I$. On a : $a = (au^{-1})u$. Comme $u \in I$, $au^{-1} \in A$ et I absorbe les éléments de A, $(au^{-1})u \in I$.

□

Conséquence. Soit K un corps et I un idéal. On suppose que $I \neq \{0\}$ donc il existe $u \in I$ avec $u \neq 0$. Comme $u \in K\backslash\{0\}$ et K est un corps, $u \in K^\times$. Donc I continent un élément inversible et donc $I = K$. Par conséquent, les idéaux d'un corps K sont $\{0\}$ et K. Réciproquement, soit A un anneau non nul. On suppose que les seuls idéaux de A sont $\{0\}$ et A. Alors A est un corps.

En effet, soit $a \in A\backslash\{0\}$; On montre que $a \in A^\times$. On considère l'ensemble $I = aA = \{ab, b \in A\}$. On vérifie que I est un idéal de A :

(i) $O_A = a0_A$, donc $0_A \in I$.

(ii) Soit $x, y \in I$, on pose $x = ab$ avec $b \in A$ et $y = ac$ avec $c \in A$. Alors $x + y = ab + ac = a(\underbrace{b + c}_{\in A}) \in I$

(iii) Soit $x \in I$ et $\alpha \in A$, on montre que $\alpha x \in I$. On pose $x = ab$, $b \in A$. Alors $\alpha x = \alpha(ab) = a'(\underbrace{\alpha b}_{\in A}) \in I$.

(iv) $a \in I$ pusique $a = a1_A$ et $a \neq 0$ donc $I \neq \{0\}$. Comme I est un idéal non nul de A et les idéaux de A sont $\{0\}$ et A, on déduit que $I = A$. En particulier, $1 \in I$ donc il existe $b \in A$ tel que $1 = ab$ et donc $a \in A^\times$.

2.3 Intersection, réunion d'idéaux

Proposition 2.3.1. *Soit $(I_i)_{i\in F}$ une famille d'idéaux d'un anneau A. Alors $\bigcap_{i\in F} I_i$ est un idéal de A.*

Proposition 2.3.2. *Soit I et J des idéaux de A. Alors $I \cup J$ est un idéal de $A \Leftrightarrow I \subset J$ ou $J \subset I$.*

Démonstration. ($\Leftarrow$) évident.

($\Rightarrow$) $I \cup J$ est un idéal de $A \Rightarrow I \cup J$ est un sous-groupe de $(A, +)$. Or la réunion des deux sous-groupes n'est un sous-groupe que si l'un des sous-groupes est contnue dans l'autre. □

Exercice 2.3.1. Soit $m, n \in \mathbb{N}^*$. Montrer que :

$$n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{PPCM}(n, m)\mathbb{Z}$$

2.4 Idéal engendré par une partie

Définition 2.4.1. Soit A un anneau et B une partie non vide de A. L'idéal engendré par B, qu'on note (B) est le plus petit idéal de A qui contient B.

Proposition 2.4.1.

$$(B) = \bigcap_{\substack{I \text{ idéal de } A \\ B\subset I}} I$$

Démonstration. On pose :

$$J = \bigcap_{\substack{I \text{ idéal de } A \\ B\subset I}} I$$

- J est un idéal de A qui contient B. Donc $(B) \subset J$.
- On montre que $J \subset (B)$.

Comme J est l'intersection de tous les idéaux qui contiennent B et (B) est un idéal qui contient B, $J \subset (B)$. □

Proposition 2.4.2.

$$(B) = \{a_1b_1 + ... + a_kb_k,\ a_i \in A,\ b_i \in B,\ k \geq 1\}$$

Démonstration. On pose :

$$I = \{a_1b_1 + ... + a_kb_k,\ a_i \in A,\ b_i \in B,\ k \geq 1\}$$

On montre que I est un idéal qui contient B.

(i) $B \neq \emptyset \Rightarrow \exists b \in B$, on a $0_A = 0_A b \in I$.

(ii) Soit $x, y \in I$, on montre que $x, y \in I$. On pose :

$$x = a_1b_1 + ... + a_kb_k,\ a_i \in A,\ b_i \in B$$

$$y = a'_1b'_1 + ... + a'_kb'_k,\ a'_i \in A,\ b'_i \in B$$

Alors :

$$x + y = a_1b_1 + ... + a_kb_k + a'_1b'_1 + ... + a'_kb'_k \in I$$

(iii) Soit $x \in I$ et $a \in A$. On montre que $a \in I$. On pose $x = a_1b_1 + ... + a_kb_k$, $a_i \in A$ et $b_i \in B$, $k \geq 1$:

$$a_x = a(a_1b_1 + ... + a_kb_k) = (\underbrace{aa_1})b_1 + ... + (\underbrace{aa_k})b_k \in I$$

(iv) Soit $b \in B$ alors $b = 1_A b \in I$.

Donc $B \subset I$. Comme I est un idéal de A qui contient B et (B) est le plus petit idéal de A qui contient B, $(B) \in I$.

On montre que $I \subset (B)$. Soit $x \in I$ alors x s'écrit :

$$x = a_1b_1 + ... + a_kb_k \text{ avec } a_i \in A,\ b_i \in B,\ k \geq 1$$

Soit $1 \leq i \leq k$, $b_i \in B$. Comme (B) contient B, $b_i \in (B)$. Or (B) est un idéal donc :

$$a_1b_1 + ... + a_kb_k \in (B)$$

□

Cas particulier. Soit A un anneau et $x_1, ..., x_m \in A$, l'idéal engendré par $x_1, ..., x_m$ qu'on note $(x_1, ..., x_n)$ est l'idéal engendré $\{x_1, ..., x_m\}$.

Conséquence.

$$\begin{aligned}(x_1, ..., x_n) &= \{a_1x_1 + ... + a_nx_n,\ a_i \in A\} \\ &= x_1A + ... + x_nA\end{aligned}$$

Exemple 2.4.1. On se place dans $\mathbb{Z}$.

- Soit $n \in \mathbb{Z}$, $(n) = n\mathbb{Z}$.
- Soit $n, m \in \mathbb{Z}$, $(n, m) = \{na + mb,\ a, b \in \mathbb{Z}\} = \text{PGCD}(m, n)\mathbb{Z}$

2.5 Somme de deux idéaux

Définition 2.5.1. Soit A un anneau, I et J des idéaux de A. La somme des idéaux I et J qu'on note $I+J$ est l'idéal engendré par l'ensemble $I \cup J$ et $I+J=(I,J)$.

Proposition 2.5.1. $I+J=\{i+j,\, i\in I,\, j\in J\}$

Démonstration. On a :

$$\begin{aligned} I+J &= \{a_1b_1+...+a_kb_k,\, a_i\in A,\ ,b_i\in I\sqcup J,\, k\geq 1\} \\ &= \{a_1i_1+...+a_ni_n+c_1j_1+...+c_mj_m,\, a_l,c_l\in A,\, i_l\in I,\, j_l\in J,\, n,m\geq 1\} \end{aligned}$$

Comme I et J sont des idéaux, les sommes :

$$a_1i_1+...+a_ni_n\in I$$

$$c_1j_1+...+c_mj_m\in J$$

Donc $I+J=\{i+j,\, i\in I,\, j\in J\}$. □

2.6 Produit d'idéaux

Définition 2.6.1. Soit A un anneau, I et J des idéaux de A. Le produit des idéaux I et J qu'on note IJ est l'idéal engendré par l'ensemble $\{ij,\, i\in I,\, j\in J\}$:

$$I.J=(ij,\, i\in I,\, j\in J)$$

Proposition 2.6.1.

$$IJ=\{i_1j_1+i_2j_1+...+i_kj_k,\, i_l\in I,\, j_l\in J,\, k\geq 1\}$$

Démonstration. On pose :

$$K=IJ=\{i_1j_1+...+i_kj_k,\, i_l\in I,\, j_l\in J,\, k\geq 1\}$$

On peut montrer que K est un idéal de A qui contient $\{ij,\, i\in I,\, j\in J\}$. K contient l'ensemble $\{ij,\, i\in I,\, j\in J\}$ et IJ est le plus petit idéal qui contient $\{ij,\, i\in I,\, j\in J\}$ donc $IJ\subset K$.

On montre que $K\subset IJ$. Soit $x\in K$, x s'écrit :

$$x=i_1j_1+...+i_kj_k,\, i_l\in I,\, j_l\in J$$

Soit $1\leq l\leq k$, $i_lj_l\in\{ij,\, i\in I,\, j\in J\}$. Comme IJ contient $\{ij,\, i\in I,\, j\in J\}$:

$$i_lj_l\in IJ,\, \forall l,\, 1\leq l\leq k$$

Or IJ est un idéal donc :

$$x=\sum_{l=1}^{k} i_lj_l\in IJ$$

□

Soit A un anneau, I un idéal de A et A/I l'anneau quotient. On donne, dans le paragraphe suivant, des conditions nécessaires et suffisantes sur I pour que l'anneau A/I soit intègre (respectivement un corps).

2.7 Idéal premier

Définition 2.7.1. Soit A un anneau non nul et I un idéal de A. I est un idéal de A si :

(i) $I \subsetneqq A$

(ii) $\forall a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$

.

Exemple 2.7.1. Les idéaux premiers de $\mathbb{Z}$ sont (0), $p\mathbb{Z}$ où p est un nombre premier de $\mathbb{Z}$. En effet,

(i) (0) est un idéal premier :
- $(0) = \{0\} \subsetneqq \mathbb{Z}$
- Soit $a, b \in \mathbb{Z}$ tel que $ab \in (0)$. Comme $\mathbb{Z}$ est un anneau intégre, $ab = 0 \Rightarrow a = 0$ ou $b = 0$ donc $a \in (0)$ et $b \in (0)$.

(ii) Soit p un nombre premier de $\mathbb{Z}$. On montre que (p) est un idéal premier.
- $(p) \subsetneqq \mathbb{Z}$
- Soit $a, b \in \mathbb{Z}$ tel que $ab \in (p)$. Comme p est premier, $a \in (p)$ ou $b \in (p)$.

(iii) Montrons qu'ils sont les seuls idéaux premiers. Soit I un idéal de $\mathbb{Z}$, alors il existe $n \in \mathbb{N}$ tel que $I = (n)$.
- Si $n = 0$, $I = (0)$ est un idéal premier.
- Supposons que $n \in \mathbb{N}^*$:

$$I = (n) \text{ idéal premier } \Rightarrow I \subsetneqq A \Rightarrow n \geq 2$$

Supposons que n n'est pas premier alors $n = n_1 n_2$ avec $n_1 > 1$ et $n_2 > 1$. Donc on a : $n_1 n_2 \in (n)$ mais $n_1 \notin (n)$ et $n_2 \notin (n)$. Donc (n) n'est pas un idéal premier.

Proposition 2.7.1. *Soit A un anneau non nul et I un idéal de A. Alors A/I est un anneau intégre si et seulement si I est un idéal premier.*

Démonstration. ($\Rightarrow$) A/I est un anneau intégre $\Rightarrow$ A/I est un anneau non nul $\Rightarrow$ $I \subsetneqq A$.
Soit $a, b \in A$ tels que $ab \in I$:

$$ab \in I \Rightarrow ab + I = 0_A + I \Rightarrow \underbrace{(a+I)}_{\in A/I}\underbrace{(b+I)}_{\in A/I} = 0_A + I = 0_{A/I}$$

Comme A/I est intégre, $a + I = 0_A + I$ ou $b + I = 0_A + I$. Donc $a \in I$ ou $b \in I$.

($\Leftarrow$) • $I \subsetneqq A \Rightarrow A/I$ est un anneau non nul.
- Soit $x, y \in A/I$ tels que $xy = 0_{A/I}$. Si $x, y \in A/I$ alors x et y s'écrivent :

$$x = a + I,\ y = b + I,\ a, b \in A$$

Donc :

$$xy = (a+I)(b+I) = ab + I = 0_{A/I} = 0_A + I$$

Donc : $ab \in I$. Comme I est premier, $a \in I$ ou $b \in I$. Donc : $x = a + I = 0_A + I = 0_{A/I}$ ou $y = b + I = 0_A + I = 0_{A/I}$.

□

2.8 Idéal maximal

Définition 2.8.1. Soit A un anneau non nul et I un idéal de A. I est un idéal maximal si :

(i) $I \subsetneqq A$

(ii) Dès qu'un idéal J contient I, alors $J = I$ ou $J = A$ (c'est-à-dire $\forall J$ idéal de A, $I \subset J \subset A \Rightarrow J = I$ ou $J = A$).

Exercice 2.8.1. Les idéaux maximaux de $\mathbb{Z}$ sont (p) où p est un élément premier de $\mathbb{Z}$.

Proposition 2.8.1. *Soit A un anneau nul et I un idéal de A. Alors A/I est un corps si et seulement si I est un idéal maximal.*

Démonstration. ($\Rightarrow$) • A/I est un corps $\Rightarrow A/I$ est un anneau non nul $\Rightarrow I \subsetneqq A$.

• Soit J un idéal de A tel que $I \subset J$. On montre que $J = I$ ou $J = A$. Supposons que $J \neq I$. On montre que $J = A$. $I \subsetneqq J \Rightarrow \exists j \in J$ tel que $j \in J$ et $j \notin I$. $j \notin I \Rightarrow j + I \neq 0_A + I = 0_{A/I}$. Comme A/I est un corps, il existe $a \in A$ tel que :

$$(j + J)(a + I) = 1_A + I$$

Donc : $\exists a \in A$ tel que $ja + I = 1_A + I$. Donc $\exists a \in A$, $\exists i \in I$ tel que $ja = 1 + i$. Comme $j \in J$, $i \in I \subset J$ et J est un idéal, $1 \in J$ donc $J = A$.

($\Leftarrow$) • $I \subsetneqq A \Rightarrow A/I$ est un anneau non nul.

• Soit $x \in A/I\backslash\{0_{A/I}\}$, on montre qu'il existe $y \in A/I$ tel que $xy = 1_{A/I}$. Comme $x \in A/I\backslash\{0_{A/I}\}$ alors x s'écrit $x = a+I$, $a \in A$ et $a \notin I$. Comme $a \notin I$, $I \subsetneqq (a, I) =: J$.

$$J = (a, I) = aA + I = (aA \cup I)$$

Comme I est maximal, $aA + I = A$. Donc il existe $b \in A$, $i \in I$ tel que $1 = ab + i$. Donc $ab + I = 1 + I$„ c'est-à-dire :

$$\underbrace{(a + I)}_{x}\underbrace{(b + I)}_{y} = 1_A + I = 1_{A/I}$$

On prend $y = b + I$. On a aussi $xy = 1_{A/I}$.

□

Corollaire. *Soit A un anneau non nul. Si I est un idéal maximal de A alors I est un idéal premier.*

Démonstration. I maximal $\Rightarrow A/I$ est un corps $\Rightarrow A/I$ est un anneau intégre $\Rightarrow I$ est un premier. □

Chapitre 3

Anneaux principaux et euclidiens - Morphismes d'anneaux

3.1 Anneau principal

Définition 3.1.1. Soit A un anneau non nul. I est un idéal principal, s'il est engendré par un élément de A.

Définition 3.1.2. Un anneau est principal si :

(i) A est un anneau intègre.

(ii) Tous ses idéaux sont principaux.

Exemple 3.1.1. $\mathbb{Z}$ est un anneau principal.

3.2 Anneau euclidien

Définition 3.2.1. Soit A un anneau non nul. A est euclidien si :

(i) A est un anneau intègre .

(ii) il existe une application $\varphi : A\backslash\{0_A\} \to \mathbb{N}$ qui vérifie $\forall a \in A$, $\forall b \in A\backslash\{0\}$, il existe $q, r \in A$ tels que :

$$a = bq + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(b)$$

Exemple 3.2.1. 1) $\mathbb{Z}$ est un anneau euclidien :

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \to & \mathbb{N} \\ & & a & \mapsto & |a| \end{array}$$

$\forall a \in \mathbb{Z}$, $\forall b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ tels que $a = bq + r$ avec $r = 0$ ou $|r| < |b|$.

2) $\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\}$ avec $i^2 = -1$. $\mathbb{Z}[i]$ est un anneau euclidien.

- $\mathbb{Z}[i]$ est un anneau intégre ($\mathbb{Z}[i] \subset \mathbb{C}$)
- On considère l'application :

$$\begin{array}{rccc} N & : & \mathbb{Z}[i] & \to & \mathbb{N} \\ & & z = a + ib & \mapsto & |z|^2 = a^2 + b^2 \end{array}$$

On montre que $(\mathbb{Z}[i], N)$ est un anneau euclidien. Soit $x \in \mathbb{Z}[i]$, $y \in \mathbb{Z}[i]\backslash\{0\}$. On montre qu'il existe $q, r \in \mathbb{Z}[i]$ tels que $x = yq + r$ avec $r = 0$ ou $N(r) < N(y)$. On pose :

$$\frac{x}{y} = \alpha + i\beta,\ \alpha, \beta \in \mathbb{Q}$$

Soit $a, b \in \mathbb{Z}$ les entiers les plus proches de α et β respectivement alors $|\alpha - a| \leq 1/2$ et $|\beta - b| \leq 1/2$. On pose $q = a + ib \in \mathbb{Z}$ et $1 = x - yq$. On a $r \in \mathbb{Z}[i]$ et :

$$\begin{aligned} N(r) &= |r|^2 = |y|^2 \left|\frac{x}{y} - q\right|^2 \\ &= |y|^2|(\alpha - a) + i(\beta - b)|^2 \\ &= |y|^2(\alpha - a)^2 + (\beta - b)^2 \\ &\leq |y|^2 \left(\frac{1}{4} + \frac{1}{4}\right) < |y|^2 = N(y) \end{aligned}$$

Proposition 3.2.1. *Si A est un anneau euclidien alors A est un anneau principal.*

Démonstration. Soit I un idéal de A, on montre qu'il existe $a \in A$ tel que $I = (a)$. On suppose que (A, φ) est euclidien.

- Si $I = \{0\}$ alors $I = (0)$.
- On suppose que $I \neq 0$. On considère l'ensemble :

$$\emptyset \neq \{\varphi(a),\, a \in I\backslash\{0\}\} \subset \mathbb{N}$$

Donc il existe $a_0 \in I\backslash\{0\}$ tel que $\varphi(a)$ est minimal. On montre que $I = (a_0) = a_0A$.

– $a_0 \in I \Rightarrow (a_0) \subset I$

– Soit $a \in I$ alors il existe $q, r \in A$ tel que ;

$$a = a_0q + r \text{ avec } r = 0 \text{ ou } \varphi(r) < \varphi(a_0)$$

On montre que $r = 0$. Supposons que $r \neq 0$ alors $\varphi(r) < \varphi(a_0)$.

$$\left.\begin{array}{l} a_0, a \in I \\ I \text{ est un idéal} \end{array}\right\} \Rightarrow \underbrace{a - a_0q}_{=r} \in I$$

Donc $r \in I\backslash\{0\}$ et $\varphi(r) < \varphi(a_0)$. Ce qui contredit le fait que :

$$\varphi(a_0) = \min\{\varphi(x),\, x \in I\backslash\{0\}\}$$

□

3.3 Morphismes d'anneaux

Définition 3.3.1. Soit A et B des anneaux et $f : A \to B$ une application. f est un morphisme d'anneau si :

(i) $\forall x, y \in A,\ f(x +_A y) = f(x) +_B f(y)$ (f est un morphisme du groupe $(A, +_A)$ dans $(B, +_B)$).

(ii) $\forall x, y \in A,\ f(x \times_A y) = f(x) \times_B f(y)$

(iii) $f(1_A) = 1_B$

Propriété 3.3.1. *Soit $f : A \to B$ un morphisme d'anneaux. Alors :*

(i) $f(0_A) = 0_B$ *et* $\forall x \in A,\ f(-x) = -f(x)$

(ii) $\mathrm{Ker}(f) = \{x \in A, f(x) = 0_B\}$ *est un idéal de A.*

(iii) $\mathrm{Im}(f) = f(A) = \{f(x), x \in A\}$ *est un sous-anneau de B.*

(iv) f est injective $\Leftrightarrow \operatorname{Ker} f = \{0_A\}$ *et f est surjective* $\Leftrightarrow f(A) = B$.

Démonstration. (*ii*) a) $f(0_A) = 0_B \Rightarrow 0_A \in \operatorname{Ker} f$

b) Soit $x, y \in \operatorname{Ker} f$, montrons que $x + y \in \operatorname{Ker} f$:

$$x \in \operatorname{Ker} f \Rightarrow f(x) = 0_B,\ y \in \operatorname{Ker} f \Rightarrow f(y) = 0_B$$

Comme f est un morphisme, $f(x + y) = f(x) + f(y) = 0_B$.

c) Soit $a \in A$, $x \in \operatorname{Ker} f$, on montre que $ax \in \operatorname{Ker} f$:

$$f(ax) = f(a)f(x) = f(x)0_B = 0_B$$

(*iii*) a)

$$0_B = f(0_A) \Rightarrow 0_B \in f(A),\ 1_B = f(1_A) \Rightarrow 1_B \in f(A)$$

b) Soit $x, y \in f(A)$, on montre que $x + y \in f(A)$ et $xy \in f(A)$. On pose $x = f(a)$ et $y = f(b)$ avec $a, b \in A$.

$$x + y = f(a) + f(b) = f(a + b) \in f(A)$$

$$xy = f(a)f(b) = f(ab) \in f(A)$$

□

Exemple 3.3.1 (de morphisme d'anneaux)**.** Soit A un anneau et I un idéal de A. Soit :

$$\begin{array}{rccc} s & : & A & \to & A/I \\ & & a & \mapsto & a + I \end{array}$$

s est un morphisme d'anneau surjectif. Soit $a, b \in A$:

$$\begin{aligned} s(a + b) &= a + b + I = (a + I) + (b + I) = s(a) + s(b) \\ s(ab) &= ab + I = (a + I).(b + I) = s(a)s(b) \\ s(1_A) &= 1_A + I = 1_{A/I} \end{aligned}$$

On appelle s la surjection canonique.

3.4 Transfert d'un idéal par un morphisme

Proposition 3.4.1. *Soit $f : A \to B$ un morphisme. Alors :*

1) Si J est un idéal de B, $f^{-1}(J) = \{x \in A,\ f(x) \in J\}$ est un idéal de A qui contient $\operatorname{Ker} f$.

2) Si I est un idéal de A, $f(I)$ n'est pas nécessairement un idéal de B. Par contre, si f est surjectif, $f(I)$ est un idéal de B.

3) On suppose que f est surjectif. On a une bijection entre les idéaux de A qui contient $\operatorname{Ker} f$ *et les idéaux de B. On pose :*

$$\begin{aligned} \mathcal{I}_A^* &= \{\textit{les idéaux de } A \textit{ qui contient } \operatorname{Ker} f\} \\ \mathcal{I}_B &= \{\textit{les idéaux de } B\} \end{aligned}$$

et :

$$\begin{array}{rccc} \varphi & : & \mathcal{I}_A^* & \to & \mathcal{I}_B \\ & & I & \mapsto & f(I) \end{array}$$

φ est une bijection.

Démonstration. 1) Soit J un idéal de B.

$$x \in f^{-1}(J) \Leftrightarrow f(x) \in J$$

(i) On a $f(0_A) = 0_B$ et $0_B \in J$, puisque que J est un idéal de B. Donc $0_A \in f^{-1}(J)$.

(ii) Soit $x, y \in f^{-1}(J)$, $x + y \in f^{-1}(J)$?

$$x, y \in f^{-1}(J) \Leftrightarrow f(x), f(y) \in J$$

Comme f est un morphisme, $f(x+y) = f(x) + f(y)$ et comme $f(x), f(y) \in J$ et J est un idéal, $f(x + y) \in J$ et donc $x + y \in f^{-1}(J)$.

(iii) Soit $a \in A$, $x \in f^{-1}(J)$. On montre que $ax \in f^{-1}(J)$. $x \in f^{-1}(J) \Rightarrow f(x) \in J$. Comme f est un morphisme $\Rightarrow f(ax) = f(a)f(x)$. Comme J est un idéal de B, $f(a)f(x) \in J$. Donc : $ax \in f^{-1}(J)$.

(iv) Montrons que $\operatorname{Ker} f \subset f^{-1}(J)$. Soit $x \in \operatorname{Ker} f$, alors $f(x) = 0_B \in J$ donc $x \in f^{-1}(J)$.

2)

Exemple 3.4.1. Soit :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & \mathbb{Q} \\ & & k & \mapsto & k \end{array}$$

Soit $I = 2\mathbb{Z}$ est un idéal de $\mathbb{Z}$, $f(I) = I = 2\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$ (tous les idéaux de $\mathbb{Q}$ sont $\{0_{\mathbb{Q}}\}$ et $\mathbb{Q}$.

On suppose que f est surjective. Soit I un idéal de A. On montre que $f(I)$ est un idéal de B.

(i) $0_B = f(0_A)$ et $0_A \in I$ donc $0_B \in f(I)$.

(ii) Soit $x, y \in f(I)$. On montre que $x + y \in f(I)$:

$$x + y \in f(I) \Rightarrow \exists x', y' \in I,\ x = f(x') \text{ et } y = f(y')$$

Comme f est un morphisme, $x + y = f(x' + y')$. Comme I est un idéal, $x' + y' \in I$. Donc $x + y \in f(I)$.

(iii) Soit $b \in B$ et $x \in f(I)$. On montre que $bx \in f(I)$.

$$x \in f(I) \Rightarrow \exists x' \in I,\ x = f(x')$$

Comme f est surjective, il existe $a_i nA$ tel que $b = f(a)$. Comme f est un morphisme, $bx = f(ax)$. Comme I est un idéal, $a \in A$ et $x' \in I$, $ax' \in I$. Donc $bx \in f(I)$.

3) On suppose que f est surjective. Soit :

$$\begin{array}{rccc} \varphi & : & \mathcal{I}_A^* & \to & \mathcal{I}_B \\ & & I & \mapsto & f(I) \end{array}$$

On montre que φ est bijective.

(i) Soit $J \in \mathcal{I}_B$ alors $f^{-1}(J) \in \mathcal{I}_A^*$. Comme f est surjective, $f(f^{-1}(J)) = J$. Donc $J = \varphi(f^{-1}(J))$.

(ii) Soit $I, I' \in \mathcal{I}_A^*$ tels que $\varphi(I) = \varphi(I')$[1]. On montre que $I = I'$. Soit $i \in I$, comme $f(I) = f(I')$, il existe $i' \in I$ tel que $f(i) = f(i')$.

$$f(i) = f(i') \Rightarrow i - i' \in \operatorname{Ker} f \subset I'$$

Comme $\operatorname{Ker} f \subset I'$ et I' est un idéal, $i \in I'$. Comme I et I' joue un même rôle, on a aussi $I' \subset I$. Donc $I = I'$.

[1] cela veut dire que $f(I) = f(I')$

□

Corollaire. *Soient A un anneau et I un idéal de A. Alors les idéaux de A/I sont J/I où J est un idéal de A qui contient I.*

Démonstration. Soit :

$$\begin{array}{rccc} s & : & A & \to & A/I \\ & & a & \mapsto & a+I \end{array} \quad \text{surjection canonique}$$

,

$$\operatorname{Ker} s = \{a \in A,, a + I = 0_A + I\} = I$$

D'après la **Proposition 3.4.1**, un idéal de A/I est $s(I')$ où I' est un idéal de A qui contient I.

$$s(I') = \{s(i'),\, i' \in I\} = \{i' + I,\, i' \in I'\} = I'/I$$

□

Exemple 3.4.2. Soit $n \in \mathbb{N}^*$. On cherche les idéaux de $\mathbb{Z}/n\mathbb{Z}$. Soit :

$$\begin{array}{rccc} s & : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & & k & \mapsto & k + n\mathbb{Z} \end{array}$$

Soit $I/n\mathbb{Z}$ où I est un idéal de $\mathbb{Z}$ qui contient $n\mathbb{Z}$. On pose $I = m\mathbb{Z}$ où $m \in \mathbb{N}$ et $m\mathbb{Z} \subset n\mathbb{Z} \Leftrightarrow m|n$. Donc les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont $m\mathbb{Z}/n\mathbb{Z}$ où $m \in \mathbb{Z}$.

On prend par exemple $n = 5$. Les idéaux de $\mathbb{Z}/5\mathbb{Z}$ sont $m\mathbb{Z}/5\mathbb{Z}$ tel que $m \in \mathbb{N}$, $m|5$. Les seuls idéaux de $\mathbb{Z}/5\mathbb{Z}$ sont :

$$\mathbb{Z}/5\mathbb{Z},\, 5\mathbb{Z}/5\mathbb{Z} = \{0_{\mathbb{Z}/5\mathbb{Z}}\}$$

On prend maintenant $n = 6$. Les idéaux de $\mathbb{Z}/6\mathbb{Z}$ sont :

$$\mathbb{Z}/6\mathbb{Z},\, 2\mathbb{Z}/6\mathbb{Z},\, 3\mathbb{Z}/6\mathbb{Z},\, 6\mathbb{Z}/6\mathbb{Z} = \{0_{\mathbb{Z}/6\mathbb{Z}}\}$$

On montre que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont principaux. Soit $I = m\mathbb{Z}/n\mathbb{Z}$ avec $m, n \in \mathbb{N}$ et $m|n$, un idéal de $\mathbb{Z}/n\mathbb{Z}$.

$$m\mathbb{Z}/n\mathbb{Z} = \{mk + n\mathbb{Z}, k \in \mathbb{Z}\} = \{(m + n\mathbb{Z})(k + n\mathbb{Z}), k \in \mathbb{Z}\} = (m + n\mathbb{Z})(\mathbb{Z}/n\mathbb{Z}) = \Big(m + n\mathbb{Z}\Big)$$

3.5 Factorisation d'un morphisme

Theorème 3.5.1. *Soit $f : A \to B$ un morphisme d'anneaux et I un idéal de A tel que $I \subset \operatorname{Ker} f$. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A/I \to B$ qui vérifie $\tilde{f} \circ s = f$ et $\operatorname{Ker} \tilde{f} = \operatorname{Ker} f/I$. On a ainsi le diagramme commutatif suivant :*

$$\begin{array}{ccccc} a & & A & \xrightarrow{f} & B \\ s\downarrow & & \downarrow & \nearrow_{\tilde{f}} & \\ a+I & & A/I & & \end{array}$$

Démonstration. (i) Soit $g : A/I \to B$ un morphise qui vérifie $g \circ s = f$. Soit $\alpha = a + I$ avec $\alpha \in A$. Alors :

$$g(\alpha) = g \circ s(a) = f(a)$$

(ii) Soit :

$$\begin{array}{rccc} g & : & A/I & \to & B \\ & & a+I & \mapsto & f(a) \end{array}$$

On vérifie que g est bien définie. Soit $a, b \in A$ tels que $a + I = b + I$. On montre que $f(a) = f(b)$.

$$a + I = b + I \Rightarrow a - b \in I$$

Comme $I \subset \operatorname{Ker} f$, $f(a - b) = 0$ et donc $f(a) = f(b)$.

(iii) Soit :

$$\begin{array}{rccc} g & : & A/I & \to & B \\ & & a+I & \mapsto & f(a) \end{array}$$

On montre que g est un morphisme d'anneaux.

- Soit $a, b \in A$:

$$g((a + I) + (b + I)) = g((a + b) + I) = f(a + b) = f(a) + f(b) = g(a + I) + g(b + I)$$

- Même chose pour le produit et pour l'élément unité.

□

Corollaire. *Soit $f : A \to B$ un morphisme d'anneaux. Alors :*

$$\begin{array}{rccc} \tilde{f} & : & A/\operatorname{Ker} f & \to & B \\ & & a + \operatorname{Ker} f & \mapsto & f(a) \end{array}$$

est un morphisme d'anneaux injectif.

Démonstration. Reste à prouver que $\tilde{f}$ est injectif :

$$\begin{array}{rcl} \operatorname{Ker} \tilde{f} & = & \{a + \operatorname{Ker} f,\ \tilde{f}(a + \operatorname{Ker} f) = 0_B\} \\ & = & \{a + \operatorname{Ker} f,\ f(a) = 0_B\} \\ & = & \{a + \operatorname{Ker} f,\ a \in \operatorname{Ker} f\} \\ & = & \{0_A + \operatorname{Ker} f\} = 0_{A/\operatorname{Ker} \tilde{f}} \end{array}$$

□

Remarque. Soit $f : A \to B$ un morphisme d'anneaux. Alors :

$$\begin{array}{rccc} \tilde{f} & : & A/\operatorname{Ker} f & \to & f(A) \\ & & a + \operatorname{Ker} f & \mapsto & f(a) \end{array}$$

$\tilde{f}$ est un isomorphisme d'anneaux.

Définition 3.5.1. La factorisation d'un morphisme $f : A \to B$ est la donnée du diagramme :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ s \downarrow & & \uparrow i \\ A/\operatorname{Ker} f & \xrightarrow{\tilde{f}} & f(A) \end{array}$$

Corollaire. *Soit A un anneau, I et J des idéaux de A tels que $I \subset J$. Alors on a un morphisme d'anneaux surjectif*

$$\begin{array}{rccc} f & : & A/I & \to & A/J \\ & & a + I & \mapsto & a + J \end{array}$$

Démonstration. • Vérifions que f est bien définie. Soit $a, b \in A$ tels que $a + I = b + I$. On montre que $a + J = b + J$.

$$a + I = b + I \Rightarrow a - b = I$$

Comme $I \subset J$, $a - b \in J$ donc $a + J = b + J$.

• f est un morphisme d'anneaux.

(i) Soit $a, b \in A$

$$f((a+I)+(b+I)) = f((a+b)+I)) = (a+b)+J = (a+J)+(b+J) = f(a+I)+f(b+I)$$

(ii)

$$f((a + I)(b + I)) = f(ab + I) = ab + J = (a + J)(b + J) = f(a + I)f(b + I)$$

(iii)

$$f(1_{A/I}) = f(1_A + I) = 1_A + J = 1_{A/J}$$

– f est surjective. Soit $\alpha \in A/J$, α s'écrit $\alpha = a + J$ avec $a \in A$. Donc : $\alpha = f(a + I)$.

□

Remarque.

$$\text{Ker } f = \{a + I,\ a + J = J\} = \{a + I,\ a \in J\} = J/I$$

D'après la factorisation canonique, on en déduit que :

$$(A/I)/(J/I) \overset{\text{isom}}{\simeq} A/J$$

Exemple 3.5.1. Soit $m, n \in \mathbb{N}^*$ tel que m divise n. Alors on a un morphisme surjectif.

$$\begin{array}{rccc} f & : & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ & & a + n\mathbb{Z} & \mapsto & a + m\mathbb{Z} \end{array}$$

On a donc :

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \overset{\text{isom}}{\simeq} \mathbb{Z}/n\mathbb{Z}$$

3.6 Caractéristique d'un anneau

Définition 3.6.1. Soit A un anneau non nul et f le morphisme d'anneau (à vérifier) :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & A \\ & & k & \mapsto & k1_A \end{array}$$

où :

$$k1_A = \begin{cases} 1_A + ... + 1_A,\ k \text{ fois, si } k > 0 \\ 0 \text{ si } k = 0 \\ (-1_A) + ... + (-1_A),\ -k \text{ fois, si } k < 0 \end{cases}$$

On a :

$$\text{Ker } f = \{k \in \mathbb{Z},\ k1_A = 0_A\} \in \mathcal{I}_{\mathbb{Z}}$$

Comme Ker f est un idéal de $\mathbb{Z}$, il existe $n \geq 0$ tel que Ker $f = n\mathbb{Z}$. On appelle n la caractéristique de l'anneau A.

- Si $n = 0$, $\forall k \in \mathbb{Z}$, $k1_A = 0_A \Rightarrow k = 0$.
- Si $n = 1 \Leftrightarrow A = \{0\}$.
- Si $n \geq 2$, n est le plus petit entier > 1 qui vérifie $n1_A = 0_A$. En effet, soit n_0 le plus petit entier tel que $n_0 1_A = 0_A$. Donc $n_0 \in \operatorname{Ker} f = n\mathbb{Z}$ donc $n|n_0 \Rightarrow n_0 = nk$, $k \in \mathbb{N}$. Or pour que n_0 soit le plus petit entier > 1, $n_0 = n$ $(n1_A = 0_A)$.

Exemple 3.6.1.
- On cherche $\operatorname{Car}(\mathbb{Z})$[2]. Soit $k \in \mathbb{Z}$, $k.1 = 0 \Rightarrow k = 0$.
- On cherche $\operatorname{Car}(\mathbb{Z}/5\mathbb{Z})$. Soit $k \in \mathbb{Z}$, $k.1_{\mathbb{Z}/5\mathbb{Z}} = 0_{\mathbb{Z}/5\mathbb{Z}} \Leftrightarrow k(1 + 5\mathbb{Z}) = 5\mathbb{Z} \Leftrightarrow k \in 5\mathbb{Z} \Leftrightarrow \operatorname{Car}(\mathbb{Z}/5\mathbb{Z} = 5$.
- On peut montrer que pour $n \in \mathbb{N}$ alors $\operatorname{Car}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 3.6.1. *Soit A un anneau non nul. Alors :*

1) Si $\operatorname{Car}(A) = 0$ *alors A contient un sous-anneau isomorphe à $\mathbb{Z}$.*

2) Si $\operatorname{Car}(A) = n > 1$ *alors A contient un sous-anneau isomorphe à $\mathbb{Z}$.*

Démonstration. On a le morphisme suivant :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & A \\ & & k & \mapsto & k1_A \end{array}$$

D'après la factorisation canonique de f, on a :

$$(\mathbb{Z}/\operatorname{Ker} f) \overset{\text{isom}}{\simeq} f(\mathbb{Z})$$

1) Si $\operatorname{Car}(A) = 0$ alors $\mathbb{Z}/\{0\} \overset{\text{isom}}{\simeq} \mathbb{Z} \overset{\text{isom}}{\simeq} f(\mathbb{Z})$, comme $f(\mathbb{Z})$ est un sous-anneau de A, A contient un sous-anneau isomorphe à $\mathbb{Z}$.

2) Si $\operatorname{Car}(A) = n > 1$ alors $\mathbb{Z}/n\mathbb{Z} \overset{\text{isom}}{\simeq} f(\mathbb{Z})$. Donc A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

□

Proposition 3.6.2. *Soit A un anneau intégre.*

$$\operatorname{Car}(A) = \begin{cases} 0 \\ \quad ou \\ p \text{ nombre premier} \end{cases}$$

(en particulier, si A est un corps).

Démonstration. On suppose que $\operatorname{Car}(A) = n > 1$. On a :

$$\mathbb{Z}/n\mathbb{Z} \overset{\text{isom}}{\simeq} f(\mathbb{Z})$$

où :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & A \\ & & k & \mapsto & k1_A \end{array}$$

Comme A est intégre et $f(\mathbb{Z})$ est un sous-anneau de A, $f(\mathbb{Z})$ est intégre donc $\mathbb{Z}/n\mathbb{Z}$ est intégre et donc n est forcément premier. □

[2] $\operatorname{Car}(A)$ = le caractéristique de l'anneau A

Chapitre 4

Polynômes

4.1 Anneau de polynômes à une indeterminée

4.1.1 Définitions

Voir **M103 Chapitre 1**.

Définition 4.1.1. Soit A un anneau, un polynôme à coefficients dans A est une expression :

$$a_0 + a_1X + ... + a_nX^n$$

où $n \in \mathbb{N}$, $a_i \in A$, X est une indéterminée.

Un polynôme est nul si tous les coefficients sont nuls.

Notation. On note $A[X]$ l'ensemble des polynômes à coefficients dans A.

Définition 4.1.2. Soit $P \in A[X]$ non nul. On pose $P = a_0 + a_1X + ... + a_nX^n$ avec $n \in \mathbb{N}$, $a_i \in A$, $a_n \neq 0_A$.

1) a_n est appelé le coefficient dominant de P.

2) Le degré de P ($\deg(P)$) est $n \in \mathbb{N}$. Par convention, le degré du polynôme nul est $-\infty$.

4.1.2 Addition et multiplication dans $A[X]$

Définition 4.1.3. Soit :

$$\begin{aligned} P &= a_0 + a_1X + ... + a_nX^n, \quad n \in \mathbb{N},\ a_i \in A \\ Q &= b_0 + b_1X + ... + b_mX^m, \quad n \in \mathbb{N},\ b_i \in A \end{aligned}$$

- $P + Q = (a_0 + b_0) + (a_1 + b_1)X + ...$
- $PQ = c_0 + c_1X + ... + c_{n+l}X^{n+m}$ où

$$c_i = \sum_{k+l} a_k b_l$$

Proposition 4.1.1. *$(A[X], +, .)$ est un anneau où :*

$$0_{A[X]} = 0 + 0X + ... + 0X^n + ...$$

$$1_{A[X]} = 1_A + 0X + 0X^2 + ... + 0X^n + ...$$

Proposition 4.1.2. *Soit :*

$$\begin{array}{rccc} f & : & A & \to & A[X] \\ & & a & \mapsto & a + 0X + 0X^2 + ... + 0X^n + ... \end{array}$$

Alors f est un morphisme d'anneaux injectif. Ceci permet d'identifier A comme un sous-anneau de $\{aX^0,\ a \in A\}$.

4.1.3 Degré d'un polynôme

Proposition 4.1.3. *Soit A un anneau et $P, Q \in A[X]$. Alors :*

1) $\deg(P+Q) \leq \max(\deg P, \deg Q)$. *De plus, si* $\deg P \neq \deg Q$ *alors :*

$$\deg(P+Q) = \max(\deg P, \deg Q)$$

2) $\deg(PQ) \leq \deg(P) + \deg(Q)$. *De plus, si on pose :*

$$\begin{aligned} P &= a_0 + a_1X + ... + a_nX^n, \quad a_n \neq 0 \\ Q &= b_0 + b_1X + ... + b_mX^m, \quad b_m \neq 0 \end{aligned}$$

et si $a_nb_m \neq 0$ alors $\deg(PQ) = \deg P + \deg Q$. *En particulier, si A est intégre :*

$$\deg(PQ) = \deg P + \deg Q$$

Exemple 4.1.1. On se place dans $\mathbb{Z}/4\mathbb{Z}[X]$. Soit :

$$\begin{aligned} P &= \overline{2}X + \overline{1} = (2 + 4\mathbb{Z})X + (1 + 4\mathbb{Z}) \\ P^2 &= \overline{4}X^2 + \overline{4}X + \overline{1} = \overline{1} \end{aligned}$$

Donc : $\deg(P^2) = 0$.

4.1.4 $A[X]$: Intégrité et éléments inversibles

Proposition 4.1.4. *Soit A un anneau intégre. Alors :*

1) $A[X]$ est intégre.

2) $(A[X])^\times = A^\times$

Démonstration. 1) Soit $P, Q \in A[X]$ tels que $PQ = 0$. On montre que $P = 0$ ou $Q = 0$. On suppose que $P \neq 0$ et $Q \neq 0$. On pose :

$$\begin{aligned} P &= a_0 + a_1X + ... + a_nX^n, \quad a_i \in A,\ a_n \neq 0 \\ Q &= b_0 + b_1X + ... + b_mX^m, \quad b_i \in A,\ b_m \neq 0 \end{aligned}$$

Alors :

$$PQ = a_nb_mX^{n+m} + ... + a_0b_0$$

Comme $a_n \neq 0$ et $b_m \neq 0$ et A est intégre, $a_nb_m \neq 0$. Donc $PQ \neq 0$. Ce qui contredit le fait que $PQ = 0$.

2) – On a $A^\times \subset (A[X])^\times$
– Soit $P \in (A[X])^\times$ alors il existe $Q \in A[X]$ tel que $PQ = 1_A$. Comme A est intégre, $\deg(PQ) = \deg P + \deg Q$. Or $PQ = 1$ et $\deg(PQ) = 0$. Donc $\deg P = \deg Q = 0$. Par conséquent, $P, Q \in A$. Comme $PQ = 1_A$, $P \in A^\times$.

□

Exemple 4.1.2.
– $(\mathbb{Z}[X])^\times = \mathbb{Z}^\times = \{-1, 1\}$.
– Si K est un corps, $(K[X])^\times = K^\times = K\backslash\{0\}$.

4.1.5 Division euclidienne

Proposition 4.1.5. *Soit A un anneau non nul. $V \in A[X]$ tel que $V \neq 0$ et le coefficient dominant de V est inversible dans A. Soit $U \in A[X]$ alors il existe $Q, R \in A[X]$ uniques tel que $U = VQ + R$ avec $\deg R < \deg V$.*

Démonstration. On pose $V = a_m X^m + ... + a_1 X + a_0$ avec $a_i \in A$, $a_m \neq 0$ et $a_m \in A^\times$. Soit $U \in A[X]$ de degré $n \in \mathbb{N} \cup \{-\infty\}$.

- Si $n < m$, on a $U + V0 + U$ et $\deg U < \deg V = m$. On fait une reccurence sur m. On suppose que $n \geq m$ et qu'on a une division euclidienne pour tout polynôme U de degré $< n$. On considère un polynôme U de degré n. On pose :

  $$U = b_n X^n + ... + b_1 X + b_0,\ b_i \in A$$

  On a :

  $$U = b_n a_m^{-1} X^{n-m} V + U'$$

  où $U' \in A[X]$ de degré $< n$. D'après l'hypothèse de reccurence, il existe $Q, R \in A[X]$ tels que :

  $$U' = VQ + R \text{ avec } \deg(R) < \deg V$$

  On déduit que $U = (b_n a_m^{-1} X^{n-m} + Q)V + R$ avec $\deg R < \deg V$.
- Unicité du quotient et du reste. On suppose que :

  $$U = VQ + R = VQ' + R' \tag{4.1}$$

  avec

  $$\deg R < \deg V,\ \deg R' < \deg V'$$

  $$(4.1) \Rightarrow V(Q - Q') = R - R' \text{ avec } \deg(R - R') < \deg V$$

  On suppose que $Q - Q' \neq 0$. On pose :

  $$\begin{array}{rcll} Q - Q' & = & a_0 + a_1 X + ... + a_n X^n, & a_n \neq 0 \\ V & = & b_m X^m + ... + b_0, & b_i \in A,\ b_n \in A^\times \end{array}$$

  Donc :

  $$V(Q - Q') = a_n b_m X^{n+m} + ... + a_0 b_0$$

  On montre que $a_n b_m \neq 0$. Si $a_n b_m = 0*$, comme $b_m \in A^\times$, on a $a_n = 0$. Ce qui est absurde. Donc $\deg(V(Q-Q')) = n+m > \deg V$. Or : $V(Q-Q') = R-R'$ et $\deg(R'-R) < \deg V$. Donc : $Q = Q'$ et $R = R'$.

□

Conséquence. Si K est un corps alors $K[X]$ est un anneau euclidien (donc principal).

Démonstration. Soit :

$$\begin{array}{rccc} \deg & : & K[X]\backslash\{0\} & \to & \mathbb{N} \\ & & P & \mapsto & \deg(P) \end{array}$$

Soit U, V avec $V \neq 0$. Comme K est un corps, le coefficient dominant de V est inversible donc il existe Q, R tels que $U = VQ + R$ avec $\deg R < \deg V$ ou $R = 0$. □

Theorème 4.1.6. *Soit A un anneau intégre. Alors $A[X]$ est principal si et seulement si A est un corps.*

Démonstration. ($\Leftarrow$) A est un corps $\Rightarrow A[X]$ est un anneau euclidien $\Rightarrow A[X]$ est principal.

($\Rightarrow$) Soit $\alpha \in A\backslash\{0\}$ et :

$$I = \{P \in A[X],\ \exists k \in A,\ P(0) = \alpha k\}$$

I est un idéal de $A[X]$ (à vérifier). Comme $A[X]$ est principal, il existe $P_0 \in A[X]$ tel que $I = (P_0)$. On a $\alpha \in I = (P_0)$ donc il existe $Q \in A[X]$ tel que $\alpha = P_0 Q$. Comme A est intégre, $\deg(P_0 Q) = \deg P_0 + \deg Q$. Si $\alpha \in A\backslash\{0\} \Rightarrow \deg \alpha = 0$. On en déduit que :

$$\deg P_0 = \deg Q = 0$$

Donc $P_0 \in A$. D'autre part, $X \in I$ donc il existe $T \in A[X]$ tel que :

$$X = P_0 T$$

Comme $\deg X = 1 = \deg P_0 + \deg T$, $\deg T = 1$. Donc il existe $a, b \in A$ tels que :

$$X = P_0(aX + b)$$

donc $1 = P_0 a$, $a \in A$. Donc $P_0 \in A^\times$. Par conséquent $I = A[X]$. En particulier, $1 \in I$ donc il existe $k \in A$ tels que $1 = \alpha k$ et donc $\alpha \in A^\times$.

□

4.1.6 Morphismes d'anneaux des polynômes

Proposition 4.1.7 (Prolongement d'un morphisme d'anneaux à l'anneau des polynômes)**.** *Soit $f : A \to B$ un morphisme d'anneaux et $b \in B$. Alors il existe un unique morphisme $g : A[X] \to B$ qui prolonge f (c'est-à-dire $g|_A = f$) et qui vérifie $g(X) = b$.*

Démonstration. (i) Soit $g : A[X] \to B$ un morphisme d'anneaux tel que $g|_A = f$ et $g(X) = b$. Soit :

$$P = a_0 + a_1 X + ... + a_n X^n \in A[X]$$

alors :

$$g(P) = g(a_0) + g(a_1)g(X) + ... + g(a_n)g(X)^n$$

Comme $g|_A = f$, $g(a_i) = f(a_i)$, $\forall i$. D'autre part, $g(X) = b$. Donc :

$$g(P) = f(a_0) + f(a_1) + b + ... + f(a_n)b^n$$

(ii) Soit $g : A[X] \to B$ définie par :

$$g(a_0 + a_1 X + ... + a_n X^n) = f(a_0) + f(a_1)b + ... + f(a_n)b^n$$

On vérifie que g est un morphisme d'anneaux.

□

Proposition 4.1.8 (Morphisme de réduction modulo un idéal)**.** *Soit A un anneau et I un idéal de A. On considère :*

$$\begin{array}{rccc} f\ : & A[X] & \to & A/I[X] \\ & a_0 + a_1 X + ... + a_n X^n & \mapsto & (a_0 + I) + (a_1 + I)X + ... + (a_n + I)X^n \end{array}$$

Alors f est un morphisme d'anneaux surjectif.

Démonstration.

$$\begin{array}{ccccc} A & \xrightarrow{s} & A/I & \xrightarrow{i} & A/I[X] \\ a & \mapsto & s\circ i(x) = a+I & & \end{array}$$

$$\begin{array}{ccccc} A & \xrightarrow{s} & A/I & \xrightarrow{i} & A/I[X] \\ \downarrow i' & & & \nearrow_g & \\ A[X] & & & & \end{array}$$

$g|_A = i\circ s$, $g(X) = X$. Alors $f = g$. □

Exercice 4.1.1. Soit p un nombre premier de $\mathbb{Z}$. Montrer que :

$$\mathbb{Z}[X]/\underbrace{(p)}_{p\mathbb{Z}[X]} \overset{\text{isom}}{\simeq} \mathbb{Z}/p\mathbb{Z}$$

Soit $f : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$ le morphisme de réduction modulo $p\mathbb{Z}$, c'est-à-dire :

$$\begin{array}{rccc} f & : & \mathbb{Z}[X] & \to & \mathbb{Z}/p\mathbb{Z}[X] \\ & & a_0+a_1X+...+a_nX^n & \mapsto & (a_0+p\mathbb{Z})+...+(a_n+p\mathbb{Z})X^n \end{array}$$

f est surjectif. On a :

$$\begin{array}{rcl} \operatorname{Ker} f & = & \{P = a_0+a_1X+...+a_nX^n,\ a_i\in\mathbb{Z},\ n\geq 0,\ \underbrace{a_i+p\mathbb{Z}=p\mathbb{Z}}_{a_i\in p\mathbb{Z}},\ \forall i\} \\ & = & p\mathbb{Z}[X] = (p) \end{array}$$

Proposition 4.1.9 (Morphisme d'évaluation)**.** *Soit A un anneau, $\alpha\in A$ et l'application :*

$$\begin{array}{rccc} e_\alpha & : & A[X] & \to & A \\ & & P(X)=a_0+...+a_nX^n & \mapsto & P(\alpha)=a_0+a_1\alpha+...+a_n\alpha^n \end{array}$$

Alors e_α est un morphisme d'anneaux qu'on appelle morphisme d'évaluation en α.

Démonstration.

$$\begin{array}{ccccc} a & \mapsto & a & & \\ A & \xrightarrow{\text{id}} & A & a & \alpha \\ \downarrow & \nearrow & & \nearrow & \nearrow \\ A[X] & & a & X & \end{array}$$

□

4.1.7 Fonctions polynômes

Définition 4.1.4. Soit A un anneau, $P\in A[X]$, et B un anneau contenant A. On appelle la fonction polynôme de B dans B associé au polynôme P, la fonction qu'on note P définie par :

$$\begin{array}{rccc} P & : & B & \to & B \\ & & \alpha & \mapsto & P(\alpha) \end{array}$$

Remarque. Deux polynômes distincts peuvent avoir la même fonction polynôme.

Exemple 4.1.3. On se place dans $\mathbb{Z}/2\mathbb{Z}[X]$. On considère les polynomes :

$$P = X,\ Q = X^7$$

Soit :

$$\begin{array}{rccc} P & : & \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z} \\ & & \alpha & \mapsto & P(\alpha) \end{array}$$

La fonction polynôme à P alors $P(0) = 0$ et $P(1) = 1$. On remarque que Q admet la même fonction polynôme : $\mathbb{Z}/2\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}$.

4.1.8 Racines d'un polynôme

Définition 4.1.5. Soit A un anneau, $P \in A[X]$ et $\alpha \in A$, α est une racine de P si $P(\alpha) = 0$.

Remarque. $P(\alpha) = 0 \Leftrightarrow \exists Q \in A[X]$ tel que $P = (X - \alpha)Q$. En effet, $X - \alpha$ est un polynôme dont le coefficient dominant est inversible donc on peut faire une division euclidienne de P par $X - \alpha$. Par conséquent, $\exists Q, R \in A[X]$ tels que :

$$P = (X - \alpha)Q + R \text{ avec } \deg R > 1$$

$\deg R < 1 \Rightarrow R \in A$:

$$P(\alpha) = 0 \Leftrightarrow R = 0 \Leftrightarrow P = (X - \alpha)Q$$

Définition 4.1.6 (Ordre de multiplicité d'une racine)**.** Soit A un anneau, $\alpha \in A$, $P \in A[X]$ et h un entier ≥ 1. On dit que α est une racine de P d'ordre de multiplicité h si $(X-a)^h$ divise P dans $A[X]$ et $(X - \alpha)^{h+1}$ ne divise pas P dans $A[X]$. Ceci revient à dire qu'il existe $Q \in A[X]$ tel que :

$$P = (X - \alpha)^h Q \text{ et } Q(\alpha) = 0$$

(danss ce cas, Q est impaire).

Proposition 4.1.10. *Soit A un anneau intégre, $P \in A[X]$, $\alpha_0, ..., \alpha_k$ des racines distincts de P dans A d'ordres de multiplicité $h_1, ..., h_k$ respectivement. Alors, il existe un unique $Q \in A[X]$ tel que :*

$$P = (X - \alpha_1)^{h_1} ... (X - \alpha_k)^{h_k} Q \text{ avec } Q(\alpha_i) \neq 0, \forall i$$

Démonstration. Par réccurence sur k :

- si $k = 1$, c'est évident.
- On suppose que $k > 1$ et qu'on a le résultat si P admet n $(< k)$ racines distincts. On démontre le résultat par un polynôme P qui admet k racines distincts. Donc P admet $k - 1$ racines : $\alpha_1, ..., \alpha_{k-1}$. D'après l'hypothèse de réccurence :

  $$P = (X - \alpha_1)^{h_1} ... (X - \alpha_{k-1})^{h_{k-1}} Q \text{ avec } Q(\alpha_i) \neq 0,\ 1 \leq i \leq k - 1$$

  $$P(\alpha_k) = (\alpha_k - \alpha_1)^{h_1} ... (\alpha_k - \alpha_{k-1})^{h_{k-1}} Q(\alpha_k) = 0$$

  Comme A est intégre et les α_i sont distincts, $Q(\alpha_k) = 0$. Soit λ_k l'ordre de multiplicité de α_k comme racines de Q

  $$Q = (X - \alpha_k)^{\lambda_k} U \text{ avec } U \in A[X],\ U(\alpha_k) \neq 0$$

  On déduit que :

  $$P = (X - \alpha_k)^{\lambda_k} (\underbrace{(X - \alpha_1)^{h_1} ... (X - \alpha_{k-1})^{h_{k-1}} U}_{T})$$

  et $T(\alpha_k) \neq 0$. Donc α_k est une racine de P d'ordre de multiplicité λ_k. Or l'ordre est h_k.

□

Corollaire. *Soit A un anneau intégre, $P \in A[X] \backslash \{0\}$ et $n = \deg P$. Alors P admet au plus n racines comptées avec les ordres de multiplicité.*

Démonstration. Soit $\alpha_1, ..., \alpha_k$ les racines distinctes de P et $h_1, ..., h_k$ les ordres de multiplicité. On a :

$$P = (X - \alpha_1)^{h_1} ... (X - \alpha_k)^{h_k} Q \text{ avec } Q(\alpha_i) \neq 0$$

Comme A est intégre :

$$\deg P = h_1 + ... + h_k + \deg Q \geq h_1 + ... + h_k$$

□

Remarque. On n'a pas nécessairement ce résultat si A n'est pas intégre.

Exemple 4.1.4. On se place dans $\mathbb{Z}/8\mathbb{Z}[X]$. Soit $P = X^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[X]$, $\deg P = 2$. On a :

$$X^2 - 1 = (X-1)(X+1) = \underbrace{(X-3)(X+3)}_{=X^2-9=X^2-1}$$

P admet 4 racines dans $\mathbb{Z}/8\mathbb{Z}$.

Corollaire. *Soit $A \neq \{0\}$ un anneau intégre et :*

$$\begin{array}{rccc} \varphi & : & A[X] & \to & \mathcal{F}(A,A) \\ & & P & \mapsto & \varphi(P) = P \end{array}$$

où $\mathcal{F}(A,A)$ est l'ensemble des fonctions de A dans A et $\varphi(P)$ est la fonction polynôme de A dans A. Alors :

$$\varphi \text{ est injectif} \Leftrightarrow A \text{ est infini}$$

Démonstration. ($\Rightarrow$) On suppose que A est fini. $A[X]$ est infini mais $\mathcal{F}(A,A)$ est fini donc φ n'est pas injective.

($\Leftarrow$) Soit $P, Q \in A[X]$ tels que $\varphi(P) = \varphi(Q)$ alors $\varphi(P-Q) = 0$. Il faut montrer que $P - Q$ est le polynôme nul. Si $P - Q \neq 0$, $P - Q$ admet au plus $\deg(P-Q)$ racines, c'est-à-dire $\varphi(P-Q)$ s'annule sur A en au plus $\deg(P-Q)$ points. Ce qui est absurde puisque $\varphi(P-Q)$ s'annule sur A et A est infini.

□

Proposition 4.1.11. *Soit A un anneau, $P \in A[X]$ et $\alpha \in A$. Si α est une racine de P d'ordre de multiplicité $h \geq 1$ alors :*

(i) α est une racine de P'[1] d'ordre de multiplicité $\geq h - 1$.

(ii) Si $h1_A \neq 0_A$ et $h1_A$ n'est pas un diviseur de zéro dans A alors α est une racine de P' d'ordre de multiplicité $h - 1$.

Démonstration. (i) On suppose que $P = (X-\alpha)^h Q$ avec $Q(\alpha) \neq 0$. Alors :

$$P' = (X-\alpha)^{h-1} \underbrace{[hQ + (X-\alpha)Q']}_{T}$$

On a ainsi que α est une racine de P d'ordre de multiplicité $\geq h - 1$.

(ii)

$$T(\alpha) = hQ(\alpha) = (h1_A).Q\alpha$$

Comme $h.1_A \neq 0$ et $h1_A$ n'admet pas de diviseurs de zéro, $T(\alpha) \neq 0$, donc l'ordre de multiplicité de α comme racine de P' est $h - 1$.

□

Corollaire. *Soit A un anneau, $P \in A[X]$ et $\alpha \in A$. Soit h un entier ≥ 1 tel que $(h!)1_A \neq 0$ et $(h!)1_A$ n'est pas un diviseeur de zéro. Alors α est une racine de P d'ordre de multiplicité h si et seulement si :*

$$\begin{aligned} P(\alpha) = P'(\alpha) = ... = P^{(h-1)}(\alpha) &= 0 \\ P^{(h)}(\alpha) &\neq 0 \end{aligned}$$

Remarque. On se place dans $\mathbb{Z}/2\mathbb{Z}$ et on considère $P = X^2 \in \mathbb{Z}/2\mathbb{Z}[X]$. On a que 0 est une racine double de P (car $P = (X-0)^2.1$). Mais on a :

$$P' = 2X = 0 \text{ et } P'' = 0$$

Cela ne vérifie pas le **Corollaire** précédent car $2.1 \neq 0$.

[1] $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ la dértivée de P

4.2 Polynômes à n indéterminées

4.2.1 Définitions

Définition 4.2.1. Soit A un annenau. Un polynôme P à coefficients dans A à n indéterminées, est une application :

$$\begin{array}{rccc} : & \mathbb{N}^n & \to & A \\ & \underline{k} = (k_1, ..., k_n) & \mapsto & a_{\underline{k}} \end{array}$$

c'est-à-dire :

$$\begin{aligned} P &= \sum_{\substack{0 \leq k_i \leq n_i \\ 1 \leq i \leq n}} a_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n} \\ &= \sum_{0 \leq \underline{k} \leq \underline{n}} a_{\underline{k}} X_1^{k_1} ... X_n^{k_n} \end{aligned}$$

où les $a_{k_1,...,k_n} \in A$ sont appelés les coefficients de P. On note $A[X_1, ..., X_n]$ l'ensemble des polynômes à coefficients dans A à n variables.

Définition 4.2.2 (Addition dans $A[X_1, ..., X_n]$)**.**

$$\sum a_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n} + \sum b_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n} = \sum (a_{k_1,...,k_n} + b_{k_1,...,k_n}) X_1^{k_1} ... X_n^{k_n}$$

Définition 4.2.3 (Multiplication dans $A[X_1, ..., X_n]$)**.**

$$\left(\sum a_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n} \right) \left(\sum b_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n} \right) = \sum c_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n}$$

où

$$c_{k_1,...,k_n} = \sum_{\substack{l_i + s_i = k_i \\ 1 \leq i \leq n}} a_{l_1,..,l_n} b_{s_1,...,s_n}$$

Proposition 4.2.1. *1)* $(A[X_1, ..., X_n], +, .)$ *est un anneau.*
2) Soit l'application :

$$\begin{array}{rccc} f & : & A & \to & A[X_1, ..., X_n] \\ & & a & \mapsto & a + 0X_1 + 0X_1X_2 + ... \end{array}$$

(tous les coefficients sont nuls sauf le coefficient constant qui vaut a). f est un morphisme d'anneaux injectif. Cette application permet d'identifier A à un sous-anneau de $A[X_1, ..., X_n]$

4.2.2 Degrés partiels et total

Définition 4.2.4. Soit :

$$P = \sum_{k_1,...,k_n} a_{k_1,...,k_n} X_1^{k_1} ... X_n^{k_n}$$

un polynôme non nul à coefficients dans un anneau A, à n indéterminées $X_1, ..., X_n$. Soit $1 \leq i \leq n$. Le degré partiel de P en X_i qu'on note $\deg_{X_i}(P)$ est :

$$\deg_{X_i}(P) = \max\{k_i, a_{k_1,...,k_i,...,k_n} \neq 0\}$$

c'est-à-dire est le degré P vu comme un polynôme à une indéterminée X_i, à un polynôme à une indéterminée X_i, à ccoeeffiints dans l'anneau des polynômes $A[X_1, ..., X_{i-1}, X_{i+1}, ..., X_n]$ à $n-1$ indéterminées.

Le degré total de P, qu'on note $\deg P$ est :

$$\deg P = \max\{k_1 + ... + k_n,\ a_{k_1,...,k_n} \neq 0$$

Exemple 4.2.1. Soit $P \in \mathbb{Z}[X_1, X_2, X_3]$:

$$P = 1 + X_1 + X_2X_3 + X_2^2 + X_3X_1^7$$

On a :

$$\deg_{X_1} P = 7,\ \deg_{X_2} P = 2,\ \deg_{X_3} P = 1$$

et le degré total de P est $\deg P = 8$.

Remarque. Soit $P \in A[X_1, ...X_n]$, P peut être vu comme un polynôme en une variable. Par exemple, on peut considérer P comme un polynôme en la variable X_n à coefficients dans $A[X_1, ..., X_{n-1}]$. Dans ce cas, on peut écrire :

$$P = a_mX^m + ... + a_1X + a_0$$

où les $a_i \in A[X_1, ..., X_{n-1}]$.

Exercice 4.2.1. Montrer que :

$$\mathbb{C}[X, Y]/(Y - X^2) \overset{\text{isom}}{\simeq} \mathbb{C}|X]$$

Soit :

$$\begin{array}{rccc} e_{X^2} & : & \mathbb{C}[X][Y] & \to & \mathbb{C}[X] \\ & & P(X, Y) & \mapsto & P(X, X^2) \end{array}$$

C'est le morphisme d'évaluation en X^2. e_{X^2} est surjectif. Soit $P \in \mathbb{C}[X]$, alors $P = e_{X^2}(P)$.

$$\operatorname{Ker} e_{X^2} = \{P(X, Y) \in \mathbb{C}[X, Y],\ P(X, X^2) = 0\}$$

Remarque. Le polynôme $Y - X^2$ considéré comme polynôme en la variable Y à coefficients dans $\mathbb{C}[X]$ admet un coefficient dominant inversible ($= 1$) donc on peut effectuer une division euclidienne de tout $P \in \mathbb{C}[X][Y]$. Soit $P \in \mathbb{C}[X][Y]$ tel que :

$$P = (Y - X^2)Q + R, \qquad \deg R \leq 0$$

Donc :

$$P = (Y - X^2)Q + R, \qquad R \in \mathbb{C}[X]$$

$$\begin{array}{rcl} P \in \operatorname{Ker} e_{X^2} & \Leftrightarrow & P(X, X^2) = 0 \\ & \Leftrightarrow & R(X) = 0 \\ & \Leftrightarrow & P \in (Y - X^2) \end{array}$$

On déduit alors que :

$$\mathbb{C}[X, Y]\backslash(Y - X^2) \overset{\text{isom}}{\simeq} \mathbb{C}[X]$$

Remarque. 1) Si A est intègre alors $A[X_1, ..., X_n]$ est intègre. En effet, par réccurence :

$$\begin{array}{rcl} A \text{ intègre} & \Rightarrow & A[X] \text{ intègre} \\ & \Rightarrow & A[X_1][X_2] = A[X_1, x_2] \\ & \Rightarrow & ... \\ & \Rightarrow & A[X_1]...[X_n] \text{ intègre} \\ & \Rightarrow & A[X_1, ..., X_n] \text{ intègre} \end{array}$$

2) Si A est intègre :

$$(A[X_1, ..., X_n])^\times = A^\times$$

En effet $(A[X_1])^\times = A^\times$ (**Proposition 4.1.4**) et on en déduit que :

$$\begin{array}{rcl} A([X_1, X_2])^\times & = & (A[X_1][X_2])^\times \\ & = & (A[X_1])^\times = A^\times \end{array}$$

4.2.3 Fonctions polynômes

Définition 4.2.5. Soit A un anneau, $P \in A[X_1, ..., X_n]$ et B un anneau contenant A. La fonction polynôme de $B^n \to B$ associée à P la fonction :

$$\begin{array}{rccc} P & : & B^n & \to & B \\ & & (b_1, ..., b_n) & \mapsto & P(b_1, ..., b_n) \end{array}$$

Proposition 4.2.2. *Soit A un anneau intègre et $\mathcal{F}(A^n, A)$ l'ensemble des fonctions de $A^n \to A$. Soit :*

$$\begin{array}{rccc} \varphi & : & A[X_1, ..., X_n] & \to & \mathcal{F}(A^n, A) \\ & & P & \mapsto & \varphi(P) \end{array}$$

la fonction polynôme associée à P. Alors :

$$\varphi \text{ est injective} \Leftrightarrow A \text{ est infini}$$

Démonstration. ($\Rightarrow$) Si A est fini, $\mathcal{F}(A^n, A)$ est fini. Par contre, $A[X_1, ..., X_n]$ est infini donc φ n'est pas injectif.

($\Leftarrow$) • Si $n = 1$, voir DÉMONSTRATION du deuxième **Corollaire** de la **Section 4.1.8**.

• On suppose que $n > 1$ et qu'on a le résultat pour tout polynôme en k variables avec $k < n$. Soit $P, Q \in A[X_1, ..., X_n]$ tels que $\varphi(P - Q) = 0$. On montre que $P - Q = 0$. On suppose que $P - Q \neq 0$. On considère $P - Q$ comme élément de $\mathbb{C}[X_1, ..., X_{n-1}][X_n]$. $P - Q$ s'écrit :

$$P - Q = a_m X_n^m + ... + a_0, \text{ avec } m \in \mathbb{N},\ a_i \in A[X_1, ..., X_{n-1}],\ a_m \neq 0$$

Comme a_m est un polynôme en $n - 1$ variables ($< n$) non nul, il existe $(b_1, ..., b_{n-1}) \in A^{n-1}$ tel que $a_m(b_1, ..., b_{n-1}) \neq 0$ d'après l'hypothèse de réccurence. Donc on a :

$$(P - Q)(b_1, ..., b_{n-1}, X_n) = a_m(b_1, ..., b_{n-1}) X_n^m + ... + a_0(b_1, ..., b_{n-1}) \in A[X_n] \backslash \{0\}$$

D'après l'hypothèse de réccurence, la fonction polynomiale $A \to A$ associée à $(P - Q)(b_1, ..., b_{n-1}, X_n)$ est non nul. Donc il existe $b_n \in A$ tel que :

$$(P - Q)(b_1, ..., b_{n-1}, b_n) \neq 0$$

Donc $\varphi(P - Q) \neq 0$. Ce qui est absurde !

□

Chapitre 5

Anneaux produit, Anneau et corps des fractions

5.1 Anneaux produit

Définition 5.1.1. Soit $A_1, ..., A_n$ des anneaux. On définit :

$$A = A_1 \times A_2 \times ... \times A_n = \{(x_1, ..., x_n),\ x_i \in A_i\}$$

l'anneau produit.

Définition 5.1.2 (Addition dans A)**.**

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 +_{A_1} y_1, ..., x_n +_{A_n} y_n)$$

Définition 5.1.3 (Multiplication dans A)**.**

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 \times_{A_1} y_1, ..., x_n \times_{A_n} y_n)$$

Proposition 5.1.1. *$(A, +, .)$ est un anneau (appelé anneau produit) et :*

$$\begin{aligned} 0_A &= (0_{A_1}, ..., 0_{A_n}) \\ 1_A &= (1_{A_1}, ..., 1_{A_n}) \end{aligned}$$

Proposition 5.1.2. $(A_1 \times ... \times A_n)^\times = A_1^\times \times ... \times A_n^\times$.

Remarque. $A_1 \times ... \times A_n$ $(n > 1)$ n'est pas intègre :

$$(1, 0, ..., 0) \times (0, 1, ..., 0) = (0, 0, ..., 0)$$

Theorème 5.1.3 (Théorème chinois I)**.** *Soit A un anneau non nul, $n \geq 2$, $I_1, ..., I_n$ des idéaux de A étrangers deux à deux (c'est-à-dire $A = I_1 + I_j$, $\forall i \neq j$) et $a_1, ..., a_n \in A$. Alors il existe $x \in A$ qui vérifie :*

$$\begin{cases} x \equiv a_1[I_1] \\ \vdots \\ x \equiv a_n[I_n] \end{cases}$$

x est unique modulo $I_1 \cap ... \cap I_n$.

Démonstration. Existence de x : par réccurence

- $n = 2$: on montre qu'il existe x tel que

$$\begin{cases} x \equiv a_1[I_1] \\ \vdots \\ x \equiv a_2[I_2] \end{cases}$$

c'est-à-dire x s'écrit :

$$x = a_1 + i_1 = a_2 + i_2 \quad \text{avec } i_1 \in I_1,\ i_2 \in I_2$$

donc :

$$a_1 - a_2 = i_1 - i_2$$

Comme $I_1 + I_2 = A$, il existe $\alpha \in I_1$ et $\beta \in I_2$ tel que $a_1 - a_2 = \alpha + \beta$. On prend aisni : $i_1 = \alpha$ et $i_2 = -\beta$.

– On suppose que $n > 2$ et qu'on la résultat si on a un système à k équations avec $k < n$. D'après l'hypothèse de réccurence, il existe $y \in A$ tel que :

$$\begin{cases} y = a_1[I_1] \\ \vdots \\ y = a_n[I_n] \end{cases} \tag{5.1}$$

S'il existe $x \in A$ qui vérifie (5.1) alors $x \equiv y[I_1 \cap ... \cap I_n]$. En effet :

$$\begin{cases} x \equiv a_1[I_1] \\ \vdots \\ x \equiv a_{n-1}[I_{n-1}] \end{cases} \quad \text{et} \quad \begin{cases} y \equiv a_1[I_1] \\ \vdots \\ y \equiv a_{n-1}[I_{n-1}] \end{cases}$$

impliquent :

$$\begin{cases} x \equiv y[I_1] \\ \vdots \\ x \equiv y[I_{n-1}] \end{cases}$$

donc $x \equiv y[I_1 \cap ... \cap I_n]$. Donc le problème revient à trouver $x \in A$ tel que :

$$\begin{cases} x \equiv y[I_1 \cap ... \cap I_n] \\ x \equiv a_n[I_n] \end{cases}$$

D'après l'hypothèse de réccurence, il suffit de montrer que :

$$(I_1 \cap ... \cap I_{n-1}) + I_n = A$$

Comme $I_n + I_k = A$, $\forall 1 \leq k \leq n$, 1_A s'écrit :

$$\begin{aligned} 1_A &= i_{n,1} + i_1, \quad i_1 \in I_1,\ i_{n,1} \in I_n \\ &= i_{n,2} + i_2, \quad i_2 \in I_2,\ i_{n,2} \in I_n \\ &\vdots \\ &= i_{n,n-1} + i_{n-1}, \quad i_{n-1} \in I_{n-1},\ i_{n,n-1} \in I_n \end{aligned}$$

Donc :

$$\begin{aligned} 1_A &= (i_{n,1} + i_1)(i_{n,2} + i_2)...(i_{n,n-1} + i_{n-1}) \\ &= \underbrace{i_1 i_2 ... i_{n-1}}_{\in \bigcap_{1 \leq k \leq n} I_k} + \alpha, \quad \alpha \in I_n \end{aligned}$$

□

Theorème 5.1.4 (Théorème chinois II)**.** *Soit A un anneau non nul, $I_1, ..., I_n$ ($n \geq 2$) des idéaux de A étrangers deux à deux. Alors on a le morphisme surjectif suivant :*

$$\begin{array}{rccc} s & : & A & \to & A/I_1 \times A/I_2 \times ... \times A/I_n \\ & & a & \mapsto & a + I_1, a + I_2, ..., a + I_n \end{array}$$

Démonstration.

- Comme les surjections canoniques $s_i : A \to A/I_i$ sont des morphismes, s est un morphisme.
- On montre que s est surjectif. Soit $(a_1 + I_1, ..., a_n + I_n) \in A/I_1 \times ... \times A/I_n$. On montre qu'il existe $a \in A$ tel que :

  $$s(a) = (a_1 + I_1, ..., a_n + I_n)$$

  c'est-à-dire qu'il existe $a \in A$ tel que :

  $$\begin{cases} a + I_1 = a_1 + I_1 \\ \vdots \\ a + I_n = a_n + I_n \end{cases}$$

  ou encore, il existe $a \in A$ tel que :

  $$\begin{cases} a \equiv a_1 [I_1] \\ \vdots \\ a \equiv a_n [I_n] \end{cases}$$

  D'après le **Théorème 5.1.3**, a existe.

□

Remarque.

$$\begin{array}{rcl} \operatorname{Ker} s & = & \{a \in A,\ (a + I_1, ..., a + I_n) = (I_1 + ... + I_n)\} \\ & = & I_1 \cap I_2 \cap ... \cap I_n \end{array}$$

On en déduit que $A/(I_1 \cap ... \cap I_n) \simeq A/I_1 \times A/I_n$.

Exemple 5.1.1. Soit $n_1, ..., n_m \in \mathbb{Z}^*$ tel que $\text{PGCD}(n_i, n_j) = 1$, $\forall i \neq j$. Alors les idéaux de $\mathbb{Z}$ sont $n_i \in \mathbb{Z}$, $1 \leq i \leq m$ sont étrangers 2 à 2.

$$n_i\mathbb{Z} + n_j\mathbb{Z} = \text{PGCD}(n_i, n_j)\mathbb{Z} = \mathbb{Z}$$

D'après le **Théorème 5.1.4** :

$$\mathbb{Z}(n_1\mathbb{Z} \cap ... \cap n_m\mathbb{Z}) \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_m\mathbb{Z}$$

Or :

$$n_1\mathbb{Z} \cap ... \cap n_m\mathbb{Z} = \text{PPCM}(n_1, ..., n_m)\mathbb{Z} = n_1...n_m\mathbb{Z}$$

Donc :

$$\mathbb{Z}(n_1....n_m\mathbb{Z}) \overset{\text{isom}}{\simeq} \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_m\mathbb{Z}$$

5.2 Anneau des fractions, corps des fractions

5.2.1 Construction de $\mathbb{Q}$

Soit $\mathbb{Z}^* \times \mathbb{Z} = \{(s,a), s \in \mathbb{Z}^*,\ a \in \mathbb{Z}\}$. Dans $\mathbb{Z}^* \times \mathbb{Z}$, on définit la relation $\mathcal{R}$:

$$(s,a)\mathcal{R}(s',a') \text{ si } as' = a's$$

$\mathcal{R}$ est une relation d'équivalence. On note la classe de (s,a) :

$$\frac{a}{s} = \{(s',a') \in \mathbb{Z}^* \times \mathbb{Z},\ as' = a's\}$$

On note $(\mathbb{Z}^*)^{-1}\mathbb{Z}$ l'ensemble des classes d'équivalence :

$$(\mathbb{Z}^*)^{-1}\mathbb{Z} = \left\{\frac{a}{s},\ a \in \mathbb{Z},\ s \in \mathbb{Z}^*\right\}$$

On définit les opérations suivantes :

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

$$\frac{a}{s}.\frac{a'}{s'} = \frac{aa'}{ss'}$$

On vérifie que ces opérations sont bien définies. On démontre que $((\mathbb{Z}^*)^{-1}\mathbb{Z}, +, .)$ est un corps et on a : $(\mathbb{Z}^*)^{-1}\mathbb{Z} \simeq \mathbb{Q}$.

5.2.2 Généralisation à un anneau quelconque

Soit A un anneau non nul et S une partie multiplicative de A, c'est-à-dire $\forall x, y \in S$, $xy \in S$ et $1 \in S$. On considère l'ensemble :

$$S \times A = \{(s,a),\ s \in S,\ a \in A\}$$

et on définit la relation $\mathcal{R}$:

$$(s,a)\mathcal{R}(s',a') \text{ si } \exists t \in S,\ t(as' - a's) = 0_A$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence. On note $\frac{a}{s}$ la classe d'un couple (s,a). On note $S^{-1}A$ l'ensemble des classes ou $A[S^{-1}]$.

$$\begin{aligned} S^{-1}A &= \left\{\frac{a}{s},\ a \in A,\ s \in S\right\} \\ \frac{a}{s} &= \{(s',a'),\ \exists t \in S,\ t(as' - a's) = 0\} \end{aligned}$$

Dans $S^{-1}A$, on définit une addition et une multiplication :

$$\begin{aligned} \frac{a}{s} + \frac{a'}{s'} &= \frac{as' + a's}{ss'} \\ \frac{a}{s}.\frac{a'}{s'} &= \frac{aa'}{ss'} \end{aligned}$$

On vérifie que ces opérations sont bien définies.

Proposition 5.2.1. *1)* $(S^{-1}A, +, .)$ *est un anneau et :*

$$0_{S^{-1}A} = \frac{0_A}{1_A},\ 1_{S^{-1}A} = \frac{1_A}{1_A}$$

2) $S^{-1}A = \{0\} \Leftrightarrow 0_A \in S$. *En effet :*
$(\Leftarrow)$

$$\begin{aligned} 0 \in S &\Rightarrow \forall (s,a) \in S \times A,\ (s,a)\mathcal{R}(1,0) \\ &\Rightarrow \forall (s,a) \in S \times A,\ \frac{a}{s} = \frac{0_A}{1_A} \\ &\Rightarrow S^{-1}A = \{0\} \end{aligned}$$

$(\Rightarrow)$

$$\begin{aligned} S^{-1}A = \{0\} &\Rightarrow \forall (s,a) \in S \times A,\ \frac{a}{s} = \frac{0_A}{1_A} \\ &\Rightarrow \forall (s,a) \in S \times A,\ \exists t \in S,\ t(a-0) = 0 \end{aligned}$$

En particulier, si $a = 1_A$, $\exists t \in S$, $t1_A = 0$. *Donc* $O_A \in S$.

Proposition 5.2.2. *Soit :*

$$\begin{array}{rccc} i & : & A & \to & S^{-1}A \\ & & a & \mapsto & \frac{a}{1_A} \end{array}$$

Alors i *est un morphisme d'anneau :*

$$\operatorname{Ker} i = \left\{ a \in A,\ \frac{a}{1} = \frac{0}{1} \right\} = \{ a \in A,\ \exists t \in S,\ ta = 0_A \}$$

Si $0 \notin S$ *et* S *ne contient pas de diviseur de zéro,* $\operatorname{Ker} i = \{0_A\}$ *donc* i *est injetive et donc* A *s'identifie à un sous-anneau de* $S^{-1}A$.

Exemple 5.2.1. 1) $A = \mathbb{Z}$, $S = \mathbb{Z}^*$:

$$S^{-1}A = \left\{ \frac{a}{s},\ a \in \mathbb{Z},\ s \in \mathbb{Z}^* \right\} \simeq \mathbb{Q}$$

$$\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow as' = a's$$

2) $A = \mathbb{Z}$, $S = \mathbb{Z}\backslash p\mathbb{Z}$[1] avec p un nombre premier.

$$S^{-1}A = \left\{ \frac{a}{s},\ a \in \mathbb{Z},\ p \not| s \right\} \simeq \mathbb{Q}_p$$

$$\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow as' = a's$$

$$(S^{-1}A)^\times = \left\{ \frac{a}{s},\ a \in \mathbb{Z},\ s \in \mathbb{Z}^*,\ p \not| a, p \not| s \right\}$$

Exercice 5.2.1. Soit $I = S^{-1}A\backslash(S^{-1}A)^{-1}$. Montrer que I est un idéal de $S^{-1}A$. En déduire que $S^{-1}A$ contient un seul idéal maximal.

[1] $\mathbb{Z}\backslash p\mathbb{Z} = \{a \in \mathbb{Z}, p \not| a\}$

Remarque. On suppose que $0 \notin S$ et S ne contient pas de divisuer de zéro.

$$S^{-1}A = \left\{ \frac{a}{s},\ a \in A,\ s \in S,\ \exists \frac{a'}{s'},\ a' \in A,\ s' \in S,\ \frac{aa'}{ss'} = \frac{1}{1} \right\}$$

$$\frac{aa'}{ss'} = \frac{1}{1} \Leftrightarrow aa' = ss' \in S$$

$\frac{a}{s} \in (S^{-1}A)^\times \Rightarrow \exists a' \in A,\ aa' \in S$. Réciproquement, soit $\frac{a}{s} \in S^{-1}A$ tel qu'il existe $a' \in A$ vérifiant $aa' \in S$. On a :

$$(S^{-1}A)^\times = \left\{ \frac{a}{s} \in S^{-1}A,\ \exists a' \in A,\ aa' \in S \right\}$$

Remarque.

$$S \subset \left\{ \frac{s'}{s},\ s', s \in S \right\} \subset (S^{-1}A)^\times$$

5.2.3 Corps des fractions

Définition 5.2.1. Soit A un anneau intègre et $S = A\backslash\{0\}$. Alors l'anneau $S^{-1}A$ est un corps, appelé le corps des franctions de A et qu'on $\mathrm{Fr}(A)$.

$$\mathrm{Fr}(A) = (A\backslash\{0\})^{-1}A$$

Exemple 5.2.2.

– $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$

– $$\mathrm{Fr}(\mathbb{Z}[i]) = \left\{ \frac{a+bi}{c+di},\ a,b,c,d \in \mathbb{Z},\ (c,d) \neq (0,0) \right\} = \{\alpha + \beta i,\ \alpha, \beta \in \mathbb{Q}\} \overset{\text{def}}{=} \mathbb{Q}[i]$$

– $$\mathrm{Fr}(\mathbb{Z}[X]) = \left\{ \frac{P(X)}{Q(X)},\ P,Q \in \mathbb{Z}[X],\ Q \neq 0 \right\} = \left\{ \frac{P(X)}{Q(X)},\ P,Q \in \mathbb{Q}[X],\ Q \neq 0 \right\} \overset{\text{def}}{=} \mathbb{Q}[X]$$

Remarque. Soit A un anneau intègre et $\mathrm{Fr}(A)$ le corps des fonctions de A. Soit :

$$\begin{array}{rccc} i & : & A & \to & \mathrm{Fr}(A) \\ & & a & \mapsto & \frac{a}{1} \end{array}$$

i est un morphisme d'anneau injectif. A s'identifie à un sous-anneau du corps des fractions de A.

Tout anneau intègre est un sous-anneau du corps des fractions.

Proposition 5.2.3. *Soit A un anneau intègre et S une partie multiplicative de $A\backslash\{0\}$ tel que $f(S) \subset B^\times$. Soit B un anneau et $f : A \to B$ un morphisme d'anneaux. Alors, il existe un unique morphisme : $g : S^{-1}A \to B$ qui prolonge f.*

Démonstration. – Soit $g : S^{-1}A \to B$ un morphisme d'anneau qui prolonge f. Soit $\frac{a}{s} \in S^{-1}A$, alors

$$g\left(\frac{a}{s}\right) = g\left(\frac{a}{1}\frac{1}{s}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{s}\right) = f(a) g\left(\frac{s}{1}^{-1}\right) = f(a)\left(g\left(\frac{s}{1}\right)^{-1}\right) = f(a)f(s)^{-1}$$

Soit

$$\begin{array}{rccc} g & : & S^{-1}A & \to & B \\ & & \frac{a}{s} & \mapsto & f(a)f(s)^{-1} \end{array}$$

On montre que g est bien définie. Soit $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}A$ tels que : $\frac{a}{s} = \frac{a'}{s'}$. On montre que $g\left(\frac{a}{s}\right) = g\left(\frac{a'}{s'}\right)$:

$$\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow as' = a's$$

$$g\left(\frac{a}{s}\right) = f(a)(f(s))^{-1},\ g\left(\frac{a'}{s'}\right) = f(a')(f(s'))^{-1}$$

.

$$g\left(\frac{a}{s}\right) = g\left(\frac{a'}{s'}\right) \Leftrightarrow f(a)f(s') = f(a')f(s) \Leftrightarrow f(as') = f(a's)$$

Comme $as' = a's$, $f(as') = f(sa')$.

– Soit

$$\begin{array}{rccc} g & : & S^{-1}A & \to & B \\ & & \frac{a}{s} & \mapsto & f(a)f(s)^{-1} \end{array}$$

Vérifier que g est un morphisme d'anneaux.

□

Corollaire. *Soit A un anneau intègre, K un corps et $f : A \to K$. Alors il existe un unique morphisme $g : \mathrm{Fr}(A) \to K$, injectif qui prolonge f*

Démonstration.

$$\begin{array}{ccc} A & \xrightarrow{f} & K \\ \uparrow i & \nearrow & \\ \mathrm{Fr}(A) & & \end{array}$$

$S = A\backslash\{0\}$, $f(S) \subset K\backslash\{0\} = K^\times$. D'après la proposition, il existe un unique morphsime $g : \mathrm{Fr}(A) \to B$ qui prolonge f.

$$g\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$$

On montre que g injectif.

$$\mathrm{Ker}\, g = \left\{\frac{a}{s},\ f(a)f(s)^{-1} = 0_K\right\} = \left\{\frac{a}{s},\ f(a) = 0\right\} = \left\{\frac{0}{s}\right\}$$

□

Remarque. Soit A un anneau intègre. Si K est un corps qui contient A dans $\mathrm{Fr}(A) \subset K$.

Chapitre 6

Arithmétique dans un anneau

6.1 Eléments associés, éléments irréductibles, éléments premiers

Définition 6.1.1. Soit A un anneau non nul et $a, b \in A$. On dit que a divise b dans A et on note $a|b$ s'il existe $c \in A$ tel que $b = ac$.

Remarque. 1. $(a|b \text{ et } b|a) \Leftrightarrow (a) = (b)$[1].

2. On suppose que a est un anneau intègre :

$$\exists a|b \text{ et } b|a \Rightarrow \exists c \in A,\ b = ac \text{ et } \exists d \in A,\ a = db$$

$\Rightarrow \exists c, d \in A,\ b = bdc \Rightarrow b = 0$ ou $dc = 1$. Donc

$$(a|b \text{ et } b|a) \Leftrightarrow \begin{cases} b = ac, \text{ avec } c \in A^\times \\ \text{ou } b = a = 0 \end{cases}$$

Définition 6.1.2 (Eléments associés)**.** Soit A un anneau intègre et $a, b \in A$. On dit que a et b sont associés s'il existe $u \in A^\times$, $a = bu$. Dans ce cas, on note $a \sim b$.

Remarque. Si $a \sim b$ alors $(a) = (b)$.

Définition 6.1.3 (Eléments irréductibles)**.** Soit A un anneau intègre et $\pi \in A \backslash A^\times$. On dit que π est un élément irréductible de A si :

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

Remarque. Si π est irréductible, $\pi \notin A^\times$, $\pi \neq 0$ ($0 = 0.0$ et $0 \notin A^\times$).

Proposition 6.1.1. *Soit A un anneau et $\pi \in A$. Alors π est irréductible si et seulement si (π) est un idéal maximal parmi les idéaux principaux de A.*

Démonstration. ($\Rightarrow$) On suppose que $(\pi) \subset (\alpha) \subset A$ où $\alpha \in A$. $(\pi) \subset (\alpha) \Rightarrow \alpha|\pi$. Or π est un élément irréductible, donc $\alpha \in A^\times$ ou $\alpha \sim \pi$.
- Si $\alpha \in A^\times$, alors $(\alpha) = A$.
- Si $\alpha \sim \pi$, alors $(\alpha) = (\pi)$.

[1] On rappelle que (a) est l'idéal engendré par a

($\Leftarrow$) Soit $\alpha \in A$ tel que $\alpha|\pi$.

$$\alpha|\pi \Rightarrow (\pi) \subset (\alpha)$$

Or (π) est maximal parmi les idéaux principaux de A, $(\alpha) = (\pi)$ ou $(\alpha) = A$.
- $(\alpha) = (\pi) \Rightarrow \alpha \sim \pi$
- $(\alpha) = A \Rightarrow \alpha \in A^\times$

□

Corollaire. *Soit A un anneau principal. Alors :*

$$\pi \text{ est un élément irrationnel} \Leftrightarrow (\pi) \text{ est maximal} \Leftrightarrow A/(\pi) \text{ est un corps}$$

Définition 6.1.4 (Eléments premiers)**.** Soit A un anneau intègre et $p \in A \backslash A^\times$. p est un élement premier de A si :

$$\forall x, y \in A,\ (p|xy \Rightarrow p|x \text{ ou } p|y)$$

Proposition 6.1.2. *p est premier $\Leftrightarrow$ (p) est un idéal premier $\Leftrightarrow$ $A/(p)$ est un anneau intègre.*

Theorème 6.1.3. *Soit A un anneau intègre et $p \in A$. Alors p est un élément premier $\Rightarrow$ p est élément irréductible. La réciproque est fausse en général.*

Démonstration. Soit $a, b \in A$ tel que $p = ab$. On montre que $a \in A^\times$ ou $b \in A^\times$.

$$p = ab \Rightarrow p|ab$$

Comme p premier :

$$p|ab \Rightarrow p|a \text{ ou } p|b$$

On suppose que $p|a$, on pose $a = pa'$ avec $a' \in A$. Alors, on a :

$$p = pa'b \Rightarrow a'b = 1 \Rightarrow b \in A^\times$$

Même si $p|a$, on dédduit que $a \in A^\times$. □

Exercice 6.1.1 (Réciproque fausse)**.** Soit $A = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5},\ a, b \in \mathbb{Z}\}$. On remarque que :

$$2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5}) \tag{6.1}$$

Montrer que :

1) Montrer que 2 est irréductible.

2) En utilisant l'égalité (6.1), montrer que 2 n'est pas premier.

Theorème 6.1.4. *Soit A un anneau principal et $p \in A$. Alors p est irréductible $\Leftrightarrow$ p premier.*

Démonstration. ($\Rightarrow$) p irréductible $\Rightarrow$ (p) est un idéal maximal $\Rightarrow$ $A/(p)$ est un corps $\Rightarrow$ $A/(p)$ est un anneau intègre $\Rightarrow$ (p) est un idéal premier $\Rightarrow$ p est un élément premier.

□

6.2 Notions de PGCD et PPCM

Définition 6.2.1. Soit A un anneau intègre et a et b deux éléments de A. Soit $d \in A$, on dit que d est un PGCD de a et b si

(i) $d|a$ et $d|b$

(ii) si $d' \in A$ tel que $d'|a$ et $d'|b$ alors $d'|d$

Traduction en terme d'idéeaux. d est un PGCD de a et b si (d) est le plus petit idéal parmi les idéaux principaux contenant l'idéal $(a) + (b)$.

Définition 6.2.2. Soit A un anneau intègre et a et b deux éléments de A. Soit $m \in A$, on dit que m est un PPCM de a et b si

(i) $a|m$ et $b|m$.

(ii) Si $m' \in A$ tel que $a|m'$ et $b|m'$ alors $m|m'$

m est un PPCM de a et b si

(i) $(m) \subset (a) \cap (b)$

(ii) Si $(m') \subset (a) \cap (b)$ alors $(m') \subset (m)$.

Donc : m est un PPCM de a et b si (m) est le plus grand idéal parmi les idéaux principaux contenu de $(a) \cap (b)$.

Proposition 6.2.1. *m est un* PPCM *de a et b si et seulement si $(a) \cap (b)$ est un idéal principal et $(a) \cap (b) = m$.*

Démonstration. ($\Rightarrow$) On a $(m) \subset (a) \cap (b)$. Soit $\alpha \in (a) \cap (b)$ alors $a|\alpha$ et $b|\alpha$. Comme m est un PPCM de a et b alors $m|\alpha$ donc $\alpha \in (m)$.

($\Leftarrow$) Si $(a) \cap (b) = (m)$, alors (m) est le plus grand parmi les idéaux principaux contenus dans $(a) \cap (b)$ donc m est un PPCM de a et b.

□

Remarque. 1) Soit $a, b \in A$, on suppose que d_1 et d_2 sont des PGCD de a et b. Donc $d_1|d_2$ et $d_2|d_1$. Comme A est intègre, $d_1 \sim d_2$. De même, si m_1 et m_2 sont des PPCM de a et b alors $d_1 \sim m_2$.

2) En général, le (un) PGCD n'existe pas.

Exemple 6.2.1. Soit $A = \mathbb{Z}(i\sqrt{5}) = \{a + bi\sqrt{5},\ a, b \in \mathbb{Z}\}$. On a :

$$6 = 2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

On montre qu'il n'existe pas un PGCD de $a = 6$ et $b = 2$, $(1 + i\sqrt{5})$.

On suppose que a et b admettent un PGCD noté d. On a : $2|d$, on pose $d = 2d'$. Alors $d'|3$ et $d'|1 + \sqrt{5}$. On montre d'abord que 3 et $1 + i\sqrt{5}$ sont des éléments irréductibles de A.

- $3 \in A^\times$,
- On suppose que $3 = xy$ avec $x, y \in A$ alors

$$N(3) = N(x)N(y) = 9$$

Or :

$$A^\times = \{z \in A,\ N(z) = 1\} \qquad \text{(à vérifier)}$$

Supposons que 3 n'est pas irréductible alors il existe $x, y \in A$ tel que $3 = xy$ et $N(x) \neq 1$, $N(y) \neq 1$ donc $N(x) = N(y) = 3$. On pose $x = a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$.

$$N(x) = a^2 + 5b^2 = 3 \tag{6.2}$$

- On montre que $1+i\sqrt{5}$ est irréductible. On suppose que $1+i\sqrt{5}$ n'est pas irréductible donc il existe $x, y \in A\backslash A^\times$ tels que $1+i\sqrt{5} = xy$. Or :

$$N(1+i\sqrt{5}) = N(x)N(y) = 2.3$$

  Comme $N(x) \neq 1$ et $N(y) \neq 1$, $N(x) = 2$ et $N(y) = 5$ ou $N(y) = 2$ et $N(x) = 3$ donc il existe $\alpha \in A$ tel que $N(x) = 3$. Impossible !
- Retour à l'histoire du PGCD :

$$d'|3 \text{ et } 3 \text{ irréductible} \Rightarrow d' \in A^\times \text{ ou } d' \sim 3$$

  Si $d' \sim 3$, comme $d'|1+i\sqrt{5}$ alors $N(d') = 9$ et tel que $N(1+i\sqrt{5}) = 6$. Impossible ! Donc $d' \in A^\times$ et donc $d \sim 2$.
  D'autre part, $1+i\sqrt{5}|d$. Donc $1+i\sqrt{5}|2$ et donc $N(1+i\sqrt{5}) = 6|N(2) = 4$, impossible.

3) – Si $(a)+(b) = (d)$, alors d un PGCD de a et b
   – $a \in (a)+(n)$ donc $a \in (d)$. De même $b \in (d)$. Donc $d|a$ et $d|b$.
   – Soit $d' \in A$ tel que $d'|a$ et $d'|b$. Comme $(a)+(b) = (d)$, il existe $u, v \in A$ tel que

$$d = ua + bv$$

   Or $d'|a$ et $d'[b$ donc $d'|d$. La réciproque est fausse (en général). Si d est un PGCD de a et b alors $(a)+(b) \neq (d)$.
   Exemple 6.2.2. $A = \mathbb{Z}[X,Y]$ et $a = X$ et $b = Y$. X et Y sont premiers entre eux (à vérifier) 1 est un PGCD de X et Y. On montre que $(X)+(Y) \neq 1$. On suppose que $1 \in (X)+(Y)$ donc il existe $P, Q \in \mathbb{Z}[X,Y]$ tels que :

$$1 = XP + YQ \tag{6.3}$$

   On pose :

$$P + P_0(X) + P_1(X)Y + ... + P_n(X)Y^n \qquad \in \mathbb{Z}[X,Y]$$

$$(6.3) : \exists P_0(X), Q_1(X,Y) \text{ tel que } 1 = XP_0(X) + YQ_1(X,Y)$$

   Si $Q_1 \neq 0$, $\deg_Y(1 - X_0P_0(X)) \geq 1$ (impossible). Si $Q_1 = 0$ alors X est un élément inversible dans $\mathbb{Z}[X,Y]$ (impossible).

4) On suppose que A est un anneau principal, $a$et b des éléments de A tels que $(a,b) \neq (0,0)$. Alors un PGCD (resp. un PPCM) de a et b existe et on a $(a)+(b) = (\text{PGCD}(a,b))$ (resp. $(a) \cap (b) = (\text{PPCM}(a,b))$).

Proposition 6.2.2. *Soit A un anneau intègre. Alors les propositions suivantes sont équivalentes.*

(i) $\forall a, b \in A\backslash\{0\}$, *un PGCD de a et b existe. On le note d.*

(ii) $\forall a, b \in A\backslash\{0\}$, *un PPCM de a et b existe. On le note m.*

Dans ce cas, $ab \sim md$.

6.3 Anneaux factoriels

Définition 6.3.1. Soit A un anneau non nul. On dit que A est factoriel si

(i) A est intègre,

(ii) $\forall a \in A\backslash\{0\}$, a se factorise en :

$$a = up_0p_1...p_k,$$

où $u \in A^\times$, $k \geq 0$, $p_0 = 1$, $p_1, p_2, ..., p_k$ sont des éléments irréductibles de $A^\times$.

(iii) Cette factorisation est unique à une permutation près et à des éléments inversibles près, c'est-à-dire si

$$a = up_0p_1...p_k = vq_0q_1...q_l,$$

où $u, v \in A^\times$, $k \geq 0$, $l \geq 0$, $p_0 = q_0 = 1$, $p_1, ..., p_k$, $q_1, ..., q_l$, des éléments irréductibles alors $k = l$ et si $k \geq 1$ alors chaque p_i (≥ 1) est associé à un q_j $(j \geq 1)$.

Exemple 6.3.1.

1) $\mathbb{Z}$ est un anneau factoriel.

$$\forall n \in \mathbb{Z}\backslash\{0\}, \quad n = \pm 1 p_0 p_1 ..., p_n,$$

où $p_0 = 1$, $k \geq 0$, les p_i $(i \geq 1)$ sont des nombres premiers.

2) Si A est un corps alors A est factoriel.

$$\forall a \in A\backslash\{0\}, \quad a = a,\ a \in A^\times.$$

Définition 6.3.2 (Reformulation de la définition d'un anneau factoriel)**.** Soit A un anneau intègre qui n'est pas un corps et $\mathcal{P}$ un ensemble d'éléments irréductibles de A ($\mathcal{P}$ peut être éventuellement vide). On dit que $\mathcal{P}$ est un système d'irréductibles de A si

(i) $\forall p, p' \in \mathcal{P}$, $p \neq p' \Rightarrow p \nsim p'$,

(ii) $\forall p$ un élément irréductible de A, $\exists p' \in \mathcal{P}$, $p \sim p'$.

Exemple 6.3.2.

1) $A = \mathbb{Z}$. Les éléments irréductibles de $\mathbb{Z}$ sont ± 2, ± 3, ± 5...

$$\mathcal{P} = \{2, 3, 5, ...\},$$

$\mathcal{P}$ est un système d'irréductibles dans $\mathbb{Z}$.

2) $A = \mathbb{C}[X]$. Les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

$$\mathcal{P} = \{x - a,\ a \in \mathbb{C}\},$$

– Soit $a, b \in \mathbb{C}$, $a \neq b$

$$X - a = u(X - b),\ u \in \mathbb{C}^* \Rightarrow 1 = u,$$
$$a \neq b \Rightarrow X - a \nsim X - b.$$

– Soit $aX + b \in \mathbb{C}[X]$ avec $a \neq 0$,

$$aX + b = a\left(X - \left(-\frac{b}{a}\right)\right), \qquad a \in (\mathbb{C}[X])^\times.$$

Définition 6.3.3. Soit A un anneau intègre et $\mathcal{P}$ un système d'irréductibles de A. A est un anneau factoriel, si tout $a \in A\backslash\{0\}$ se factorise en

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)} \tag{6.4}$$

où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ et $v_p(a)$ sont nuls sauf pour un nombre fini de $p \in \mathcal{P}$. (6.4) est unique à l'ordre près des éléments $p \in \mathcal{P}$ et à un élément inversible près.

Exemple 6.3.3. $A = \mathbb{Z}$ et $\mathcal{P} = \{2, 3, 5, ...\}$

$$\forall a \in \mathbb{Z}\backslash\{0\}, \qquad a = \pm 2^{v_2(a)} 3^{v_3(a)} ... = \pm \prod_{p \in \mathcal{P}} p^{v_p(a)}.$$

Par exemple,

$$12 = 2^2 3^1.$$

On a ainsi :

$$\begin{aligned} &v_2(12) = 2, \\ &v_3(12) = 1, \\ &v_p(12) = 0, \qquad v_p \text{ premier} \neq 2, \neq 3. \end{aligned}$$

Définition 6.3.4. Soit A un anneau factoriel, $\mathcal{P}$ un système d'irréductibles de A et $a\backslash A\backslash\{0\}$, a se factorise par

$$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}.$$

– Soit $p \in \mathcal{P}$, $v_p(a)$ est caractérisé par

$$p^{v_p(a)} | a \text{ et } p^{v_p(a)+1} \nmid a$$

– Soit p et p' des éléments irréductibles tels que $p \sim p'$ alors $\forall a \in A\backslash\{0\}$, $v_p(a) = v_{p'}(a)$.
Le nombre $v_p(a)$ est appelé la valuation p-adique de a. Soit l'application

$$\begin{array}{rccc} v_p & : & A\backslash\{0\} & \to & \mathbb{N} \\ & & a & \mapsto & v_p(a) \end{array}.$$

Cette application est bien définie. Par convention, $v_p(0) = +\infty$. On peut donc considérer l'application

$$\begin{array}{rccc} v_p & : & A & \to & \mathbb{N} \cup \{+\infty\} \\ & & a & \mapsto & v_p(a) \end{array}.$$

Propriété 6.3.1 (Valuation p-adique)**.** *Soit A un anneau factoriel, p un élément irréductible de A et $a, b \in A$. Alors :*

(1) si $a|b$, $v_p(b) \geq v_p(a)$,

(2) $v_p(ab) = v_p(a) + v_p(b)$,

(3) $v_p(a + b) \geq \min(v_p(a), v_p(b))$ et on a l'égalité si $v_p(a) \neq v_p(b)$.

Démonstration. (1) $p^{v_p(a)} | a$ et $a|b$ donc $p^{v_p(a)} | b$ donc $v_p(b) \geq v_p(a)$.

(2) (exercice)

(3) (exercice)

□

Theorème 6.3.2. *Soit A un anneau factoriel et a et b des éléments de A tels que $(a, b) \neq (0, 0)$ alors un* PGCD *et un* PPCM *existent.*

Plus précisement,

– *Si $a = 0$ et $b \neq 0$,* $\text{PGCD}(a, b) \sim b$ *et* $\text{PPCM}(a, b) \sim 0$.

– *Si $a \neq 0$ et $b \neq 0$ et $\mathcal{P}$ un système d'irréductibles de A,*

$$\text{PGCD}(a, b) \sim \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))} \text{ et } \text{PPCM}(a, b) \sim \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}.$$

Démonstration. On factorise a et b en éléments irréductibles. Soit $\mathcal{P}$ un système d'éléments irréductibles,

$$a = u \prod_{p\in\mathcal{P}} p^{v_p(a)},\ b = v \prod_{p\in\mathcal{P}} p^{v_p(b)}, \qquad u, v \in A^\times.$$

On démontre que (facilement)

$$\mathrm{PGCD}(a,b) \sim \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))} \text{ et } \mathrm{PPCM}(a,b) \sim \prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}.$$

□

Theorème 6.3.3. *Soit A un anneau factoriel. Alors tout élément irréductible de A est premier (en fait, on a équivalence entre les éléments premiers et les irréductibles).*

Démonstration. On a toujours p premier $\Rightarrow$ p irréductible. Reste à montrer que p irréductible $\Rightarrow$ p est premier. Soit p un élément irréductible de A. Soit $a, b \in A$ tels que $p|ab$. On montre que $p|a$ ou $p|b$.

$$o|ab \Rightarrow v_p(ab) \geq 0.$$

Or :

$$v_p(ab) = v_p(a) + v_p(b),$$

donc :

$$v_p(a) \geq 1 \text{ ou } v_p(b) \geq 1$$

et donc $p|a$ ou $p|b$. □

Theorème 6.3.4. *Dans un anneau factoriel, on a le théorème de Gauss :* Si a, b et c sont des éléments d'un anneau factoriel tels que a divise bc et a et b sont premiers entre eux, alors a divise c.

Démonstration. Soit $a, b, c \in A$ tels que $a|bc$ et $\mathrm{PGCD}(a,b) = 1$. On montre que $a|c$.

- Si $a \in A^\times$, $a|c$.
- On suppose que $a \notin A^\times$. Soit p un élément irréductible tel que p divise a. On montre que $v_p(c) \geq v_p(a)$.

  $$a|bc \Rightarrow v_p(bc) \geq v_p(a).$$

  Or $v_p(bc) = v_p(b) + v_p(c)$ et $\mathrm{PGCD}(a,b) \sim 1$. On en déduit que $v_p(c) \geq v_p(a)$. Comme p est un élément irréductible qui divise a et qu'il est quelconque, on en déduit que $a|c$.

□

Theorème 6.3.5. *Dans un anneau factoriel, on n'a pas forcément le théorème de Bezout.*

Démonstration. On considère l'anneau $\mathbb{Z}[X,Y]$.

- On démontre dans le théorème 6.4.4 que $\mathbb{Z}[X,Y]$ est factoriel.
- On démontre que $\mathrm{PGCD}(X,Y) \sim 1$ et que $(X,Y) \neq 1$.

□

Theorème 6.3.6. *Si A est un anneau principal alors A est factoriel.*

Démonstration. (i) A est intègre.

(ii) *Factorisation en éléments irréductibles* : On suppose qu'il existe un élément $a \in A\backslash\{0\}$ qui ne se factorise pas. Donc, en particulier, $a \notin A^\times$ et a n'est pas irréductible. Donc a s'écrit

$$a = a_1 a_2 \text{ avec } a_1, a_2 \in A^\times.$$

Comme a ne se factorise pas, a_1 ou a_2 ne se factorise pas.
On suppose que a_1 ne se factorise pas. Donc il existe $a_1 \in A$ qui ne se factorise pas tel que $(a) \subsetneqq (a_1)$.
En répétant ce procédé, on construit une suite d'idéaux strictement croissante,

$$(a_0) = (a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq ... \subsetneqq (a_n) \subsetneqq ...$$

Soit $I = \bigsqcup_{k\geq 0}(a_k)$. On vérifie que I est un idéal de A.
Comme A est un anneau principal, il existe $b \in A$ tel que $I = (b)$. Comme $b \in I$, $\exists k_0 \geq 0$ tel que $b \in (a_{k_0})$. Or $(a_{k_0}) \subset (b)$. on en déduit que $I = (b) = (a_{k_0})$. Donc :

$$\forall k \geq k_0, \qquad (a_k) = (a_{k_0}).$$

Ce qui contredit le fait que la suite d'idéaux $(a_{k_0})_{k\geq 0}$ est strictement croissante.

(iii) *Unicité de la décomposition :* Soit $a \in A\backslash\{0\}$.

$$up_1...p_k = vq_0q_1...q_t,$$

où $u, v \in A^\times$, $p_0 = q_0 = 1$, $k \geq 0$ et $t \geq 0$ et $p_1, ..., p_k$, $q_1, ..., q_t$ des éléments irréductibles de A. On suppose que $k \geq 1$, soit $i \geq 1$ tel que

$$p_i | vq_0q_1...q_t.$$

Comme A est principal, p_i irréductible $\Rightarrow p_i$ est premier, donc

$$p_i | q_{i_j}, \qquad 1 \leq i_j \leq t.$$

Comme p_i et q_{i_j} sont irréductibles, on en déduit que $p_i \sim q_{i_j}$. Par conséquent, $k = t$ et chaque p_i est associé à un q_{i_j}.

□

6.4 Factorialité de $A[X]$ si A est factoriel

Soit A un anneau factoriel.

Définition 6.4.1. Soit $P \in A[X]\backslash\{0\}$, on pose

$$P = a_nX^n + ... + a_1X + a_0 \text{ avec } a_i \in A,\ n \geq 0,\ a_n \neq 0.$$

Le contenu de P, qu'on note $c(P)$ est un $\mathrm{PGCD}(a_n, a_{n-1}, ..., a_0)$,

$$c(P) \sim \mathrm{PGCD}(a_n, a_{n-1}, ..., a_0).$$

Définition 6.4.2. On dit que P est primitif si $c(P) \sim 1$.

Proposition 6.4.1. *Soit $P, Q \in A[X]\backslash\{0\}$. Alors*

$$c(PQ) = c(P)c(Q)$$

Démonstration. On pose

$$P = c(P)P_0 \text{ et } Q = c(Q)Q_0,$$

où P_0, Q_0 sont des polynômes primitives. Donc

$$c(PQ) = c(P)c(Q)c(P_0Q_0)$$

Le problème revient à montrer que si P_0 et Q_0 sont primitifs alors P_0Q_0 est primitif. Par l'absurde, on suppose que P_0Q_0 n'est pas primitif alors $c(P_0Q_0) \notin A^\times$ donc il existe $p \in A$ irréductible tel que $p|c(P_0Q_0)$. On considère le morphisme de réduction

$$\begin{array}{rccc} : & A[X] & \to & A/(P)[X] \\ & P = a_0 + a_1X + ... + a_nX^n & \mapsto & \overline{P} = a_0 + (P) + (a_1 + (P))X + ... + (a_n + (P))X^n \end{array}$$

On a $\overline{P_0Q_0} = \overline{0} = \overline{P_0}\,\overline{Q_0}$. A est factoriel donc p est premier, puisque p est irréductible et donc (p) est un idéal premier. Par conséquent, $A/(P)$ est un anneau intègre, on déduit que $A/(P)[X]$ est intègre. De l'égalité $\overline{P_0Q_0} = \overline{0}$, on en déduit que

$$\overline{P_0} = \overline{0} \text{ ou } \overline{Q_0} = \overline{0}.$$

$\overline{P_0} = \overline{0} \Rightarrow p|c(P_0)$, ce qui est absurde puisque P_0 est un polynôme primitif. □

Theorème 6.4.2 (Caractérisation des éléments irréductibles de $A[X]$)**.** *Soit A un anneau factoriel alors les éléments irréductibles de $A[X]$ sont :*

(i) $a \in A$, *avec a irréductible dans A,*

(ii) $P \in A[X]\backslash\{0\}$ *tel que* $\deg P \geq 1$, *P est irréductible dans* $\mathrm{Fr}(A)[X]$ *et P est primitif.*

Lemme 6.4.3. *Soit $P \in \mathrm{Fr}(A)[X]$ alors il existe $\alpha \in \mathrm{Fr}(A)$ et $P_0 \in A[X]$ primitif tel que*

$$P = \alpha P_0.$$

Démonstration du lemme 6.4.3. On pose

$$P = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + ... + \frac{a_n}{b_n}X^n, \qquad \text{où } a_i, b_i \in A.$$

Alors P s'écrit

$$\begin{aligned} P &= \frac{c_0 + c_1X + ... + c_nX^n}{b_0 + b_1 + ... + b_n}, \qquad c_i \in A \\ &= \frac{Q(x)}{b} \qquad \text{avec } Q \in A[X],\ b \in A \\ &= \frac{c(Q)}{b}Q_0 \qquad \text{où } Q_0 \in A[X] \text{ primitif.} \end{aligned}$$

□

Démonstration du théorème 6.4.2. 1) Soit $P \in A[X]\backslash\{0\}$ tel que P est irréductible dans $A[X]$.

(i) On suppose que $P \in A\backslash\{0\}$. on veut montrer que P est un élément irréductible de A. On suppose que $P = ab$ avec $a, b \in A$. On a cette écriture dans $A[X]$. Comme P est irréductible dans $A[X]$,

$$Q \in (A[X])^\times \quad \text{où } b \in (A[X])^\times.$$

Or : $(A[X])^\times = A^\times$. Donc :

$$a \in A^\times \text{ ou } b \in A^\times.$$

(ii) On suppose que $\deg P \geq 1$.

- On montre que P est primitif. On pose

$$P = c(P)P_0 \quad \text{où } P_0 \text{ est primitif, } \deg(P_0) \geq 1.$$

Comme P est irréductible dans $A[X]$,

$$c(P) \in \underbrace{(A[X])^\times}_{=A^\times} \quad \text{où } P_0 \in \underbrace{(A[X])^\times}_{=A^\times}.$$

Comme $\deg P_0 \geq 1$, $P_0 \notin A^\times$. Donc $c(P) \in A^\times$. Par conséquent, P est primitif.

- On montre que P est irréductible dans $\mathrm{Fr}(A)[X]$. Par l'absurde, on suppose que P s'écrit

$$P = P_1P_2 \quad \text{avec } P_i \in \mathrm{Fr}(A)[X].$$

D'après le lemme 6.4.3, il existe $\alpha \in \mathrm{Fr}(A)$, $P_{1,0}, P_{2,0} \in A[X]$ primitifs tels que :

$$P = \alpha P_{1,0}P_{2,0} \text{ et } \deg(P_{i,0}) \geq 1.$$

On pose : $\alpha = \frac{a}{b}$, $a, b \in A$. On a :

$$bP = aP_{1,0}P_{2,0}.$$

En considérant le contenu des polynômes :

$$b\underbrace{c(P)}_{=1} \sim a\underbrace{c(P_{1,0})}_{=1}\underbrace{c(P_{2,0})}_{=1}$$
$$\Rightarrow b \sim a.$$

Donc on obtient :

$$P = uP_{1,0}P_{2,0} \text{ où } u \in A^\times.$$

et $\deg(P_{i,0} \geq 1$. Comme P est irréductible dans $A[X]$, on a une contradiction.

2) Reste à montrer que si $P \in A[X]$ est du type (i) ou (ii), P est irréductible.

(i) On suppose que $P \in A\backslash\{0\}$ et que P est irréductible dans A. On montre que P est irréductible dans $A[X]$. On suppose que $P = P_1P_2$ avec $P_i \in A[X]$. On a :

$$\deg P = \deg P_1 + \deg P_2 = 0.$$

Donc : $P_1 + P_2 \in A$. Comme P est irréductible dans A, P_1 ou $P_2 \in A^\times$. Or $A^\times = (A[X])^\times$. Donc P_1 ou $P_2 \in (A[X])^\times$.

(ii) On suppose que $\deg P \geq 1$, P primitif et P est irréductible dans $\mathrm{Fr}(A)[X]$. On montre que P est irréductible dans $A[X]$. On suppose que

$$P = P_1P_2 \text{ avec } P_1, P_2 \in A[X].$$

Comme P est irréductible dans $\mathrm{Fr}(A)[X]$, P_1 ou $P_2 \in (\mathrm{Fr}(A)[X])^\times = \mathrm{Fr}(A)\backslash\{0\}$. On suppose que $P_1 = a \in A$. Donc $P = aP_2$ avec $a \in A$ et $P_2 \in A[X]$. On a aussi

$$c(P) = ac(P_2) \sim 1.$$

Puisque P est primitif, $P_1 = a \in A^\times$.

Même démonstration si $P_2 \in A$.

□

Exercice 6.4.1. Soit

$$A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3},\ a, b \in \mathbb{Z}\}.$$

On pose :

$$K = \mathrm{Fr}(A) = \{a + ib\sqrt{3},\ a, b \in \mathbb{Q}\}.$$

Soit $P = X^2 + X + 1$.

1) *Montrer que P est irréductible dans $A[X]$.* On suppose que P n'est pas irréductible donc P s'écrit :

$$P = P_1 P_2, \quad P_1, P_2 \in A[X], \deg P_i = 1 \text{ (pusique } P \text{ primitif)}.$$

On pose

$$P = (aX + b)(cX + d), \quad a, b, c, d \in A,\ a, c \neq 0.$$

$$ac = 1 \Rightarrow a \in A^\times \Rightarrow P = a(X + ba^{-1})(cX + d)$$
$$\Rightarrow \exists \alpha \in A \text{ tel que } P(\alpha) = 0$$

Or les racines de P ne sont pas des éléments de A ($\frac{-1 \pm i\sqrt{3}}{2} \notin A$). Contradiction !

2) *Montrer que P est non irréductible dans $K[X]$.* Cette fois-ci, on a :

$$P = (X - j)(X - j^2) \text{ et } j, j^2 \in K.$$

Theorème 6.4.4 (Théorème de Gauss)**.** *Si A est factoriel, $A[X]$ est aussi factoriel.*

Démonstration. (i) A factoriel $\Rightarrow$ A intègre $\Rightarrow$ $A[X]$ intègre.

(ii) *Factorisation en éléments irréductibles.* Soit $P \in A[X]\backslash\{0\}$, $K = \mathrm{Fr}(A)$, K est un corps donc $K[X]$ est un anneau principal et donc $K[X]$ est un anneau factoriel. P vu comme élément de $K[X]$ se factorise :

$$P = uP_0P_1...P_k,$$

où $u \in (K[X])^\times = K\backslash\{0\}$, $k \geq 0$, $P_0 = 1$, et pour $i \geq 1$, P est un élément irréductible de $K[X]$ (donc $\deg P_i \geq 1$). Pour $i \geq 1$, on pose :

$$P = \alpha P_{i,0}$$

où $\alpha_i \in K\backslash\{0\}$, $P_{i,0} \in A[X]$ primitif ($\deg P_{i,0} \geq 1$). Donc il existe $\alpha \in K\backslash\{0\}$ tel que :

$$P = \alpha P_0 P_{1,0}...P_{k,0}.$$

On a, pour $i \geq 1$, $P_i \sim P_{i,0}$ dans $K[X]$, P_i est irréductible dans $K[X]$ donc $P_{i,0}$ est irréductible dans $K[X]$. Comme $P_{i,0} \in A[X]$ et $P_{i,0}$ est primitif, $P_{i,0}$ est irréductible dans $A[X]$. On pose $\alpha = a/b$, avec $a, b \in A$. Donc on a :

$$bP = aP_0P_{1,0}...P_{k,0}.$$

En considérant le contenu, on a :

$$bc(P) \sim a \qquad \text{dans } A,$$

puisque pour $i \geq 1$, $P_{i,0}$ est primitif. On pose $a = vbc(P)$, $v \in A^\times$. Donc on a :

$$P = vc(P)P_0P_{1,0}...P_{k,0}, \qquad \text{où } v \in A^\times,$$

et pour $i \geq 1$, $P_{i,0}$ est irréductible dans $A[X]$. Comme $c(P) \in A\backslash\{0\}$ et A est factoriel, $c(P)$ se factorise :

$$c(P) = wq_0q_1...q_t,$$

où $w \in A^\times$, $q_0 = 1$, $t \geq 0$ et pour $i \geq 1$, q_i est un élément irréductible de A (donc q_i est irréductible dans $A[X]$). Finalement, on a

$$P = \alpha q_0q_1...q_tP_0P_{1,0}...P_{k,0},$$

où $\alpha \in A^\times$, $t \geq 0$, $k \geq 0$, $q_0 = p_0 = 1$ et pour $i \geq 1$, $P_{i,0}$ et q_i sont des éléments irréductibles de $A[X]$.

(iii) *Unicité de la factorisation.* Soit $P \in A[X]\backslash\{0\}$, on suppose que

$$P = \alpha p_0p_1...p_kP_0P_1...P_t = \beta q_0q_1...q_nQ_0...Q_n, \tag{6.5}$$

où $\alpha, \beta \in A^\times$, $k \geq 0$, $t \geq 0$, $n \geq 0$, $m \geq 0$, $p_0 = P_0 = Q_0 = q_0 = 1$, pour $i \geq 1$, p_i et q_i sont irréductibles dans A et P_i et Q_i sont des polynômes de degré ≥ 1 irréductibles dans $A[X]$. En regardant l'égalité (6.5) dans $K[X]$, il existe $\alpha \in K\backslash\{0\}$ tel que

$$P_0P_1...P_t = \alpha Q_0Q_1...Q_n.$$

Comme pour $i \geq 1$, les P_i et Q_i sont des polynômes de degré ≥ 1, irréductibles dans $A[X]$, ils sont primitifs et irréductibles dans $K[X]$. $K[X]$ étant factoriel, on en déduit que $t = m$ et pour $i \geq 1$,

$$P_i \sim Q_{i,j} \qquad \text{dans } K[X],$$

c'est-à-dire $\alpha_i \in K\backslash\{0\}$ tel que $P_i = \alpha_iQ_{ij}$. On montre que $P_i \sim Q_i$, dans $A[X]$, on pose $\alpha_i = a_i/b_i$, $a_i, b_i \in A$, on a :

$$b_iP_i = a_iQ_{ij}.$$

En considérant le contenu et comme les P_i et Q_{ij} sont primitifs,

$$u_ib_i = a_i, \qquad \text{où } u_i \in A^\times.$$

Donc $\alpha_i = a_i/b_i = u_i \in A^\times$. On revient à l'égalité (6.5) et on déduit qu'il existe $\gamma \in A^\times$ tel que

$$p_0p_1...p_k = \gamma q_0q_1...q_n.$$

On a cette égalité dans A. Comme A est factoriel, on en déduit que $k = n$ et pour $i \geq 1$, $p_i \sim q_{ij}$ dans A.

□

Corollaire. *A factoriel $\Rightarrow A[X_1, ..., X_n]$ factoriel.*

Démonstration. A est factoriel implique que $A[X_1]$ est factoriel d'après le théorème 6.4.4. On veut montrer

$$A[X_1] \text{ factoriel} \overset{?}{\Rightarrow} A[X_1, X_2] \text{ factoriel.}$$

On peut voir $A[X_1, X_2]$ comme l'ensemble des polynômes à coefficients dans X_1 et à indéterminées dans X_2. Comme $A[X_1]$ est factoriel, on applique de nouveau le théorème 6.4.4 pour avoir que $A[X_1][X_2]$ est factoriel et donc, par conséquent, $A[X_1, X_2]$ est factoriel... □

Remarque. Si A est factoriel et si on a Bezout (c'est-à-dire $\forall a, b \in A\backslash\{0\}$, si $d = \text{PGCD}(a, b)$, alors il existe $u, v \in A$ tels que $d = ua + bv$) alors A est principal.

Démonstration. Soit I un idéal non nul et propre de A. On montre que I est principal. Soit $a \in I\backslash\{0\}$ (donc $a \notin A^\times$). Comme A est factoriel, a se factorise

$$a = up_1...p_k,$$

où $u \in A^\times$, $k \geq 1$, p_i irréductible dans A. Donc a admet un nombre fini de diviseurs non associés et donc il exsite une suite d'idéaux

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq ... \subsetneqq (a_n) \subset I.$$

Soit (α) le plus grand idéal qui vérifie

$$(a) \subsetneqq (\alpha) \subset I.$$

On montre que $I = (\alpha)$. On suppose que $(\alpha) \subsetneqq I$ alors il existe $\beta \in I\backslash(\alpha)$, on a : $(\alpha) \subsetneqq (\alpha, \beta) \subset I$. Soit $d = \text{PGCD}(\alpha, \beta)$. D'après Bezout, il existe $u, v \in A$ tels que

$$d = \alpha u + \beta v.$$

Donc :

$$(\alpha, \beta) = (d),$$

et on obtient que

$$(\alpha) \subsetneqq (d) \subset I,$$

ce qui est absurde. □

6.5 Critères d'irréductibilité dans $A[X]$

Theorème 6.5.1 (Critère de réduction modulo un idéal premier)**.** *Soit A un anneau factoriel, I un idéal premier de A et $P \in A[X]$ de degré ≥ 1. Soit le morphisme de réduction* $\bmod I$ *:*

$$\begin{array}{rccc} : & A[X] & \to & A/I[X] \\ & F & \mapsto & \overline{F} = F \mod I \end{array}.$$

Si $\deg \overline{P} = \deg P$ *et* $\overline{P}$ *est irréductible dans* $A/I[X]$ *alors* P *est irréductible dans* $\text{Fr}(A)[X]$ *et s'il est primitif,* P *est irréductible dans* $A[X]$*.*

Démonstration. Par l'absrude, on suppose que P est réductible dans $K[X]$ alors P s'écrit

$$P = P_1P_2 \text{ avec } P_i \in K[X], \deg P_i \geq 1.$$

Lemme 6.5.2. *P s'écrit aussi dans $A[X]$,*

$$P = Q_1Q_2 \text{ avec } Q_1, Q_2 \in A[X], \deg Q_i \geq 1.$$

Démonstration du lemme 6.5.2. en exercice. □

En utilisant le lemme 6.5.2,

$$\overline{P} = \overline{Q_1Q_2}.$$

Comme I est un idéal, A/I est un anneau intègre donc $A/I[X]$ est intègre. Par conséquent,

$$\deg \overline{P} = \deg \overline{Q_1} + \deg \overline{Q_2}.$$

Or $\deg \overline{Q_i} \leq \deg Q_i$ et $\deg \overline{P} \leq \deg P$, donc :

$$\deg P = \deg \overline{Q_1} + \deg \overline{Q_2} \leq \deg Q_1 + \deg Q_2 = \deg P.$$

On déduit que $\deg \overline{Q_i} = \deg Q_i \geq 1$. Donc, on a :

$$\overline{P} = \overline{Q_1 Q_2} \text{ et } \deg \overline{Q_i} \geq 1,$$

ce qui contredit le fait que $\overline{P}$ est irréductible dans $A/I[X]$. □

Exercice 6.5.1. *Les polynômes suivanats sont-ils irréductibles ?*

1. $P = X^3 - X - 1$ *dans* $\mathbb{Z}/2\mathbb{Z}[X]$ (irréductible) *et dans* $\mathbb{Z}[X]$.

$$\begin{array}{rccc} : & \mathbb{Z}[X] & \to & \mathbb{Z}/2\mathbb{Z}[X] \\ & P = X^3 - X - 1 & \mapsto & \overline{P} = X^3 - X - 1 \end{array},$$

   $\deg \overline{P} = \deg P$.

2. $P(X, Y) = X^2 + Y^2 + 1$ *dans* $\mathbb{R}[X, Y]$. On considère P comme élément de $\mathbb{R}[X][Y]$, (Y) est un idéal premier de $\mathbb{R}[Y]$,

$$\begin{array}{rccc} : & \mathbb{R}[Y][X] & \to & (\mathbb{R}[Y]/(Y))[X] \\ & P = X^2 + Y^2 + 1 & \mapsto & \overline{P} = X^2 + 1 \end{array},$$

$$\deg_X \overline{P} = \deg_X P,$$

   et

$$\mathbb{R}[Y]/(Y) \overset{\text{isom}}{\simeq} \mathbb{R} \qquad \text{(exercice)}.$$

   $\overline{P}$ est irréductible dans $\mathbb{R}[X]$ et donc dans $(\mathbb{R}[Y]/(Y))[X]$.

Theorème 6.5.3 (Critère d'Eisentein)**.** *Soit A un anneau factoriel et p un élément irréductible de A. Soit $P \in A[X]$ de degré ≥ 1, on pose :*

$$P = a_0 + a_1 X + ... + a_n X^n,$$

avec $a_i \in A$, $a_n \neq 0$. Soit p un élément irréductible de A vérifiant :

(i) p divise a_i pour tout $0 \leq i \leq n-1$,

(ii) p ne divise pas a_n,

(iii) p^2 ne divise pas a_0.

Alors P est irréductible dans $(\mathrm{Fr}(A))[X]$ et s'il est primitif, P est irréductible dans $A[X]$.

Démonstration. On suppose que P est réductible dans $K[X]$. Donc P s'écrit :

$$P = P_1 P_2 \qquad \text{avec } P_i \in A[X], \deg P_i \geq 1.$$

On pose :

$$P_1 = c_0 + c_1 X + ... + c_n X^n,$$
$$Q_1 = b_0 + b_1 X + ... + b_k X^k.$$

On a ainsi $a_i = \sum_{l+t=i} c_l b_t$. Comme $p | a_0$ et $p^2 \nmid a_0$, p divise par exemple b_0 et ne divise pas c_0. Comme $p \nmid a_n$, $p \nmid c(P)$ et donc $p \nmid c(P_i)$, $i = 1, 2$. Soit j le plus petit entier ≥ 1 tel que $p \nmid b_j$. On considère

$$a_j = \underbrace{b_0 c_j + b_1 c_{j-1} + ... + b_{j-1} c_1}_{\text{divisible par } p} + b_j c_0.$$

Par ailleurs,

$$P = P_1 P_2, \qquad \deg P_i \geq 1.$$

Donc : $j \leq n-1$ et donc $p|a_j$. On en déduit que $p|b_j c_0$. Ce qui est absurde puisque $p \nmid b_j$ et $p \nmid c_0$. □

Exercice 6.5.2. Les polynômes suivants sont-ils irréductibles ?
- $P(X) = 2X^9 + 3X^6 - 6X^3 + 9X - 12$, dans $\mathbb{Q}[X]$, dans $\mathbb{Z}[X]$,
- $P(X,Y) = 4YX^4 + 2Y^2 - 2$, dans $\mathbb{Z}[X,Y]$, dans $\mathbb{Q}[X,Y]$, dans $\mathbb{Q}(X,Y)$ où

$$\mathbb{Q}(X,Y) = \left\{ \frac{P(X,Y)}{Q(X,Y)},\ P, Q \in \mathbb{Q}[X,Y] \right\}.$$

6.6 Arithmétique dans un anneau

Pour fixer les idées, on donner un résumé des types d'anneaux dans lesquels on peut manipuler certaines notions arithmétiques.

(i) D'abord, on rappelle que : un anneau euclidien ⇒ principal ⇒ factoirel et les réciproques sont fausses.

(ii) Dans un anneau non factoriel, deux éléments n'admettent pas nécessairement un PGCD, PPCM.

(iii) Dans un anneau factoriel,
- on a une factorisation en éléments irréductibles et cette factorisation est unique à éléments inversibles près et à permutation des irréductibles près,
- deux éléments non nuls quelconques admettent un PGCD, PPCM,
- on a le théorème de Gauss : Si a divise bc et a et b sont premiers entre eux, a divise c,
- en général, on n'a pas le théorème de Bezout : Si $d = \mathrm{PGCD}(a,b)$, alors il existe u, v tel que $au + bv = d$.

(iv) Dans un anneau principal, on a le théorème de Bezout.