

# Outils d’algèbre générale

B. Seddoug. Médiane Sup, Oujda

## Table des matières

<b>I Idéaux d’un anneau commutatif</b>	<b>1</b>
I.1 Définitions . . . . .	1
I.2 Idéaux de $\mathbb{Z}$ . . . . .	3
<b>II Congruence dans <math>\mathbb{Z}</math></b>	<b>5</b>
II.1 Définitions – Exemples . . . . .	5
II.2 L’anneau $\mathbb{Z}/n\mathbb{Z}$ . . . . .	6
II.3 Fonction indicatrice d’Euler . . . . .	9
<b>III Le cas de <math>\mathbb{K}[X]</math></b>	<b>16</b>
III.1 Division euclidienne dans $\mathbb{K}[X]$ . . . . .	16
III.2 Idéaux de $\mathbb{K}[X]$ . . . . .	17

III.3 Propriétés arithmétiques de $\mathbb{K}[X]$ . . . . .	17
---	----

<b>IV Fonction polynômiale</b>	<b>20</b>
IV.1 Rappels . . . . .	20
IV.2 Polynôme annulateur . . . . .	24
IV.3 Polynôme minimal . . . . .	26

## I Idéaux d’un anneau commutatif

### I.1 Définitions

**Définition I.1** Un idéal  $I$  est un sous-groupe additif, stable par multiplication par tout élément de l’anneau  $\mathcal{A}$  :

- $\forall x, y \in I : x - y \in I$
- $\forall a \in \mathcal{A}, \forall x \in I : ax \in I$

**Définition I.2** Un idéal principal est une partie de la forme  $a\mathcal{A} = \{ax \mid x \in \mathcal{A}\}$ . C’est l’idéal engendré par  $a$  (le plus petit qui contienne  $a$ ).

**Exercice I.1**  $a\mathcal{A} = b\mathcal{A}$  si, et seulement si,  $a = bu$  avec  $u$  inversible.

①

**Remarque I.1** Si  $\mathcal{A}$  est une algèbre tout idéal est en un sous espace vectoriel.

#### propriétés

- (1) La somme (resp. l’intersection) d’une famille d’idéaux est un idéal.
- (2) Le noyau d’un morphisme d’anneaux est un idéal.
- (3) Un idéal est l’anneau entier si et seulement si il contient un élément inversible.
- (4)  $a$  divise  $b$  (ie  $\exists c \in \mathcal{A} \mid b = ac$ ) si et seulement si l’idéal  $a\mathcal{A}$  contient l’idéal  $b\mathcal{A}$ .

②

### I.2 Idéaux de $\mathbb{Z}$

**Théorème I.1** Tout idéal de  $\mathbb{Z}$  est principal.

**Preuve:** Utilise la division euclidienne.

#### PGCD et PPCM dans $\mathbb{Z}$

Dans  $\mathbb{Z}$  tout idéal est principal, on déduit donc :

**Proposition I.1** Soient  $a, b \in \mathbb{Z}$ , on a :

- $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$  avec  $d = \text{PGCD}(a, b)$ .
- $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$  avec  $m = \text{PPCM}(a, b)$ .

③

**Théorème I.2 (Bezout)** Les entiers  $a$  et  $b$  sont premiers entre eux si et seulement si il existe  $u, v$  tels que  $au + bv = 1$ .

**Théorème I.3 (Gauss)** Soient  $a, b, c \in \mathbb{Z}$ ; si  $a$  divise  $bc$  en étant premier avec  $c$ , alors  $a$  divise  $b$ .

Deux autres propositions :

**Proposition I.2 (Euclide)** Si  $a$  est premier avec  $b$  et avec  $c$ , alors il est premier avec  $bc$ .

**Proposition I.3** Si  $a$  et  $b$  sont premiers entre eux et divisent tous deux  $c$ , alors  $ab$  divise  $c$ .

④

**Exercice I.2** Montrer que si le carré d’un rationnel est un entier, alors ce rationnel est entier.

## II Congruence dans $\mathbb{Z}$

### II.1 Définitions – Exemples

**Définition II.1** On dit que  $a$  est congru à  $b$  modulo  $n$  et on note  $a \equiv b \pmod{n}$  si  $n$  divise  $|b - a|$ , i.e :

$$a \equiv b \pmod{n} \iff a - b \in n\mathbb{Z}.$$

⑤

<p>La relation <math>(\text{mod } n)</math> est une relation d'équivalence, ses classes constituent l'ensemble <math>\mathbb{Z}/n\mathbb{Z}</math>. Ainsi la classe de <math>a \in \mathbb{Z}</math> est</p> $\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}.$ <p><b>II.2 L'anneau <math>\mathbb{Z}/n\mathbb{Z}</math></b></p> <p><b>Théorème II.1</b> L'ensemble <math>\mathbb{Z}/n\mathbb{Z}</math> a exactement <math>n</math> éléments. C'est un anneau avec les lois définies par</p> $\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \times \bar{b} = \overline{a \times b}$ <p>Ses éléments neutres sont <math>\bar{0}</math> et <math>\bar{1}</math>.</p> <p><b>Preuve:</b> La faire comme exercice (Sup).</p> <p style="text-align: right;">⑥</p>	<p><b>Proposition II.1</b> L'application <math>a \in \mathbb{Z} \mapsto \bar{a} \in \mathbb{Z}/n\mathbb{Z}</math> est un morphisme d'anneaux surjectif.</p> <p><b>Théorème II.2</b> <math>\mathbb{Z}/n\mathbb{Z}</math> est un corps si et seulement si <math>n</math> est premier.</p> <p>On a ainsi une famille infinie de corps, finis et de cardinal premier.</p> <p><b>Preuve:</b> Utiliser Bezout.</p> <p><b>Exercice II.1</b> Dédurre du Théorème de Gauss que pour <math>p</math> premier, <math>p</math> divise tous les <math>\binom{p}{k}, k = 1 \dots p-1</math>. On en déduit dans <math>\mathbb{Z}/p\mathbb{Z}</math>, on a la relation <math>(a+b)^p = a^p + b^p</math>.</p> <p style="text-align: right;">⑦</p>
<p><b>Exercice II.2</b> Montrer que tout anneau (commutatif) FINI et intègre est un corps.</p> <p>Dans ce cas, on a des résultats classiques :</p> <p><b>Exercice II.3</b> Dans <math>\mathbb{Z}/p\mathbb{Z}</math>, <math>p</math> premier, on considère l'application <math>x \mapsto ax</math> où <math>a</math> est un élément inversible fixé.</p> <p>(1) Montrer que l'application est bijective (c'est même un automorphisme du groupe additif). En déduire le (petit !)</p> <p>(2) Théorème de Fermat : <math>a^{p-1} \equiv 1 \pmod{p}</math> pour <math>a \wedge p = 1</math>, et le</p> <p style="text-align: right;">⑧</p>	<p>(3) Théorème de Wilson : <math>(p-1)! \equiv -1 \pmod{p}</math> en travaillant sur <math>\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} ax</math></p> <p><b>Exercice II.4</b> Trouver les diviseurs de zéro dans <math>\mathbb{Z}/20\mathbb{Z}</math>.</p> <p><b>Exercice II.5</b> Résoudre <math>6x^2 - 5x + 1 \equiv 0 \pmod{p}</math> pour divers nombres premiers <math>p</math>.</p> <p><b>II.3 Fonction indicatrice d'Euler</b></p> <p><b>Théorème II.3</b> Les éléments de <math>\mathbb{Z}/n\mathbb{Z}</math> se répartissent en deux classes :</p> <p style="text-align: right;">⑨</p>
<ul style="list-style-type: none"> <li>• Les diviseurs de zéro; ce sont les <math>\bar{a} \in \mathbb{Z}/n\mathbb{Z}</math> tels qu'il existe <math>\bar{b} \neq \bar{0}</math> avec <math>\bar{a} \times \bar{b} = \bar{0}</math></li> <li>• Les éléments inversibles pour <math>\times</math>, qui vérifient</li> </ul> $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^* \iff a \wedge n = 1$ <p><math>(\mathbb{Z}/n\mathbb{Z})^*</math> désigne le groupe des inversible de <math>\mathbb{Z}/n\mathbb{Z}</math>. Ces éléments inversibles sont précisément les générateurs du groupe <b>cyclique</b> <math>\mathbb{Z}/n\mathbb{Z}</math>.</p> <p><b>Définition II.2</b> le cardinal de <math>(\mathbb{Z}/n\mathbb{Z})^*</math> est noté <math>\Phi(n)</math>, appelé indicateur d'Euler de <math>n</math>. <math>\Phi</math> est appelée fonction indicatrice d'Euler. On convient que <math>\Phi(1) = 1</math>. Par exemple, <math>\Phi(p) = p-1</math> pour <math>p</math> premier. Et en général, on a :</p> <p style="text-align: right;">⑩</p>	<p><b>Proposition II.2</b> Si <math>p \geq 2</math> est premier alors pour tout <math>\alpha \in \mathbb{N}^*</math> ;</p> $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \left(1 - \frac{1}{p}\right).$ <p><b>Preuve:</b> <math>\Phi(p^\alpha)</math> est égal au nombre des <math>m \in [1, p^\alpha - 1]</math> qui ne sont pas divisibles par <math>p</math>. Il s'agit donc des entiers qui ne sont pas de la forme</p> $kp \text{ avec } 1 \leq k \leq p^{\alpha-1} - 1$ <p>qui sont en nombre de <math>p^{\alpha-1} - 1</math>. Donc <math>\Phi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^\alpha - p^{\alpha-1}</math>.</p> <p><b>Théorème II.4</b> Soient <math>m \geq 2</math> et <math>n \geq 2</math> deux entiers <b>premiers entre eux</b>. Alors <math>\Phi(nm) = \Phi(m)\Phi(n)</math>.</p> <p style="text-align: right;">⑪</p>
<p><b>Preuve:</b> Il s'agit de montrer que</p> $\text{card} (\mathbb{Z}/nm\mathbb{Z})^* = \text{card} (\mathbb{Z}/m\mathbb{Z})^* \times \text{card} (\mathbb{Z}/n\mathbb{Z})^*.$ <p>Pour cela on montre que l'application <math>\psi</math> :</p> $(\mathbb{Z}/nm\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$ $\bar{k} \longmapsto \left( \overset{\bullet}{\bar{k}}, \overset{\bullet\bullet}{\bar{k}} \right)$ <p>où <math>\overset{\bullet}{\bar{k}}</math> et <math>\overset{\bullet\bullet}{\bar{k}}</math> désignent respectivement les classes de <math>k</math> dans <math>\mathbb{Z}/n\mathbb{Z}</math> et <math>\mathbb{Z}/m\mathbb{Z}</math>, est bijective. On démontre d'abord le</p> <p><b>Lemme II.1 (Théorème des restes chinois)</b> Si <math>m \geq 2</math> et <math>n \geq 2</math></p> <p style="text-align: right;">⑫</p>	<p>deux entiers <b>premiers entre eux</b>. Alors le système de congruence</p> $\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad (\text{II.1})$ <p>admet des une solution pour tout <math>a, b</math> dans <math>\mathbb{Z}</math>. En plus si <math>x</math> et <math>y</math> sont solution alors <math>x \equiv y \pmod{nm}</math>.</p> <p><b>En effet:</b> Soient <math>u, v \in \mathbb{Z}</math> tels que <math>un + vm = 1</math>, donc <math>\overset{\bullet\bullet}{un} = \overset{\bullet}{1}</math> et <math>\overset{\bullet}{vm} = \overset{\bullet\bullet}{1}</math>. On pose <math>x = avn + bum</math>. On a alors</p> $\overset{\bullet}{x} = \overset{\bullet}{avn} + \overset{\bullet}{bum} = \overset{\bullet}{a} \text{ et } \overset{\bullet\bullet}{x} = \overset{\bullet\bullet}{avn} + \overset{\bullet\bullet}{bum} = \overset{\bullet\bullet}{b}$ <p>ce qui signifie que <math>x</math> est solution du problème (II.1).</p> <p style="text-align: right;">⑬</p>

<p>Soient <math>x = a + kn = b + k'm</math> et <math>y = a + hn = b + h'm</math> deux solutions.          Alors <math>y - x \in n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}</math> (car <math>n \wedge m = 1</math>).  <b>Retour au théorème:</b> Le lemme montre que <math>\psi</math> est surjective : si <math>\begin{pmatrix} \dot{a} &amp; \ddot{b} \\ \dot{a} &amp; \ddot{b} \end{pmatrix} \in (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*</math> alors il existe <math>x \in \mathbb{Z}</math> tel que</p> $\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$ <p>ce qui signifie que <math>\dot{x} = \dot{a}</math> et <math>\ddot{x} = \ddot{b}</math> et puisque <math>x \wedge n = a \wedge n = 1</math> et <math>x \wedge m = b \wedge m = 1</math> alors <math>x</math> est premier avec <math>n</math> et <math>m</math> qui sont premiers entre eux donc il est premier avec leur produit.</p> <p style="text-align: right;">(14)</p>	<p>D'autre part si <math>\bar{k}'</math> et <math>\bar{k}</math> ont même image <math>\begin{pmatrix} \dot{a} &amp; \ddot{b} \\ \dot{a} &amp; \ddot{b} \end{pmatrix}</math> alors <math>k</math> et <math>k'</math> sont solution du problème (II.1) et sont donc <math>\equiv \pmod{mn}</math> donc <math>k' = k</math>. Donc <math>\psi</math> est injective et par conséquent bijective.</p> <p><b>Théorème II.5</b> Pour tout <math>n = \prod_i p_i^{m_i} \geq 2</math>, les <math>p_i</math> premiers,</p> $\Phi(n) = \prod_i p_i^{m_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{p \text{ premier, divisant } n} \left(1 - \frac{1}{p}\right)$ <p><b>Exemple II.1</b> <math>\Phi(n = 2^a 3^b) = \frac{1}{2} \frac{2}{3} n</math> si <math>a, b \in \mathbb{N}^*</math>.</p> <p style="text-align: right;">(15)</p>
<p><b>III Le cas de <math>\mathbb{K}[X]</math></b></p> <p>Curieusement, tout se passe comme dans <math>\mathbb{Z}</math>. C'est qu'on a la même propriété d'existence d'une division euclidienne :</p> <p><b>III.1 Division euclidienne dans <math>\mathbb{K}[X]</math></b></p> <p><b>Théorème III.1</b> Soient <math>A, B \in \mathbb{K}[X]</math>, <math>B</math> non nul. Alors il existe un et un seul couple <math>(Q, R)</math> tel que <math>A = B.Q + R</math> et <math>\deg(R) &lt; \deg(B)</math>.</p> <p><b>Preuve:</b> par récurrence sur le degré : c'est effectuer la division en partant du terme de plus haut degré !</p> <p style="text-align: right;">(16)</p>	<p><b>III.2 Idéaux de <math>\mathbb{K}[X]</math></b></p> <p><b>Théorème III.2</b> <math>\mathbb{K}[X]</math> est principal, i.e. les idéaux de <math>\mathbb{K}[X]</math> sont engendrés par un seul élément : ils sont de la forme <math>I = P.\mathbb{K}[X]</math>.</p> <p><b>Preuve:</b> La division euclidienne ! ...</p> <p><b>III.3 Propriétés arithmétiques de <math>\mathbb{K}[X]</math></b></p> <p>Comme dans <math>\mathbb{Z}</math>, <math>\mathbb{K}[X]</math> étant principale, alors les Théorèmes de Gauss, Bezout, Euclide, . . . s'appliquent. PGCD et PPCM existent et sont uniques (à un élément inversible, càd une unité, càd une constante non nulle, près). Il y a factorisation unique en produit de facteurs irréductibles, unique à l'ordre près, en</p> <p style="text-align: right;">(17)</p>
<p>prenant les facteurs unitaires. Dans <math>\mathbb{Z}</math> tout idéal est principal, on déduit donc :</p> <p><b>Proposition III.1</b> Soient <math>A, B \in \mathbb{K}[X]</math>, on a :</p> <ul style="list-style-type: none"> <li><math>A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]</math> avec <math>D = \text{PGCD}(A, B)</math>.</li> <li><math>A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]</math> avec <math>M = \text{PPCM}(A, B)</math>.</li> </ul> <p><b>Théorème III.3 (Bezout)</b> Deux polynômes <math>A</math> et <math>B</math> sont premiers entre eux si et seulement si il existe <math>U, V</math> dans <math>\mathbb{K}[X]</math> tels que <math>AU + BV = 1</math>.</p> <p><b>Théorème III.4 (Gauss)</b> Soient <math>A, B, C \in \mathbb{K}[X]</math>; si <math>A</math> divise <math>BC</math> en étant premier avec <math>C</math>, alors <math>A</math> divise <math>B</math>.</p> <p style="text-align: right;">(18)</p>	<p>Des dizaines de propriétés arithmétiques, comme dans <math>\mathbb{Z}</math>, en découlent. En voici deux autres :</p> <p><b>Proposition III.2 (Euclide)</b> Si <math>A</math> est premier avec <math>B</math> et avec <math>C</math>, alors il est premier avec <math>BC</math>.</p> <p><b>Proposition III.3</b> Si <math>A</math> et <math>B</math> sont premiers entre eux et divisent tous deux <math>C</math>, alors <math>AB</math> divise <math>C</math>.</p> <p><b>Remarque III.1</b> D'après le Théorème de D'Alembert-Gauss, les facteurs irréductibles sont :</p> <ul style="list-style-type: none"> <li>dans <math>\mathbb{C}[X]</math>, les polynômes de degré 1.</li> <li><math>\mathbb{R}[X]</math>, les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.</li> </ul> <p style="text-align: right;">(19)</p>
<p><b>IV Fonction polynômiale</b></p> <p><b>IV.1 Rappels</b></p> <p><b>Racine d'un polynômes</b></p> <ul style="list-style-type: none"> <li>Soit <math>P \in \mathbb{K}[X]</math>, <math>\alpha \in \mathbb{K}</math> est racine de <math>P</math> si <math>P(\alpha) = 0</math>.</li> </ul> <p><b>Proposition IV.1</b> <math>\alpha</math> est racine de <math>P</math> si et seulement si <math>(X - \alpha)</math> divise <math>P</math>.</p> <ul style="list-style-type: none"> <li>On dit que <math>\alpha</math> est racine de <math>P</math> de multiplicité <math>\mu \in \mathbb{N}^*</math>, si <math>(X - \alpha)^\mu</math> divise <math>P</math> et <math>(X - \alpha)^{\mu+1}</math> ne divise pas <math>P</math>.</li> <li>Si <math>P(\alpha) \neq 0</math>, on dit que <math>\alpha</math> est de multiplicité 0.</li> </ul> <p style="text-align: right;">(20)</p>	<p><b>Formules de Taylor</b></p> <p>Soient <math>P \in \mathbb{K}[X]</math>, <math>n = \deg(P)</math> et <math>\alpha \in \mathbb{K}</math>. Les formules suivantes sont équivalentes et s'appellent formule de Taylor :</p> $P(X) = \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k \quad \text{(IV.1)}$ $P(X + \alpha) = \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} X^k \quad \text{(IV.2)}$ $P(X) = \sum_{k=0}^n \frac{\alpha^k}{k!} P^{(k)}(X) \quad \text{(IV.3)}$ <p style="text-align: right;">(21)</p>

<p>une application de ces formules est la caractérisation suivante de la multiplicité :</p> <p><b>Proposition IV.2</b> <math>P \in \mathbb{K}[X]</math>, <math>\mu \in \mathbb{N}^*</math> et <math>\alpha \in \mathbb{K}</math>. <math>\alpha</math> est racine de <math>P</math> de multiplicité <math>\mu</math> si et seulement si</p> $P(\alpha) = P'(\alpha) = \dots = P^{(\mu-1)}(\alpha) = 0 \text{ et } P^{(\mu)}(\alpha) \neq 0.$ <p><b>Relations entre coefficients et racines</b></p> <p>Le principale résultat généralise les relations :</p> $x_1 + x_2 = -\frac{a_1}{a_2} \text{ et } x_1 x_2 = \frac{a_0}{a_2}$ <p style="text-align: right;">(22)</p>	<p>si <math>P = a_2 X^2 + a_1 X + a_0</math> (avec <math>a_2 \neq 0</math>) admettant les deux racines <math>x_1</math> et <math>x_2</math> (non nécessairement distinctes).</p> <p><b>Proposition IV.3</b> Soit <math>P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]</math>, de degré <math>n</math>, admettant les racines <math>x_i</math>, <math>1 \leq i \leq n</math> (non nécessairement distinctes), alors</p> $\frac{a_{n-k}}{a_n} = (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}.$ <p style="text-align: right;">(Formules de Newton)</p> <p>pour tout <math>k \in [1, n]</math>.</p> <p style="text-align: right;">(23)</p>
<p><b>IV.2 Polynôme annulateur</b></p> <p>Soit <math>\mathcal{A}</math> une <math>\mathbb{K}</math>-algèbre, pour tout <math>u \in \mathcal{A}</math>, on pose</p> $u^0 = 1_{\mathcal{A}}, u^1 = u \text{ et } \forall n \in \mathbb{N} : u^{n+1} = u \times u^n$ <p>Et l’application <math>\mathcal{A} \rightarrow \mathcal{A}, u \mapsto P(u) := \sum_{k=0}^n a_k u^k</math> est appelée fonction polynômiale dans <math>\mathcal{A}</math></p> <p><b>Proposition IV.4</b> Pour tout <math>u \in \mathcal{A}</math>, l’application <math>\mathbb{K}[X] \rightarrow \mathcal{A}, P \mapsto P(u)</math> est un morphisme d’algèbre :</p> $\forall P, Q \in \mathbb{K}[X], \forall \lambda \in \mathbb{K} : (P + \lambda Q)(u) = P(u) + \lambda Q(u)$ $(P \times Q)(u) = P(u)Q(u)$ <p style="text-align: right;">(24)</p>	<p>et de manière évidente <math>(P \circ Q)(u) = P(Q(u))</math>. Son image est noté <math>\mathbb{K}[u]</math>.</p> <p><b>Théorème IV.1</b> Pour tout <math>u \in \mathcal{A}</math>, le noyau</p> $\{P \in \mathbb{K}[X] \mid P(u) = 0\}$ <p>du morphisme d’algèbre <math>\mathbb{K}[X] \rightarrow \mathcal{A}, P \mapsto P(u)</math> est un idéal de <math>\mathcal{A}</math>, c’est un idéal principal, donc il existe <math>A \in \mathbb{K}[X]</math> tel que</p> $\{P \in \mathbb{K}[X] \mid P(u) = 0\} = \mathbb{K}[X] A.$ <p><b>Preuve:</b> facile</p> <p style="text-align: right;">(25)</p>
<p><b>IV.3 Polynôme minimal</b></p> <p><b>Définition IV.1</b> Si <math>\{P \in \mathbb{K}[X] \mid P(u) = 0\} \neq \{0\}</math>, l’unique polynôme <b>unitaire</b> <math>A</math> tel que <math>\{P \in \mathbb{K}[X] \mid P(u) = 0\} = \mathbb{K}[X] A</math> est appelé polynôme minimal de <math>u</math>. On le notera <math>\pi_u</math>. C’est le polynôme de <b>degré minimal</b> dans <math>\mathbb{K}[u] \setminus \{0\}</math>.</p> <p><b>Exemples</b></p> <ol style="list-style-type: none"> <li>(1) Si <math>a \in \mathbb{K}</math> (<math>\mathcal{A} = \mathbb{K}</math>), <math>\pi_a = (X - a)</math>.</li> <li>(2) Dans <math>\mathbb{C}</math> (comme <math>\mathbb{R}</math>-algèbre), <math>\pi_i = X^2 + 1</math>.</li> <li>(3) Dans <math>\mathcal{M}_n(\mathbb{K})</math>, <math>\pi_{\lambda I_n} = X - \lambda</math>. Si <math>N \in \mathcal{M}_n(\mathbb{K})</math> est nilpotente d’indice <math>p</math> alors <math>\pi_N = X^p</math>.</li> </ol> <p style="text-align: right;">(26)</p>	<p>(4) Dans <math>\mathcal{L}(E)</math> (<math>E</math> un <math>\mathbb{K}</math>-ev), si <math>u</math> est un projecteur (respectivement symétrie), <math>\pi_u = X^2 - X</math> (resp <math>X^2 - 1</math>).</p> <p><b>Théorème IV.2</b> <math>u \in \mathcal{A}</math> admet un polynôme annulateur non nul si et seulement si <math>\mathbb{K}[a]</math> est de dimension finie, auquel cas <math>\dim \mathbb{K}[a] = \deg \pi_a</math>.</p> <p><b>Preuve:</b> Une base de <math>\mathbb{K}[a]</math> est <math>(1, u, \dots, u^{p-1})</math> où <math>p = \deg \pi_a</math>.</p> <p style="text-align: right;">(27)</p>