UFR MATHÉMATIQUES
Université Clermont Auvergne

Licence de mathématiques

troisième année

Anneaux et applications

Notes de cours de François DUMAS - année 2020-2021

version du 6 juillet 2020

Ces notes correspondent au programme d'une unité d'enseignement de second semestre de la troisième année de la licence de mathématiques. Elles ne constituent pas un cours d'algèbre autonome et complet sur les notions présentées, mais s'insèrent entre le contenu d'enseignements préalables de licence et d'enseignements ultérieurs pour le master. Les prérequis essentiels concernent bien sûr le contenu de l'unité d'enseignement de théorie des groupes du premier semestre de L3, mais aussi tout ce qui a été vu en L1 et L2 sur l'arithmétique élémentaire dans $\mathbb{Z}$ et sur les polynômes.

Le mode de rédaction n'est pas celui d'un traité, mais de simples notes destinées à servir de support au travail personnel des étudiants, à compléter évidemment par des exercices et des problèmes.

Les quatre premiers chapitres présentent les notions essentielles sur la structure d'anneau. Les chapitres 5 et 6 sont axés sur les applications arithmétiques, en mettant en avant le caractère général et efficace du langage des idéaux. Le chapitre 7 concerne des applications à l'algèbre linéaire.

Dans chaque chapitre, les premiers paragraphes contiennent les concepts et résultats principaux les plus importants, situés au cœur du programme et à connaître absolument ; des paragraphes de compléments présentent des prolongements et développement intéressants qui pourront être traités en cours, en travaux dirigés ou à titre personnel en fonction du temps et du déroulement du semestre.

Je remercie Nicolas Billerey pour sa relecture attentive de ces notes. Il subsiste probablement des coquilles ou des erreurs. Merci de m'en faire part.

Francois.Dumas@uca.fr

0 – Table des matières

1 – Anneaux, sous-anneaux, morphismes d'anneaux

1.1 Notion d'anneau

1.1.1 Définitions. Un *anneau* est un ensemble muni de deux lois de composition internes, l'une notée comme une addition et l'autre comme une multiplication, vérifiant les propriétés:

(1) A est un groupe abélien pour l'addition (on note 0 son élément neutre),

(2) la multiplication est associative, c'est-à-dire :

$$x(yz) = (xy)z \quad \text{pour tous } x, y, z \in A,$$

(3) la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire :

$$x(y+z) = xy + xz \quad \text{et} \quad (x+y)z = xz + yz \quad \text{pour tous } x, y, z \in A.$$

On dit que l'anneau A est *commutatif* si de plus la multiplication est commutative, c'est-à-dire :

$$xy = yx \quad \text{pour tous } x, y \in A.$$

On dit que A est *unitaire* si de plus la multiplication admet un élément neutre 1 :

$$x.1 = 1.x = x \quad \text{pour tout } x \in A.$$

► **Remarque.** Dans tout anneau unitaire A, on a : $x.0 = 0.x = 0$ pour tout $x \in A$.

Il suffit pour le montrer d'observer que $x = x.1 = x.(1+0) = x.1 + x.0 = x + x.0$, d'où $x.0 = x - x = 0$, et on obtient de même $0.x = 0$ en partant de $x = 1.x = (1+0).x$.

1.1.2 Premiers exemples

(a) L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

(b) L'ensemble des matrices carrées d'ordre $n \geq 2$ à coefficients réels est un anneau non commutatif (pour le produit matriciel) unitaire (de neutre multiplicatif la matrice identité). Il en est de même de l'anneau des endomorphismes d'un espace vectoriel (pour la loi $\circ$).

(c) L'anneau nul (ou anneau trivial) est l'anneau $\{0\}$ formé d'un unique élément.

(d) Pour tout intervalle I de $\mathbb{R}$, l'ensemble $\mathcal{F}(I, \mathbb{R})$ des applications de I dans $\mathbb{R}$ est un anneau commutatif (la multiplication étant le produit des fonctions défini par $(fg)(x) = f(x)g(x)$ pour tout $x \in I$) unitaire (de neutre multiplicatif la fonction constante égale à 1). Il en est de même pour l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites de réels.

1.1.3 Exemple de $\mathbb{Z}/n\mathbb{Z}$.

Fixons un entier $n \geq 2$.

Considérons le groupe additif $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Rappelons que l'addition est définie par :

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{pour tous } \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$

On a vu que cette définition est indépendante des représentants choisis, et que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est abélien. On définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ à partir de celle de $\mathbb{Z}$ en posant :

$$\overline{x}\ \overline{y} = \overline{xy} \quad \text{pour tous } \overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}.$$

Cette multiplication est bien définie, indépendamment des représentants choisis.

En effet, si $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, alors $x' = x + nu$ et $y' = y + nv$ pour deux entiers $u, v \in \mathbb{Z}$, de sorte que $x'y' = xy + n(uy + vx + nuv)$, d'où $\overline{x'y'} = \overline{xy}$.

Il est immédiat de vérifier que $\mathbb{Z}/n\mathbb{Z}$ satisfait les conditions (2) et (3) de 1.1.1, que $\overline{1}$ est neutre pour la multiplication, et que la multiplication est commutative. On conclut que :

$\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire.

1.1.4 Exemple des anneaux de polynômes. On fixe un anneau commutatif unitaire A.

Notons (provisoirement) $B = A^{(\mathbb{N})}$ l'ensemble des suites d'éléments de A qui sont "à support fini" ce qui signifie que tous les termes sont nuls sauf un nombre fini d'entre eux.

On note $0_B = (0_A, 0_A, \ldots)$. Pour tout élément $f = (a_n)_{n\in\mathbb{N}}$ de B distinct de 0_B, on appelle degré de f le plus grand des entiers $n \in \mathbb{N}$ tels que $a_n \neq 0$. On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ dans B,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad fg = (c_n)_{n\in\mathbb{N}}, \text{ avec } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

On peut montrer (vérification technique et fastidieuse, mais élémentaire) que, pour ces opérations, B est un anneau commutatif unitaire, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)_{n\in\mathbb{N}}$ en posant $\alpha f = (\alpha a_n)_{n\in\mathbb{N}}$. A noter que le produit externe αf n'est autre que le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore α l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B, ce qui permet d'identifier A à un sous-ensemble de B. En particulier $0_B = 0_A$ et $1_B = 1_A$.

En posant $e_i = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, 0_A, \ldots)$, avec 1_A en $(i+1)$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n\in\mathbb{N}} a_n e_n$ avec les $a_n \in A$ nuls sauf un nombre fini d'entre eux (de sorte que la somme est finie). Il est clair que $e_n e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$. On note traditionnellement $X = e_1$ et $B = A[X]$, et l'on retrouve les notations usuellement utilisées pour désigner les polynômes.

On retiendra que:

(a) Pour tout anneau commutatif unitaire A, les polynômes en une indéterminée à coefficients dans A forment un anneau commutatif unitaire, noté $A[X]$. Le neutre pour l'addition est 0_A. Le neutre pour la multiplication est 1_A.

(b) Pour tout élément non nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'éléments de A, appelés les *coefficients* de P tels que :

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{et} \quad a_n \neq 0.$$

L'entier n est appelé le *degré* de P, noté $\deg P$. L'élément non nul a_n de A est appelé le *coefficient dominant* de P, noté $\mathrm{cd}(P)$. L'élément a_0 est appelé le *terme constant* de P. Par convention, un polynôme est nul si et seulement si tous ses coefficients sont nuls, et l'on pose $\deg 0 = -\infty$ et $\mathrm{cd}(0) = 0$.

(c) Deux polynômes non nuls $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$ sont égaux si et seulement si $n = m$ et $a_i = b_i$ pour tout $0 \leq i \leq n$.

(d) Si $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$, on a : $\quad P+Q = \sum_{i=0}^{\max(n,m)} (a_i+b_i) X^i$ et $PQ = \sum_{i=0}^{n+m} (\sum_{j=0}^{i} a_j b_{i-j}) X^i$, avec la convention de notation $a_i = 0$ si $i > n$ et $b_i = 0$ si $i > m$.

Sous forme développée explicite, la formule du produit est donc:

$PQ = (a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_1 X + a_0)(b_m X^m + b_{m-1} X^{m-1} + b_{m-2} X^{m-2} + \cdots + b_1 X + b_0) =$
$a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + (a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m) X^{n+m-2} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0.$

(e) On en déduit que, pour tous P et Q dans $A[X]$, on a:

$$\deg(P + Q) \leq \max(\deg P, \deg Q) \quad \text{et} \quad \deg(PQ) \leq \deg P + \deg Q.$$

1.2 Sous-anneau

1.2.1 Définitions. Soit A un anneau. On appelle *sous-anneau* de A toute partie B de A qui vérifie les deux conditions suivantes :

(1) B est un sous-groupe du groupe additif A,

(2) B est stable par la multiplication de A, c'est-à-dire que l'on a :

$$xy \in B \quad \text{quels que soient } x \in B \text{ et } y \in B.$$

Si A est unitaire, on appelle *sous-anneau unitaire* de A tout sous-anneau de A qui contient 1_A.

1.2.2 Remarques

(a) Si B est un sous-anneau de A, alors B est lui-même un anneau (pour les lois déduites de celles de A par restriction à B). De fait, dans la pratique, pour montrer qu'un ensemble donné est un anneau, on cherche souvent à montrer que c'est un sous-anneau d'un anneau déjà connu.

(b) Si B est un sous-anneau unitaire non trivial d'un anneau unitaire A, alors B est lui-même un anneau unitaire, et l'on a $1_B = 1_A$.

(c) Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.

(d) Dans la pratique, pour montrer qu'un sous-ensemble non vide B d'un anneau A est un sous-anneau de A, il suffit de vérifier que:

$$\text{pour tous } x \in B \text{ et } y \in B, \text{ on a } \quad x - y \in B \quad \text{et} \quad xy \in B.$$

Pour montrer qu'un sous-ensemble B d'un anneau unitaire A est un sous-anneau unitaire de A, il suffit de vérifier que:

$$(\ 1_A \in B\ ) \quad \text{et} \quad (\ \text{pour tous } x \in B \text{ et } y \in B, \text{ on a } \ x - y \in B \ \text{ et } \ xy \in B\ ).$$

1.2.3 Premiers exemples

(a) Si A est un anneau, alors $\{0\}$ et A lui-même sont des sous-anneaux de A.

(b) Tout anneau unitaire A est un sous-anneau unitaire de $A[X]$ (le produit dans $A[X]$ de deux polynômes réduits à leur terme constant est égal à leur produit dans l'anneau A).

(c) $\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Q}$ (et de $\mathbb{R}$, et de $\mathbb{C}$). Pour tout $n \geq 2$, l'ensemble $n\mathbb{Z} = \{nx\,;\, x \in \mathbb{Z}\}$ est un sous-anneau non unitaire de $\mathbb{Z}$.

(d) Dans $\mathcal{F}(I, \mathbb{R})$ les fonctions continues sur I forment un sous-anneau unitaire.

1.2.4 Exemple des entiers de Gauss. On appelle entier de Gauss tout nombre complexe dont la partie réelle et la partie imaginaire sont des entiers. On note $\mathbb{Z}[i]$ leur ensemble:

$$\mathbb{Z}[i] = \{a + ib\ ;\ a, b \in \mathbb{Z}\}.$$

On a : $\mathbb{Z}[i]$ *est un anneau commutatif unitaire, contenant* $\mathbb{Z}$ *comme sous-anneau.*

En effet, quels que soient $x = a+ib$ et $x' = c+id$ avec $a, b, c, d \in \mathbb{Z}$, les complexes $x-x' = (a-c)+i(b-d)$ et $xx' = (ac - bd) + i(ad + bc)$ ont des parties réelles et imaginaires dans $\mathbb{Z}$, donc appartiennent à $\mathbb{Z}[i]$. Ceci prouve que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ (donc en particulier un anneau commutatif). Il est clair que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[i]$, et en particulier $1 \in \mathbb{Z}[i]$. □

L'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a+ib) = (a+ib)(a-ib) = a^2+b^2$ jouera dans l'étude de l'anneau $\mathbb{Z}[i]$ un rôle important. Bornons-nous pour l'instant à observer que, puisque $N(x) = x\overline{x} = |x|^2$ pour tout $x \in \mathbb{Z}[i]$, on a clairement $N(xx') = N(x)N(x')$ pour tous $x, x' \in \mathbb{Z}[i]$.

▶ **Généralisation.**
Soit d un entier non nul, que l'on suppose sans facteurs carrés (c'est-à-dire que d n'est divisible par aucun carré d'entier hormis 1). On désigne par ω une racine carrée dans $\mathbb{C}$ de d. On vérifie (la preuve est laissée en exercice):

$\mathbb{Z}[\omega] = \{a+\omega b\ ;\ a, b \in \mathbb{Z}\}$ *est un anneau commutatif unitaire, contenant* $\mathbb{Z}$ *comme sous-anneau,*

et que l'application $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ définie par $N(a+\omega b) = (a+\omega b)(a-\omega b) = a^2 - db^2$ vérifie $N(xx') = N(x)N(x')$ pour tous $x, x' \in \mathbb{Z}[\omega]$.

1.3 Morphisme d'anneaux

Définitions. Soient A et B deux anneaux commutatifs unitaires. On appelle *morphisme d'anneaux unitaires* de A dans B toute application $f : A \to B$ vérifiant les trois propriétés suivantes:

$$[\ f(x+y) = f(x) + f(y)\ \text{ et }\ f(xy) = f(x)f(y)\ \text{ pour tous } x, y \in A\ ]\ \text{ et }\ [\ f(1_A) = 1_B\ ].$$

Il résulte de la première condition qu'un morphisme d'anneaux unitaires est a fortiori un morphisme de groupes additifs. Les propriétés générales des morphismes d'anneaux unitaires sont de fait analogues à celles qui ont été démontrées pour les morphismes de groupes. C'est pourquoi nous synthétisons ci-dessous les plus usuelles en laissant au lecteur le soin d'adapter les démonstrations.

▶ **Propriétés**

(a) Si $f : A \to B$ est un morphisme d'anneaux unitaires, alors l'image directe par f de tout sous-anneau unitaire de A est un sous-anneau unitaire de B, et l'image réciproque par f de tout sous-anneau unitaire de B est un sous-anneau unitaire de A.

(b) Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux unitaires, alors $g \circ f : A \to C$ est un morphisme d'anneaux unitaires.

(c) Si $f : A \to B$ est un morphisme d'anneaux unitaires bijectif, alors sa bijection réciproque $f^{-1} : B \to A$ est un morphisme d'anneaux unitaires; on dit dans ce cas que f est un *isomorphisme*, et que les deux anneaux A et B sont *isomorphes*.

1.4 Anneaux produits

1.4.1 Proposition et définition. *Soient A_1 et A_2 deux anneaux commutatifs unitaires.*

(i) *Le produit cartésien $A_1 \times A_2 = \{(x_1, x_2),\ x_1 \in A_1,\ x_2 \in A_2\}$ est un anneau commutatif unitaire pour les lois définies par:*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)\ \text{ et }\ (x_1, x_2).(y_1, y_2) = (x_1y_1, x_2y_2),$$

pour tous $x_1, y_1 \in A_1,\ x_2, y_2 \in A_2$, et l'on a $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$. Cet anneau est appelé le produit direct de A_1 par A_2.

(ii) *L'application $p_1 : A_1 \times A_2 \to A_1$ qui, à tout élément $(x_1, x_2) \in A_1 \times A_2$, associe sa première composante x_1, est un morphisme d'anneaux unitaires (appelé première projection).*

(iii) *L'application $p_2 : A_1 \times A_2 \to A_2$ qui, à tout élément $(x_1, x_2) \in A_1 \times A_2$, associe sa seconde composante x_2, est un morphisme d'anneaux unitaires (appelé seconde projection).*

Preuve. Simple vérification, laissée au lecteur. □

▶ **Remarques.**

(a) Le produit direct $A_1 \times A_2$ est isomorphe au produit direct $A_2 \times A_1$.

(b) On définit de même de façon évidente le produit direct d'un nombre fini quelconque d'anneaux.

1.4.2 Proposition (dit théorème des restes chinois). *Soient deux entiers $n \geq 2$ et $m \geq 2$. L'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/nm\mathbb{Z}$ si et seulement si n et m sont premiers entre eux.*

Preuve. Il a été démontré dans le cours de théorie des groupes que, si n et m sont premiers entre eux, l'application $\overline{x} \mapsto (\widetilde{x}, \widehat{x})$ réalise un isomorphisme de groupes de $\mathbb{Z}/nm\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Il est clair, par définition même des multiplications dans ces différents anneaux, que c'est aussi un isomorphisme d'anneaux unitaires. La réciproque est évidente. □

CONVENTION.

Bien que les anneaux non commutatifs interviennent dans de nombreuses situations variées et intéressantes en mathématiques, on se limitera dans la suite de ce cours, comme le prévoient les programmes, à l'étude des anneaux commutatifs et unitaires.

C'est pourquoi, dans les pages qui suivent, même lorsqu'on ne le précise pas dans les énoncés, tous les anneaux sont supposés commutatifs, unitaires, et de plus non triviaux (c'est-à-dire distincts de l'anneau nul).

2 – Eléments inversibles d'un anneau, corps, intégrité

2.1 Groupe des éléments inversibles

2.1.1 Définition. Soit A un anneau commutatif unitaire. On appelle *élément inversible dans A* (ou *unité* de A) tout élément $x \in A$ tel qu'il existe un élément $y \in A$ vérifiant $xy = 1$.

▶ **Remarques.**

(a) Si $x \in A$ est inversible dans A, il est facile de vérifier qu'il n'existe qu'un seul élément $y \in A$ tel que $xy = 1$. On note $y = x^{-1}$; on l'appelle l'inverse de x dans A.

(b) Les éléments 1 et -1 sont toujours inversibles dans A, avec $1^{-1} = 1$ et $(-1)^{-1} = -1$. L'élément 0 n'est jamais inversible (dès lors que l'anneau A n'est pas trivial, c'est-à-dire $1 \neq 0$) car on a $0x = 0 \neq 1$ pour tout $x \in A$.

2.1.2 Proposition et définition. *Soit A un anneau commutatif unitaire. L'ensemble des éléments de A inversibles dans A est un groupe abélien pour la multiplication, noté $U(A)$.*

On dit que $U(A)$ est le groupe des éléments inversibles de A (ou le groupe des unités de A).

Preuve. D'après la remarque (b) ci-dessus, $U(A)$ n'est pas vide, car il contient 1. Soient x et y deux éléments de $U(A)$. Il existe x' et y' dans A tels que $xx' = 1 = yy'$. Donc $(xy)(y'x') = x(yy')x' = x1x' = xx' = 1$, ce qui prouve que $xy \in U(A)$ (et que $(xy)^{-1} = y^{-1}x^{-1}$). On a ainsi vérifié que la multiplication de A se restreint en une loi de composition interne de $U(A)$. Elle est associative, commutative, et admet comme neutre 1 qui, comme on l'a observé, appartient à $U(A)$. Il reste à vérifier que tout élément $x \in U(A)$ admet un inverse dans $U(A)$, ce qui est évident puisque l'inverse $x' = x^{-1}$ d'un élément $x \in U(A)$ est lui-même dans $U(A)$, d'inverse $(x')^{-1} = x$. □

2.1.3 Exemples

(a) $U(\mathbb{Z}) = \{-1, 1\}$.

(b) $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Preuve. Reprenons les notations de 1.2.4. Soient $x = a + ib$ et $y = c + id$ avec $a, b, c, d \in \mathbb{Z}$ tels que $xy = 1$. On a alors $1 = N(xy) = N(x)N(y)$ avec $N(x), N(y) \in \mathbb{N}^*$, d'où $N(x) = N(y) = 1$ d'après l'exemple précédent. Or $N(x) = 1$ équivaut à $a^2 + b^2 = 1$ ce qui, dans $\mathbb{Z}$, se produit si et seulement si (a, b) est l'un des quatre couples $(1, 0)$, $(-1, 0)$, $(0, 1)$ ou $(0, -1)$. □

(c) Pour tout entier $n \geq 2$, $U(\mathbb{Z}/n\mathbb{Z}) = \{\ \overline{x}\ ;\ 0 \leq x \leq n-1,$ et x premier avec $n\}$.

Preuve. Soit $\overline{x}$ un élément quelconque de $\mathbb{Z}/n\mathbb{Z}$, avec $0 \leq x \leq n-1$. On a:

$$\begin{aligned}
(\ \overline{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z}\ ) &\Leftrightarrow (\text{ il existe } u \in \mathbb{Z} \text{ tel que } \overline{x}\,\overline{u} = \overline{1}\ ) \\
&\Leftrightarrow (\text{ il existe } u \in \mathbb{Z} \text{ tel que } \overline{xu - 1} = \overline{0}\ ) \\
&\Leftrightarrow (\text{ il existe } u, v \in \mathbb{Z} \text{ tels que } xu - 1 = nv\ ) \\
&\Leftrightarrow (\text{ il existe } u, v \in \mathbb{Z} \text{ tels que } xu + n(-v) = 1\ )
\end{aligned}$$

d'où le résultat par le théorème de Bézout dans $\mathbb{Z}$. □

Rappelons que, comme cela a été montré dans le cours de théorie des groupes, les éléments $\overline{x}$ tels que x est premier avec n sont aussi ceux qui engendrent le groupe additif $\mathbb{Z}/n\mathbb{Z}$. Il en résulte en particulier que :

le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est fini d'ordre $\varphi(n)$, où φ désigne l'indicatrice d'Euler.

2.2 Corps

2.2.1 Définition. On appelle *corps commutatif* (ou plus simplement corps) tout anneau commutatif unitaire dans lequel tout élément non nul est inversible.
En notant, pour tout anneau A commutatif unitaire $A^* = A \setminus \{0\}$, on a donc :

$$(\ A \text{ corps }) \ \Leftrightarrow \ (\ U(A) = A^*).$$

2.2.2 Définition. Soit K un corps. On appelle *sous-corps* de K tout sous-anneau unitaire F de K tel que l'inverse de tout élément non nul de F appartient à F.

2.2.3 Exemples

(a) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des corps; ils contiennent comme sous-anneau $\mathbb{Z}$ qui, lui, n'est pas un corps.

(b) $\mathbb{Q}(i) = \{p + qi \ ; \ p, q \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$; il contient $\mathbb{Z}[i]$ comme sous-anneau qui, lui, n'est pas un corps.

> *Preuve.* On vérifie aisément que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$; pour tout $x = p + qi \in \mathbb{Q}(i)$ non nul, son inverse x^{-1} dans $\mathbb{C}$ est égal à $\frac{p}{p^2+q^2} + \frac{-q}{p^2+q^2} i$ et appartient donc à $\mathbb{Q}(i)$. Ce qui prouve que $\mathbb{Q}(i)$ est un sous-corps de $\mathbb{C}$. Il est clair que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{Q}(i)$, et le fait que ce n'est pas un corps découle immédiatement de 2.1.3.(b). □

(c) Pour tout entier $n \geq 2$, $(\ \mathbb{Z}/n\mathbb{Z}$ est un corps $) \ \Leftrightarrow \ (\ n$ est un nombre premier $)$.

> *Preuve.* Résulte immédiatement de 2.1.3.(c). □

2.3 Intégrité

2.3.1 Définition. Soit A un anneau commutatif. On dit que A est *intègre*, ou encore que A est un *domaine d'intégrité*, lorsqu'il est non nul et vérifie la propriété suivante :

$$\text{pour tous } x, y \in A, \ (\ xy = 0\ ) \ \Leftrightarrow \ (\ x = 0 \ \text{ ou } \ y = 0\ ).$$

► Si l'on a dans un anneau intègre A une égalité de la forme $ax = bx$ où $a, b, x \in A$ avec $x \neq 0$, alors $(a - b)x = 0$, donc $a - b = 0$ puisque $x \neq 0$, et donc $a = b$. On exprime cette propriété en disant que : *dans un anneau intègre, on peut simplifier par un élément non nul.*

► Un élément x de A est appelé un *diviseur de zéro* dans A lorsque $x \neq 0$ et lorsque qu'il existe $y \neq 0$ dans A tel que $xy = 0$. Donc A est intègre si et seulement s'il n'admet pas de diviseurs de zéro.

2.3.2 Premiers exemples et contre-exemples

(a) Tout corps est un anneau intègre.

> *Preuve.* Soit K un corps. Soient $x, y \in K$ tels que $xy = 0$. Si $x \neq 0$, alors x est inversible dans K par définition d'un corps. Donc $x^{-1}xy = x^{-1}0$, c'est-à-dire $y = 0$. De même $y \neq 0$ implique $x = 0$. En résumé l'un au moins des deux facteurs x et y est nul. □

(b) Tout sous-anneau d'un anneau intègre est intègre. En particulier tout sous-anneau d'un corps est intègre. Par exemple, $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont intègres (bien que ce ne soient pas des corps).

(c) Attention: un anneau produit $A_1 \times A_2$ n'est pas intègre (même si A_1 et A_2 le sont). En effet, les éléments $(1_{A_1}, 0_{A_2})$ et $(0_{A_1}, 1_{A_2})$ sont non nuls, alors que leur produit l'est.

(d) Considérons les tables de multiplication des anneaux $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

L'anneau $\mathbb{Z}/5\mathbb{Z}$ est un corps puisque 5 est un nombre premier ; il est donc a fortiori intègre.

Au contraire, l'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car, par exemple, $\overline{2}\,.\,\overline{3} = \overline{0}$ bien que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$; a fortiori, ce n'est pas un corps.

Ces exemples sont des cas particuliers de la proposition suivante.

2.3.3 Proposition (cas des anneaux $\mathbb{Z}/n\mathbb{Z}$). *Pour tout entier $n \geq 2$, on a :*

(*l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre*) $\Leftrightarrow$ (*n est un nombre premier*) $\Leftrightarrow$ (*l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps*).

Preuve. D'après 2.2.3.(c) et 2.3.2.(a), le seul point à montrer est que $\mathbb{Z}/n\mathbb{Z}$ intègre implique n premier. Par contraposée, supposons que n n'est pas premier; il existe donc $k, m \in \mathbb{Z}$ tels que $n = km$ avec $1 < k < n$ et $1 < m < n$. On a alors $\overline{k}.\overline{m} = \overline{n} = \overline{0}$, bien que $\overline{k} \neq \overline{0}$ et $\overline{m} \neq \overline{0}$. □

2.3.4 Proposition (cas des anneaux de polynômes). *Soit A un anneau commutatif unitaire.*

(i) *Si A est intègre, alors pour tous polynômes $P, Q \in A[X]$, on a :*
$$\deg(PQ) = \deg P + \deg Q \quad \text{et} \quad \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q).$$

(ii) *$A[X]$ est intègre si et seulement si A est intègre.*

(iii) *En particulier, si K est un corps, alors l'anneau $K[X]$ est intègre.*

Preuve. Les égalités $\deg(PQ) = \deg P + \deg Q$ et $\mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q)$ sont claires si P ou Q est nul. Supposons-les tous les deux non nuls, et écrivons $P = a_nX^n + \cdots + a_1X + a_0$ et $Q = b_mX^m + \cdots + b_1X + b_0$, avec $\mathrm{cd}(P) = a_n \neq 0$ et $\mathrm{cd}(Q) = b_m \neq 0$. Alors :
$$PQ = a_nb_mX^{n+m} + (a_nb_{m-1} + a_{n-1}b_m)X^{n+m-1} + \cdots + (a_1b_0 + a_0b_1)X + a_0b_0.$$
L'intégrité de A implique $a_nb_m \neq 0$, donc $\mathrm{cd}(PQ) = a_nb_m$, d'où $\deg(PQ) = n + m$, ce qui prouve (i). Il résulte immédiatement de (i) que, si A est intègre, le produit de deux éléments non nuls de $A[X]$ est non nul, ce qui prouve que $A[X]$ est intègre. L'implication réciproque étant triviale d'après 2.3.2.(b), le point (ii) est établi. Le point (iii) en découle d'après 2.3.2.(a). □

2.3.5 Corollaire (groupe des éléments inversibles d'un anneau de polynômes). *Soit A un anneau commutatif unitaire. Si A est intègre, alors: $U(A[X]) = U(A)$.*

Preuve. L'inclusion $U(A) \subset U(A[X])$ est claire puisque A est un sous-anneau unitaire de $A[X]$. Pour la réciproque, considérons $P \in U(A[X])$. Il existe donc $Q \in A[X]$ tel que $PQ = 1$. Ces deux polynômes sont nécessairement non nuls, donc il résulte du point (i) de la proposition précédente que $\deg P + \deg Q = 0$. On en tire $\deg P = \deg Q = 0$, c'est-à-dire $P \in A$ et $Q \in A$, et donc l'égalité $PQ = 1$ implique $P \in U(A)$ et $Q \in U(A)$. □

Remarque. Si A n'est pas intègre, $A[X]$ peut contenir des éléments inversibles de degré non-nul.

Par exemple, pour $A = \mathbb{Z}/4\mathbb{Z}$, le polynôme $\overline{2}X + \overline{1}$ est inversible dans $A[X]$, d'inverse égal à lui-même, puisque $(\overline{2}X + \overline{1})(\overline{2}X + \overline{1}) = \overline{1}$. □

Remarque. $A[X]$ n'est jamais un corps, que A soit ou non intègre.

En effet, L'élément X de $A[X]$ vérifie toujours $\deg(PX) = \deg P + 1$ pour tout $P \in A[X]$, de sorte que l'on ne peut pas avoir $PX = 1$, ce qui montre que X n'est jamais inversible. □

2.4 Corps des fractions d'un anneau intègre

2.4.1 Construction. Il existe, on l'a vu, des anneaux intègres qui ne sont pas des corps. Le but de ce qui suit est de montrer que, néanmoins, on peut construire de façon canonique pour tout anneau intègre A un corps K qui le contient, et qui est (en un sens que l'on précisera) le plus petit corps qui le contient. Evidemment, la question ne se pose pas pour des anneaux non intègres, d'après les remarques 2.3.2.(a) et 2.3.2.(b).

Fixons A un anneau commutatif unitaire intègre. Posons $A^* = A \setminus \{0\}$. On définit dans $A \times A^*$ la relation $\sim$ par :

$$(a,b) \sim (c,d) \;\Leftrightarrow\; ad = bc.$$

► Etape 1. – *la relation $\sim$ est une relation d'équivalence dans $A \times A^*$.*

Preuve. La réflexivité et la symétrie sont évidentes. Pour la transitivité, considérons trois couples (a,b), (c,d) et (e,f) dans $A \times A^*$. Supposons que $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$. On a donc: $ad = bc$ et $cf = de$. Il vient $adf = bcf = bde$, et comme $d \neq 0$, l'intégrité de A implique $af = be$, d'où $(a,b) \sim (e,f)$. □

Pour tout couple $(a,b) \in A \times A^*$, on note $\frac{a}{b}$ la classe d'équivalence de (a,b) pour la relation $\sim$:

$$\tfrac{a}{b} = \{(c,d) \in A \times A^* \,;\, (c,d) \sim (a,b)\} = \{(c,d) \in A \times A^* \,;\, ad = bc\}.$$

Une telle classe s'appelle une fraction. On note $K = (A \times A^*)/\sim$ l'ensemble quotient de $A \times A^*$ par la relation $\sim$, c'est-à-dire l'ensemble des fractions. Tout couple (c,d) appartenant à $\frac{a}{b}$ s'appelle un représentant de la fraction $\frac{a}{b}$. On a :

$$(\ \tfrac{a}{b} = \tfrac{c}{d} \text{ dans } K\ ) \;\Leftrightarrow\; (\ (a,b) \sim (c,d) \text{ dans } A \times A^*\ ) \;\Leftrightarrow\; (\ ad = bc \text{ dans } A\ ).$$

► Etape 2. – *L'application $\phi : A \to K$ qui, à un élément $a \in A$ associe la fraction $\phi(a) = \frac{a}{1}$, est injective, et est appelée injection canonique de A dans K.*

Preuve. Soient $a, c \in A$ tels que $\phi(a) = \phi(c)$. Alors $\frac{a}{1} = \frac{c}{1}$, d'où $a.1 = 1.c$, donc $a = c$. □

On convient d'identifier A avec le sous-ensemble $\phi(A)$ de K, qui lui est équipotent. Via cette identification, A est un sous-ensemble de K, et on pose $a = \frac{a}{1}$, pour tout $a \in A$. En d'autres termes :

$$\text{quel que soit } a \in A, \text{ on a: } \; a = \tfrac{a}{1} = \{(c,d) \in A \times A^* \,;\, c = ad\} = \tfrac{ad}{d} \;\text{ pour tout } d \in A^*.$$

En particulier: $0 = \frac{0}{1} = \frac{0}{b}$ pour tout $b \in A^*$ et $1 = \frac{1}{1} = \frac{b}{b}$ pour tout $b \in A^*$.

► Etape 3. – *Les lois de composition internes dans K définies par :*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{et} \qquad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

sont bien définies (indépendamment des représentants choisis), munissent K d'une structure d'anneau commutatif unitaire, et prolongent celles de A (ce qui signifie que l'injection canonique est un morphisme d'anneaux unitaires, ou encore que A peut être considéré, en l'identifiant avec son image par ϕ, comme un sous-anneau unitaire de K).

Preuve. Supposons que $\frac{a}{b} = \frac{a'}{b'}$ et $\frac{c}{d} = \frac{c'}{d'}$. Un calcul évident montre que $ab' = a'b$ et $cd' = c'd$ impliquent:

– d'une part: $(ad+bc)b'd' = (a'd' + b'c')bd$, et donc $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$,

– d'autre part: $(ac)(b'd') = (a'c')(bd)$, et donc $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Ce qui prouve que les deux lois sont bien définies. Qu'elles satisfont alors tous les axiomes de la structure d'anneau commutatif unitaire (avec $0 = \frac{0}{1}$ pour neutre additif et $1 = \frac{1}{1}$ pour neutre multiplicatif) est une simple vérification laissée au lecteur. Enfin quels que soient deux éléments $a, c \in A$, on a:

$$\phi(a+c) = \tfrac{a+c}{1} = \tfrac{a}{1} + \tfrac{c}{1} = \phi(a) + \phi(c) \quad \text{et} \quad \phi(ac) = \tfrac{ac}{1} = \tfrac{a}{1}.\tfrac{c}{1} = \phi(a).\phi(c),$$

ce qui achève la preuve. □

▶ Etape 4. – *Tout élément non nul de K est inversible dans K. Plus précisément, tout élément $\frac{a}{b} \in K$ avec $(a,b) \in A^* \times A^*$ admet $\frac{b}{a}$ pour inverse.*

Preuve. Evident puisque $\frac{a}{b}.\frac{b}{a} = \frac{ab}{ba} = 1$. □

En particulier, tout élément non nul $a \in A$ admet dans K l'inverse $\frac{1}{a}$.

On déduit de cette construction et des vérifications faites aux différentes étapes le théorème suivant.

2.4.2 Théorème. *Soit A un anneau commutatif unitaire intègre.*

(i) *L'ensemble $K = (A \times A^*)/\sim$ des fractions sur A, muni des lois construites ci-dessus, est un corps commutatif, qui contient A comme sous-anneau unitaire.*

(ii) *Si K' est un sous-corps de K contenant A comme sous-anneau, alors $K' = K$.*

Preuve. Le (i) a été montré en 2.4.1. Pour le (ii), supposons que $A \subseteq K' \subseteq K$ avec K' un corps. Soit $x \in K$. Par définition, il existe $a \in A$ et $b \in A^*$ tel que $x = \frac{a}{b} = a.\frac{1}{b}$. On a $b \in A$ donc $b \in K'$, avec $b \neq 0$; comme l'inverse de b dans K est $\frac{1}{b} \in K$, et que cet inverse doit appartenir à K' puisque K' est un sous-corps, on a $\frac{1}{b} \in K'$. Par ailleurs $a \in A$ donc $a \in K'$. Le sous-corps K' est stable par produit, donc $a.\frac{1}{b} \in K'$, c'est-à-dire $\frac{a}{b} = x \in K'$. Cela prouve que $K \subseteq K'$, donc $K = K'$. □

Le point (ii) exprime que le corps de fractions est "le plus petit corps" contenant A, ce que précise encore le corollaire suivant qui établit que tout corps contenant un sous-anneau contient aussi (à identification près) le corps de fractions de celui-ci.

2.4.3 Corollaire. *Soit L un corps commutatif. Soient A un sous-anneau unitaire de L et K son corps de fractions. Alors il existe un morphisme d'anneaux unitaires injectif de K dans L.*

Preuve. On considère l'application $f : K \to L$ qui, à un élément $\frac{a}{b}$ de K, associe $a.b^{-1}$, produit dans L de a par l'inverse de b. Si $a, b, c, d \in A$ avec $b \neq 0$ et $d \neq 0$ sont tels que $\frac{a}{b} = \frac{c}{d}$, alors on a $ad = bc$ dans A donc dans L, d'où $a.b^{-1} = c.d^{-1}$, ce qui prouve que l'application f est bien définie (indépendamment des représentants choisis). Il est facile de vérifier que f est alors un morphisme d'anneaux unitaires, et que son noyau est nul. □

2.4.4 Exemples

(a) Le corps de fractions de l'anneau intègre $\mathbb{Z}$ est appelé *corps des rationnels* et est noté $\mathbb{Q}$.

(b) Le corps de fractions de l'anneau intègre de polynômes $\mathbb{R}[X]$, noté $\mathbb{R}(X)$, a déjà été rencontré lors de l'étude des fonctions fractions rationnelles.

D'une façon générale, pour tout corps K, le corps de fractions de l'anneau intègre $K[X]$ est appelé *corps des fractions rationnelles à coefficients dans K*, noté $K(X)$. Ses éléments sont de la forme :

$$F(X) = \frac{P(X)}{Q(X)} \text{ avec } P, Q \in K[X],\ Q \neq 0.$$

▶ **Remarque.** Il est facile de vérifier (via l'identification du corollaire 2.4.3) que, pour tout anneau intègre A de corps de fractions K, le corps de fractions de l'anneau intègre $A[X]$ est égal à $K(X)$. C'est pourquoi on peut parler aussi du corps des fractions rationnelles à coefficients dans A. Ses éléments sont de la forme $F(X) = \frac{P(X)}{Q(X)}$ avec $P, Q \in A[X]$, $Q \neq 0$. □

(c) Montrer à titre d'exercice que le corps de fractions de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est le corps $\mathbb{Q}(i) = \{p + qi\,;\, p \in \mathbb{Q}, q \in \mathbb{Q}\}$ introduit en 2.2.3.(b).

2.5 *Complément* : inverses à droite et à gauche

Bien que l'intégralité de ce que l'on fera dans ce cours concerne des anneaux commutatif, il peut être utile d'avoir réfléchi aux difficultés que peut poser la notion d'inverse dans un anneau non-commutatif, ne serait-ce que pour les plus usuels d'entre eux (anneaux d'endomorphismes ou de matrices).

2.5.1 Définitions Soit a un élément d'un anneau unitaire A non nécessairement commutatif.
On dit que a admet un *inverse à droite* dans A lorsqu'il existe un élément $b \in A$ tel que $ab = 1$.
On dit que a admet un *inverse à gauche* dans A lorsqu'il existe un élément $c \in A$ tel que $ca = 1$.

2.5.2 Proposition *Soit a un élément d'un anneau unitaire A non nécessairement commutatif. Si a admet dans A un inverse à droite b et un inverse à gauche c, alors ils sont uniques et $b = c$.*

Preuve. On a $ab = 1$, donc $cab = c$; mais $ca = 1$, d'où $b = c$.

S'il existe un autre élément $b' \in A$ tel que $ab' = 1$, alors on a de la même façon $cab' = c$ puis $b' = c$, d'où $b = b'$. L'unicité de l'inverse à gauche se montre de façon identique. □

2.5.3 Remarque Dès lors que A n'est pas commutatif, un élément peut admettre un inverse à droite mais pas d'inverse à gauche.

Exemple. On considère l'espace vectoriel $E = \mathbb{R}[X]$ des polynômes à coefficients réels, et l'anneau non commutatif $A = \operatorname{End} E$ des endomorphismes de E. Considérons l'application $f : E \to E$ qui, à tout polynôme $P \in E$ associe le polynôme dérivé $f(P) = P'$. Il est clair que $f \in A$.

Considérons l'application $h : E \to E$ qui, à un polynôme quelconque $Q = \sum_{i=0}^{n} \alpha_i X^i$ associe $h(Q) = \sum_{i=0}^{n} \frac{1}{i+1} \alpha_i X^{i+1}$. Il est clair que h est un endomorphisme de E et que $f(h(Q)) = Q$ pour tout $Q \in E$. En d'autres termes $f \circ h = \mathrm{id}_E$, ce qui signifie que h est un inverse de f à droite dans A.

Si f admettait un inverse à gauche $g \in A$, on aurait $g \circ f = \mathrm{id}_E$, donc f serait injective, ce qui n'est clairement pas le cas puisque $\operatorname{Ker} f = \mathbb{R}$. Donc f n'admet pas d'inverse à gauche dans A.

3 – Idéaux d'un anneau

3.1 Notion d'idéal

3.1.1 Définition. Soit A un anneau commutatif unitaire. On appelle *idéal* de A toute partie I de A qui vérifie les deux conditions suivantes:

(1) I est un sous-groupe du groupe additif A,

(2) pour tous $x \in I$ et $a \in A$, on a $xa \in I$.

Exemples.

(a) $\{0\}$ et A sont des idéaux de A.

(b) Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de l'anneau $\mathbb{Z}$.

(c) Dans l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions qui s'annulent en 0 est un idéal.

3.1.2 Lemme (très utile dans la pratique). *Soit A un anneau commutatif unitaire.*

(i) *si I est un idéal de A qui contient* 1, *alors $I = A$.*

(ii) *si I est un idéal de A qui contient un élément de $U(A)$, alors $I = A$.*

Preuve. Supposons $1 \in I$. Tout $a \in A$ s'écrit $a = 1.a$ donc, comme $1 \in I$, il résulte de la propriété (2) que $a \in I$. On a alors $A \subseteq I$, donc $A = I$, ce qui prouve (i). Supposons maintenant que I contienne un élément x inversible dans A. On a $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$, et on applique (i) pour conclure que $I = A$. □

3.1.3 Proposition. *Soient A et B des anneaux commutatifs unitaires. Soit $f : A \to B$ un morphisme d'anneaux unitaires. On a:*

(i) *Pour tout idéal J de B, l'image réciproque $f^{-1}(J)$ est un idéal de A.*

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

(iii) *Pour tout idéal I de A, l'image directe $f(I)$ est un idéal de l'anneau $f(A) = \operatorname{Im} f$; attention, ce n'est pas en général un idéal de B.*

Preuve. Sous les hypothèses de (i), $f^{-1}(J)$ est un sous-groupe additif de A comme image réciproque d'un sous-groupe additif de B par un morphisme de groupes. Soit $x \in f^{-1}(J)$ et $a \in A$. On a $f(xa) = f(x)f(a)$ avec $f(a) \in B$ et $f(x) \in J$, donc $f(xa) \in J$ puisque J est un idéal de B, c'est-à-dire $xa \in f^{-1}(J)$. Ceci prouve que $f^{-1}(J)$ est un idéal de A. On obtient (ii) en appliquant ce qui précède à $J = \{0_B\}$. Pour (iii), considérons un idéal I de A. On sait déjà que $f(I)$ est un sous-groupe additif de B. Soit $y \in f(I)$, de sorte qu'il existe $x \in I$ tel que $y = f(x)$. Pour tout élément $b \in B$ qui appartient à $\operatorname{Im} f$, il existe $a \in A$ tel que $b = f(a)$; on a alors $yb = f(a)f(x) = f(ax)$ avec $ax \in I$ puisque $x \in I$ et que I est un idéal, et donc $yb \in f(I)$. Ceci prouve que $f(I)$ est un idéal de l'anneau $\operatorname{Im} f$. □

3.1.4 Proposition. *Soit A un anneau commutatif unitaire. L'intersection de deux idéaux de A est un idéal de A. Plus généralement, l'intersection d'une famille quelconque d'idéaux de A est un idéal de A.*

Preuve. Il suffit de montrer le second point. Soit donc $(I_j)_{j \in X}$ une famille d'idéaux de A. Posons $I = \bigcap_{j \in X} I_j$ l'intersection de tous les I_j. On sait déjà que I est un sous-groupe additif en tant qu'intersection d'une famille de sous-groupes. Soient $x \in I$ et $a \in A$. On a $xa \in I_j$ pour tout $j \in X$ puisque I_j est un idéal, et donc $xa \in I$. Ce qui prouve que I est un idéal de A. □

3.2 Idéal principal, anneau principal

3.2.1 Proposition et définition. *Soit A un anneau commutatif unitaire. Pour $x \in A$, on note :*

$$xA = \{xy\,;\, y \in A\} = \{z \in A\,;\, \text{il existe } y \in A \text{ tel que } z = xy\}.$$

Alors :

(i) *xA est un idéal de A, appelé l'idéal principal engendré par x ;*

(ii) *xA est le plus petit idéal de A contenant x ;*

(iii) *on a :* $(\ xA = A\ ) \Leftrightarrow (\ x \in U(A))$ et $(\ xA = \{0\}\ ) \Leftrightarrow (\ x = 0)$.

Preuve. Il est clair que xA est non vide (il contient x puisque $x = x.1$). Soient $y \in xA$ et $z \in xA$ quelconques; il existe $a, b \in A$ tels que $y = xa$ et $z = xb$, donc $y - z = x(a - b) \in xA$, ce qui prouve que xA est un sous-groupe additif. Soient $y \in xA$ et $c \in A$ quelconques; il existe $a \in A$ tel que $y = xa$, donc $yc = xac = x(ac) \in xA$. On conclut que xA est un idéal de A.

Soit I un idéal de A contenant x. Comme $x \in I$, on a $xa \in I$ pour tout $a \in A$. Donc $xA \subseteq I$, d'où (ii).

Si $xA = A$, alors $1 \in xA$, de sorte qu'il existe $y \in A$ tel que $xy = 1$, ce qui prouve $x \in U(A)$. L'implication réciproque découle de 3.1.2.(ii). La dernière équivalence est claire. □

3.2.2 Corollaire. *Soit A un anneau commutatif unitaire.*

$$(\ A \text{ est un corps}\ ) \Leftrightarrow (\ \text{les seuls idéaux de } A \text{ sont } \{0\} \text{ et } A\ ).$$

Preuve. Supposons que A est un corps. Soit I un idéal de A. Si $I \neq \{0\}$, il existe dans I un élément non nul, donc inversible dans A puisque A est un corps. On conclut avec 3.1.2.(ii) que $I = A$. Supposons réciproquement que A n'admette que $\{0\}$ et A comme idéaux. Soit $x \in A$ quelconque non nul. L'idéal xA étant alors distinct de $\{0\}$, on a nécessairement $xA = A$, d'où $x \in U(A)$ d'après 3.2.1.(iii). Ainsi tout élément non nul de A est inversible dans A: on conclut que A est un corps. □

3.2.3 Définitions. On appelle *idéal principal* d'un anneau commutatif unitaire A tout idéal I de A pour lequel il existe un élément $x \in A$ tel que $I = xA$. On appelle *anneau principal* tout anneau commutatif unitaire A qui est intègre et dans lequel tout idéal est principal.

De nombreux exemples d'anneaux principaux seront donnés plus loin. Bornons-nous ici à citer:

$\mathbb{Z}$ est un anneau principal,

ce qui découle immédiatement du lemme suivant:

3.2.4 Lemme (idéaux de $\mathbb{Z}$). *Pour tout idéal I de l'anneau $\mathbb{Z}$, il existe un unique $k \in \mathbb{N}$ tel que $I = k\mathbb{Z}$. Les seuls entiers m tels que $I = m\mathbb{Z}$ sont alors $m = k$ et $m = -k$.*

Preuve. Il a été démontré dans le cours de théorie des groupes que les seuls sous-groupes du groupe additif $\mathbb{Z}$ sont les sous-groupes $k\mathbb{Z}$ avec $k \in \mathbb{Z}$. Comme il est clair que ce sont des idéaux de l'anneau $\mathbb{Z}$, voir 3.1.1, le résultat est établi. □

3.2.5 Contre-exemple. *L'anneau $\mathbb{Z}[X]$ n'est pas principal.*

Preuve. On le montre de façon élémentaire en vérifiant que, par exemple, dans $A = \mathbb{Z}[X]$, l'idéal $I = 2A + XA$ (voir ci-dessous la définition 3.3.1) n'est pas un idéal principal.

Par l'absurde, supposons qu'il existe $P \in A$ tel que $I = PA$. Comme $2 \in I$, il existerait $Q \in A$ tel que $2 = PQ$, ce qui impliquerait par un raisonnement sur les degrés que $P \in \mathbb{Z}$. Comme de plus $X \in I$, il existerait $R \in A$ tel que $X = PR$, ce qui impliquerait $P = \pm 1$ (et $R = \pm X$). On aurait donc $1 = \pm P \in I$, de sorte qu'il existerait $S, T \in A$ tels que $1 = 2S + TX$, ce qui est clairement impossible dans $A = \mathbb{Z}[X]$, puisque le coefficient constant de $2S + TX$ est pair. □

3.3 Idéal engendré par une partie, somme d'idéaux

3.3.1 Proposition et définition. *Soit A un anneau commutatif unitaire.*

(i) *Si I et J sont des idéaux de A, alors l'ensemble $I + J = \{x + y\,;\, x \in I, y \in J\}$ est un idéal de A, appelé l'idéal somme de I et J, et c'est le plus petit idéal contenant I et J.*

(ii) *En particulier, si x et y sont des éléments de A, l'ensemble $xA + yA = \{xa + yb\,;\, a, b \in A\}$ est le plus petit idéal de A contenant x et y.*

Preuve. Soient I et J deux idéaux de A. Il est clair que $I + J$ est un sous-groupe additif de A (c'est le sous-groupe engendré par $I \cup J$). Soit $z \in I + J$ et $a \in A$ quelconques; il existe $x \in I$ et $y \in J$ tels que $z = x + y$, d'où $za = xa + ya$. Or $xa \in I$ car $x \in I$ et I est un idéal; de même $ya \in J$. On conclut que $za \in I + J$, ce qui prouve que $I + J$ est un idéal de A. Il est clair que $I \subseteq I + J$, puisque tout $x \in I$ s'écrit $x = x + 0$ avec $0 \in J$; de même $J \subseteq I + J$. Pour montrer que c'est le plus petit, supposons que K est un idéal de A contenant I et J. En particulier, K est stable par addition, et donc, quels que soient $x \in I \subseteq K$ et $y \in J \subseteq K$, on a $x + y \in K$. Donc $I + J \subseteq K$. Ce qui achève de prouver (i). Le point (ii) s'en déduit avec $I = xA$ et $J = yA$. □

3.3.2 Remarques. Soit A un anneau commutatif unitaire.

(a) Plus généralement pour toute partie $X \neq \emptyset$ de A, l'*idéal engendré* par X est par définition l'intersection de tous les idéaux de A contenant X; c'est le plus petit idéal de A contenant X.

La proposition 3.2.1 correspond à $X = \{x\}$, le point (i) de 3.3.1 à $X = I \cup J$, et le point (ii) de 3.3.1 à $X = \{x, y\}$.

(b) L'intérêt de la notion d'idéal somme réside bien sûr dans le fait que la réunion de deux idéaux n'est en général pas un idéal (ce n'est pas en général un sous-groupe additif : prendre par exemple $A = \mathbb{Z}$, $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$).

3.4 Produit d'idéaux, opérations sur les idéaux

3.4.1 Définition et proposition. *Soit A un anneau commutatif unitaire. Si I et J sont des idéaux de A, on note IJ l'ensemble des éléments de A qui sont somme d'un nombre fini de produits d'un élément de I par un élément de J. Autrement dit, pour tout $x \in A$:*

$$x \in IJ \text{ signifie qu'il existe } n \in \mathbb{N}^*,\ y_1, \ldots, y_n \in I \text{ et } z_1 \ldots, z_n \in J \text{ tels que } x = \sum_{i=1}^{n} y_i z_i.$$

Alors IJ est un idéal de A, appelé l'idéal produit de I et J ; c'est le plus petit idéal contenant l'ensemble $\{yz\,;\, y \in I, z \in J\}$, et il vérifie: $IJ \subset I \cap J$.

Preuve. Il est clair que IJ est un sous-groupe additif de A. Soit $x = \sum_{i=1}^{n} y_i z_i$ un élément quelconque de IJ, avec $y_1, \ldots, y_n \in I$ et $z_1, \ldots, z_n \in J$. Pour tout $a \in A$, on a $ay_i \in I$ quel que soit $1 \leq i \leq n$, donc $ax = \sum_{i=1}^{n} (ay_i) z_i$ appartient encore à IJ. Ceci prouve que IJ est un idéal. Il est clair qu'il contient $X = \{yz\,;\, y \in I, z \in J\}$. Soit maintenant K un idéal qui contient X. Il contient aussi les sommes d'éléments de X, et donc $IJ \subseteq K$. Ceci s'applique en particulier à $K = I \cap J$, qui contient bien X. □

3.4.2 Exercice. Soit A un anneau commutatif unitaire. Montrer que, si I, J et K sont des idéaux de A, on a :

$$I + (J + K) = (I + J) + K, \qquad I(JK) = (IJ)K, \qquad I(J + K) = IJ + IK.$$

3.5 *Complément* : caractéristique d'un anneau

3.5.1 Remarques préliminaires.

(a) Soit A un anneau commutatif unitaire. Pour tout $x \in A$, on note $2x = x+x$, $3x = x+x+x$ et de même $nx = x+x+\cdots+x$ (avec n termes) pour tout entier $n \geq 2$. On pose naturellement $1x = x$ et $0x = 0$, ce qui définit la notation nx pour tout $n \in \mathbb{N}$. Si l'on considère maintenant un entier $m \leq 0$, on convient que $mx = n(-x) = -(nx)$ où $n = -m \in \mathbb{N}$. On a ainsi défini la notation nx pour tout $x \in A$ et tout $n \in \mathbb{Z}$.

(b) Soit A un anneau commutatif unitaire. On vérifie aisément que, pour tout $n \in \mathbb{Z}$, on a:

$$(\ n1_A = 0_A \ ) \Leftrightarrow (\ nx = 0_A \ \text{ pour tout } x \in A \ ).$$

3.5.2 Lemme et définition. *Soit A un anneau commutatif unitaire. Il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Il est défini par $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On l'appelle le morphisme canonique de $\mathbb{Z}$ dans A.*

Preuve. Si f est un morphisme d'anneaux unitaires de $\mathbb{Z}$ dans A, on doit avoir $f(1) = 1_A$, d'où par additivité $f(2) = f(1) + f(1) = 1_A + 1_A = 2\,1_A$, et par récurrence $f(n) = n1_A$ pour tout entier $n \geq 1$. Comme f est un morphisme de groupes additifs, on a aussi $f(0) = 0_A$ et $f(m) = f(-n) = -f(n) = -(n1_A) = (-n)1_A = m1_A$ pour tout entier $m \leq 0$ et en posant $n = -m$. En résumé, on a $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. Réciproquement, il est facile de vérifier (faites-le) que f ainsi défini est bien un morphisme d'anneaux unitaires. □

3.5.3 Définition. Soit A un anneau commutatif unitaire. On appelle *caractéristique* de A, notée $\operatorname{car} A$, l'unique entier $k \in \mathbb{N}$ tel que $\operatorname{Ker} f = k\mathbb{Z}$, où f est le morphisme canonique de $\mathbb{Z}$ dans A.

Comme $f : \mathbb{Z} \to A$ est un morphisme d'anneaux unitaires d'après ce qui précède, $\operatorname{Ker} f$ est un idéal de $\mathbb{Z}$ d'après 3.1.3.(ii), et il est donc de la forme $k\mathbb{Z}$ pour un unique $k \in \mathbb{N}$ d'après 3.2.4.

Grâce à la remarque 3.5.1.(b), cette définition se traduit par:

$$\operatorname{car} A = 0 \ \Leftrightarrow \ \left[\ (nx = 0_A \text{ pour tout } \ x \in A \ ) \Leftrightarrow (n = 0) \ \right]$$

$$\operatorname{car} A = k > 0 \ \Leftrightarrow \ \left[\ (nx = 0_A \text{ pour tout } \ x \in A \ ) \Leftrightarrow (n \in k\mathbb{Z}) \ \right]$$

3.5.4 Exemples.

(a) L'anneau $\mathbb{Z}$ est de caractéristique nulle, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) Pour tout $n \geq 2$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. En particulier, pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

(c) Soit A un anneau commutatif unitaire. Pour tout sous-anneau unitaire B de A, on a:

$$\operatorname{car} A = \operatorname{car} B.$$

4 – Anneaux quotients

4.1 Quotient d'un anneau par un idéal

4.1.1 Remarques préliminaires. Soient A un anneau commutatif unitaire et I un idéal de A.

(a) L'idéal I est en particulier un sous-groupe du groupe additif A, et il est trivialement normal (on dit aussi distingué) puisque A est abélien. On peut considérer le groupe additif quotient A/I. Rappelons que, si l'on note $\overline{x}$ la classe dans A/I d'un élément x de A, on a par définition :

$$\overline{x} = \{y \in A\,;\, x - y \in I\} := x + I.$$

Rappelons aussi que l'addition dans A/I est définie par : $\overline{x} + \overline{y} = \overline{x+y}$ pour tous $x, y \in A$.

En particulier A/I est abélien, de neutre additif $\overline{0} = I$. La surjection canonique $p : A \to A/I$ qui à tout élément x de A associe sa classe $\overline{x}$ est alors un morphisme de groupes pour l'addition.

(b) On définit dans A/I une multiplication en posant: $\overline{x}.\overline{y} = \overline{xy}$ pour tous $x, y \in A$,

1. Elle est bien définie, indépendamment des représentants choisis.

   Preuve. Soient $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors $x' - x \in I$ et $y' - y \in I$. On calcule : $x'y' - xy = x'(y'-y) + (x'-x)y$. Comme $x' - x \in I$ et que I est un idéal, on a $(x'-x)y \in I$; de même $x'(y'-y) \in I$ puisque $y'-y \in I$. On conclut que $x'y'-xy \in I$ comme somme de deux éléments de I, et donc $\overline{x'y'} = \overline{xy}$. □

2. Elle est associative, commutative, distributive sur l'addition dans A/I, et admet $\overline{1}$ comme élément neutre.

   Preuve. Quels que soient $x, y, z \in A$, on a $(\overline{x}.\overline{y}).\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}.(\overline{y}.\overline{z})$, ce qui montre l'associativité. Le reste se montre de même. □

3. La surjection canonique p vérifie $p(1) = \overline{1}$ et $p(xy) = p(x).p(y)$ pour tous $x, y \in A$.

   Preuve. Par définition de p d'une part, et de la multiplication dans A/I d'autre part, on a $p(xy) = \overline{xy} = \overline{x}.\overline{y} = p(x).p(y)$. □

On a ainsi démontré :

4.1.2 Théorème. *Soit A un anneau commutatif unitaire. Pour tout idéal I de A, l'ensemble quotient A/I muni de l'addition et de la multiplication définies ci-dessus est un anneau commutatif unitaire, et la surjection canonique $p : A \to A/I$ est un morphisme d'anneaux unitaires.*

4.1.3 Théorème (dit premier théorème d'isomorphisme). *Soient A et B deux anneaux commutatifs unitaires, et $f : A \to B$ un morphisme d'anneaux unitaires. Alors l'anneau quotient de A par l'idéal* $\operatorname{Ker} f$ *est isomorphe au sous-anneau* $\operatorname{Im} f = f(A)$ *de B. On note :*

$$A/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Preuve. On a déjà démontré en théorie des groupes que l'application :

$$\begin{aligned} \varphi :\ A/\operatorname{Ker} f &\longrightarrow \operatorname{Im} f \\ \overline{x} &\longmapsto f(x) \end{aligned}$$

est bien définie et réalise un isomorphisme de groupes additifs de $A/\operatorname{Ker} f$ sur $\operatorname{Im} f$. Par ailleurs, en utilisant le fait que f est un morphisme d'anneaux unitaires, on a clairement $\varphi(\overline{1_A}) = f(1_A) = 1_B$ et $\varphi(\overline{x}\ \overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$ pour tous $x, y \in A$, ce qui achève de prouver que φ est un isomorphisme d'anneaux unitaires. □

Remarquons qu'en particulier, $A/I \simeq A$ lorsque $I = \{0_A\}$, et A/I est l'anneau nul lorsque $I = A$.

4.2 Idéaux d'un anneau quotient

4.2.1 Proposition. *Soient A un anneau commutatif et I un idéal de A. Pour tout idéal J de A contenant I, l'image $p(J)$ est un idéal de A/I que l'on note J/I. Réciproquement, tout idéal de A/I est de la forme J/I pour J un unique idéal de A contenant I.*

Preuve. La première assertion découle du point (iii) de la proposition 3.1.3 et de la surjectivité de p. Pour la réciproque, considérons K un idéal de A/I. Posons $J = p^{-1}(K) = \{x \in A\,;\, p(x) \in K\}$. D'après le point (i) de la proposition 3.1.3, J est un idéal de A. Si $x \in I$, on a $p(x) = \overline{0}$, donc $p(x) \in K$, de sorte que $x \in p^{-1}(K)$, c'est-à-dire $x \in J$. Ceci montre que $I \subseteq J$. Par définition de J, on a $p(J) \subseteq K$. Réciproquement, soit $\overline{x} \in K$, avec $x \in A$; comme $p(x) = \overline{x} \in K$, on a clairement $x \in p^{-1}(K) = J$, et donc $\overline{x} = p(x) \in p(J)$. En résumé, $K = p(J)$, ce que l'on note $K = J/I$.

Pour l'unicité, considérons un idéal J' de A tel que $I \subseteq J'$ et $p(J') = p(J)$. Quel que soit $x' \in J'$, il existe $x \in J$ tel que $p(x') = p(x)$ donc $x' - x \in I$. On a $x' = y + x$ avec $y \in I$ et l'hypothèse $I \subseteq J$ implique $y \in J$ d'où $x' \in J$. On conclut que $J' \subseteq J$. L'inclusion réciproque s'obtient de même. □

Cette proposition établit qu'il existe une bijection (à savoir $J \mapsto J/I$) entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I.

► *Exemples des idéaux de $\mathbb{Z}/n\mathbb{Z}$.* Fixons un entier $n \geq 2$. Alors $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et l'anneau quotient n'est autre que l'anneau commutatif unitaire $\mathbb{Z}/n\mathbb{Z}$ déjà considéré en 1.1.3. Pour tout diviseur q de n, il existe un et un seul idéal de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, qui est $d\mathbb{Z}/n\mathbb{Z}$ où $n = dq$. Réciproquement tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est de ce type.

Exemple: dans $\mathbb{Z}/12\mathbb{Z}$, les idéaux sont: $\{\overline{0}\} = 12\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{6}\} = 6\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{4}, \overline{8}\} = 4\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = 3\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} = 2\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$. □

4.2.2 Théorème (dit troisième théorème d'isomorphisme). *Soient A un anneau commutatif unitaire et I un idéal de A. Pour tout idéal J/I de A/I, avec J idéal de A contenant I, on a l'isomorphisme d'anneaux $(A/I)/(J/I) \simeq A/J$.*

Preuve. Considérons les surjections canoniques $p : A \to A/I,\ x \mapsto \overline{x}$ et $p' : A \to A/J,\ x \mapsto \widehat{x}$. Pour tout $x \in A$, posons $\varphi(\overline{x}) = \widehat{x}$. L'application $\varphi : A/I \to A/J$ est bien définie : en effet, si x et y sont deux éléments de A tels que $\overline{x} = \overline{y}$, alors $x - y \in I$, donc $x - y \in J$ puisque $I \subseteq J$, et donc $\widehat{x} = \widehat{y}$. Cette application vérifie par définition $\varphi \circ p = p'$, et il est facile de vérifier que φ est un morphisme d'anneaux de A/I dans A/J. Tout élément de A/J est de la forme $\widehat{x}$ avec $x \in A$, et l'élément $\overline{x}$ de A/I vérifie alors $\varphi(\overline{x}) = \widehat{x}$, ce qui prouve que φ est surjective. De plus, un élément $\overline{x}$ de A/I appartient au noyau de φ si et seulement si $\widehat{x} = \widehat{0}$, c'est-à-dire si et seulement si $x \in J$, ce qui prouve que $\operatorname{Ker}\varphi = J/I$. En appliquant le théorème 4.1.3, l'isomorphisme $(A/I)/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$ se traduit par $(A/I)/(J/I) \simeq A/J$. □

► *Exemple des polynômes.* Soit A un anneau commutatif unitaire. Pour tout idéal I de A, on note $I[X]$ le sous-ensemble de $A[X]$ formé des polynômes à coefficients dans I. Alors $I[X]$ est un idéal de $A[X]$ et les anneaux $(A/I)[X]$ et $A[X]/I[X]$ sont isomorphes.

Preuve. La première assertion est une simple vérification. Pour la seconde, considérons la surjection canonique $p : A \to A/I$ et considérons son extension canonique $f : A[X] \to (A/I)[X]$, définie par $P = \sum_{i=0}^{n} a_i X^i \mapsto f(P) = \sum_{i=0}^{n} p(a_i) X^i$. Il est clair que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $\operatorname{Ker} f = I[X]$. L'isomorphisme $A[X]/\operatorname{Ker} f \simeq \operatorname{Im} f$ du théroème 4.1.3 devient donc $A[X]/I[X] \simeq (A/I)[X]$. □

Remarquons qu'en particulier A/I est intègre si et seulement si $(A/I)[X]$ intègre d'après 2.3.4.(ii), donc si et seulement si $A[X]/I[X]$ intègre. Avec la notion introduite ci-dessous, ceci montre que l'idéal $I[X]$ est premier dans $A[X]$ si et seulement si l'idéal I est premier dans A.

4.3 Idéaux premiers, idéaux maximaux

4.3.1 Définitions. Soit A un anneau commutatif unitaire.

Un idéal P de A est dit *premier* lorsque $P \neq A$ et vérifie:

quels que soient x et y deux éléments de A, si $xy \in P$, alors $x \in P$ ou $y \in P$.

Un idéal M de A est dit *maximal* lorsque $M \neq A$ et vérifie:

quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

► *Remarque.* Par définition, ($\{0\}$ premier) $\Leftrightarrow$ (A intègre). Si A est un corps, l'idéal $\{0\}$ est l'unique idéal maximal de A, et si A n'est pas un corps, $\{0\}$ n'est pas maximal (résulte de 3.2.2).

4.3.2 Théorème fondamental. *Soit I un idéal d'un anneau commutatif unitaire A. On a :*

$$\begin{array}{ccc} I \text{ maximal} & \Longleftrightarrow & A/I \text{ corps} \\ \Downarrow & & \Downarrow \\ I \text{ premier} & \Longleftrightarrow & A/I \text{ intègre} \end{array}$$

Preuve. Supposons que M est un idéal maximal de A. Comme $M \neq A$, l'anneau A/M est non nul. Considérons un idéal quelconque K de A/M. D'après la proposition 4.2.1, il existe un idéal J de A tel que $M \subseteq J$ et $K = J/M$. Mais, par maximalité de M, l'inclusion $M \subseteq J$ implique que $J = M$ ou $J = A$, c'est-à-dire $J/M = \{\overline{0}\}$ ou $J/M = A/M$. Ceci prouve que les seuls idéaux de A/M sont $\{\overline{0}\}$ et A/M. On conclut avec 3.2.2 que A/M est un corps. L'implication réciproque découle des mêmes calculs. L'équivalence de la première ligne est donc vérifiée.

Supposons que P est un idéal premier de A. Comme $P \neq A$, l'anneau A/P est non nul. Considérons $\overline{x}, \overline{y} \in A/P$ tels que $\overline{x}\ \overline{y} = \overline{0}$. On a $\overline{xy} = \overline{0}$, c'est-à-dire $xy \in P$. Comme P est premier, on a $x \in P$ ou $y \in P$, c'est-à-dire $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Donc A/P est intègre. L'implication réciproque découle des mêmes calculs. L'équivalence de la seconde ligne est donc vérifiée. Il suffit de rappeler que tout corps est un anneau intègre pour achever la preuve. □

4.3.3 Corollaire (idéaux premiers et maximaux d'un anneau quotient). *Soient A un anneau commutatif unitaire et I un idéal de A. La bijection $J \mapsto J/I$ entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I induit par restriction une bijection entre l'ensemble des idéaux premiers (respectivement maximaux) de A contenant I et l'ensemble des idéaux premiers (respectivement maximaux) de A/I.*

Preuve. Soit K un idéal de A/I et J l'unique idéal de A contenant I tel que $K = J/I$ (voir proposition 4.2.1). D'après le théorème 4.2.2, on a l'isomorphisme d'anneaux $(A/I)/K \simeq A/J$. Dès lors, J est premier (resp. maximal) dans A si et seulement si A/J est intègre (resp. est un corps), c'est-à-dire si et seulement si $(A/I)/K$ est intègre (resp. est un corps), ce qui est équivaut à dire que K est un idéal premier (resp. maximal) de A/I. □

► *Remarque : idéaux premiers et morphismes d'anneaux.* Soient A et B des anneaux commutatifs unitaires. On peut montrer à titre d'exercice que :

1. si $f : A \to B$ est un morphisme d'anneaux unitaires, alors, quel que soit Q un idéal premier de B, l'image réciproque $f^{-1}(Q)$ est un idéal premier de A, qui contient $\operatorname{Ker} f$;
2. si $f : A \to B$ est un morphisme d'anneaux unitaires surjectif, alors, quel que soit P un idéal premier de A contenant $\operatorname{Ker} f$, l'image directe $f(P)$ est un idéal premier de B.

4.3.4 Remarques (lien entre primalité et maximalité)

(a) D'après le théorème ci-dessus, tout idéal maximal est premier.

(b) Il existe des anneaux commutatifs unitaires A possédant des idéaux premiers non nuls qui ne sont pas maximaux.

Exemple. Prenons $A = \mathbb{Z}[X]$ et $I = XA$ l'idéal principal engendré par X. Soit $f : A \to \mathbb{Z}$ l'application qui à tout polynôme $P = a_m X^m + \cdots + a_1 X + a_0$, avec les $a_i \in \mathbb{Z}$, associe le terme constant a_0. Il est facile de vérifier que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $I = XA$. D'après 4.1.3, on a alors $A/I \simeq \mathbb{Z}$. Comme $\mathbb{Z}$ est intègre sans être un corps, l'idéal I est premier sans être maximal. □

(c) Dans l'anneau $\mathbb{Z}$, considérons un idéal quelconque I. D'après 3.2.4, il existe $k \in \mathbb{N}$ unique tel que $I = k\mathbb{Z}$. Si $k = 1$, alors $I = \mathbb{Z}$ n'est ni premier, ni maximal. Si $k = 0$, alors $I = \{0\}$ est premier mais non maximal. Si maintenant $k \geq 2$, il résulte de la proposition 2.3.3 que :

($k\mathbb{Z}$ est premier) $\Leftrightarrow$ (k est un nombre premier) $\Leftrightarrow$ ($k\mathbb{Z}$ est maximal)

Ainsi dans l'anneau $\mathbb{Z}$, les notions d'idéal maximal et d'idéal premier non nul coïncident. C'est en fait le cas pour tous les anneaux principaux (au sens de la définition 3.2.3), comme le montre la proposition suivante.

4.3.5 Proposition. *Dans un anneau principal, tout idéal premier non nul est maximal (et donc, pour les idéaux non nuls, les notions de premier et de maximal coïncident).*

Preuve. Soit I un idéal premier non nul de A. Il existe donc $a \in A$, $a \neq 0$, tel que $I = aA$. Soit J un idéal de A tel que $I \subset J$. Comme A est un anneau principal, il existe $b \in A$, $b \neq 0$, tel que $J = bA$. Comme $a \in I$, on a $a \in J$ donc il existe $x \in A$ tel que $a = bx$. Supposons que $I \neq J$, c'est-à-dire que $b \notin I$. On a $a = bx \in I$ avec $b \notin I$, donc le fait que I soit premier implique que $x \in I$. Donc il existe $y \in A$ tel que $x = ay$. On déduit que $a = bx = bay$, ou encore $a(1 - by) = 0$. D'une part A est intègre car principal. D'autre part $a \neq 0$. Donc $1 - by = 0$, d'où $by = 1$, ce qui prouve que $b \in U(A)$. D'après 3.2.1.(iii), on conclut que $J = A$. Ainsi, pour tout idéal J de A tel que $I \subset J$ et $J \neq I$, on a $J = A$. Donc I est maximal. □

On a vu ci-dessus que $\mathbb{Z}[X]$ possède des idéaux premiers non nuls non maximaux, ce qui donne une nouvelle preuve du fait, déjà montré en 3.2.5, que l'anneau $\mathbb{Z}[X]$ n'est pas principal.

4.4 *Complément* : à propos des idéaux maximaux

Le théorème suivant est un résultat important et non trivial, admis au niveau de ce cours de licence, qui démontre l'existence d'idéaux maximaux dans tout anneau unitaire commutatif.

4.4.1 Théorème (de Krull). *Tout anneau commutatif unitaire a au moins un idéal maximal.*

Parmi les applications pratiques de ce résultat théorique, les suivantes sont parmi les plus utiles :

4.4.2 Corollaire. *Soit A un anneau commutatif unitaire.*

(i) *Pour tout idéal I de A, distinct de A, les idéaux maximaux de A/I sont de la forme M/I où M est un idéal maximal de A contenant I.*

(ii) *Tout idéal distinct de A est contenu dans un idéal maximal de A.*

(iii) *Tout élément de A non inversible dans A appartient à un idéal maximal de A.*

Preuve. Soit I un idéal de A tel que $I \neq A$. D'après le théorème de Krull, l'anneau A/I admet un idéal maximal N. D'après 4.2.1, il existe un unique idéal M de A contenant I tel que $N = M/I$, et d'après le corollaire 4.3.3, M est un idéal maximal de A ; ceci prouve à la fois (i) et (ii).

Le point (iii) résulte immédiatement du point (ii) et de 3.2.1.(iii). □

4.5 *Complément* : propriété universelle de l'anneau quotient

Par leur caractère très général, les deux résultats suivants permettent d'apporter une réponse rapide à de multiples problèmes formulés dans des situations particulières. Par exemple, le raisonnement que l'on a fait pour démontrer le théorème 4.2.2 n'est qu'un cas particulier du théorème ci-dessous.

4.5.1 Lemme (factorisation des morphismes).
Soient A un anneau commutatif unitaire, I un idéal de A, et p la surjection canonique $A \to A/I$. Soient A' un anneau commutatif unitaire, I' un idéal de A', et p' la surjection canonique $A' \to A'/I'$. Alors, pour tout morphisme d'anneaux unitaires $f : A \to A'$ vérifiant la condition $f(I) \subseteq I'$, il existe un unique morphisme $\varphi : A/I \to A'/I'$ tel que $\varphi \circ p = p' \circ f$.

On représente la situation par le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p'} \\ A/I & \xrightarrow[\varphi]{} & A'/I' \end{array}$$

Preuve. Notons $\overline{x} = p(x)$ pour tout $x \in A$ et $\widehat{y} = p'(y)$ pour tout $y \in A'$. Posons $\varphi(\overline{x}) = \widehat{f(x)}$ pour tout $x \in A$. Il est facile de vérifier que l'hypothèse $f(I) \subseteq I'$ assure que φ est bien définie (c'est-à-dire que $\widehat{f(x)} = \widehat{f(x')}$ lorsque $\overline{x} = \overline{x}'$). On définit ainsi une application $\varphi : A/I \to A'/I'$, qui est clairement un morphisme d'anneaux unitaires puisque f, p, p' sont des morphismes d'anneaux unitaires. Par construction, φ vérifie $\varphi \circ p = p' \circ f$, et cette condition impose que ce choix de définition de φ est unique. □

4.5.2 Théorème (propriété universelle de l'anneau quotient). *Soient A un anneau commutatif unitaire, I un idéal de A, et p la surjection canonique $A \to A/I$.*

(i) *Pour tout anneau commutatif unitaire A' et tout morphisme d'anneaux unitaires $f : A \to A'$ tel que $I \subseteq \operatorname{Ker} f$, il existe un unique morphisme d'anneaux unitaires $\varphi : A/I \to A'$ tel que $f = \varphi \circ p$.*

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle p}\downarrow & \nearrow_{\varphi} & \\ A/I & & \end{array}$$

(ii) *De plus: (f surjectif $\Rightarrow$ φ surjectif) et ($I = \operatorname{Ker} f$ $\Rightarrow$ φ injectif).*

Preuve. Le point (i) résulte de l'application immédiate du lemme précédent en prenant $I' = \{0_{A'}\}$, de sorte que la condtion $f(I) \subseteq I'$ se traduit par $I \subseteq \operatorname{Ker} f$. Les deux assertions du point (ii) se déduisent immédiatement du fait que $\varphi(\overline{x}) = f(x)$ pour tout $x \in A$. □

5 – Divisibilité et idéaux

5.1 Multiples, diviseurs et idéaux principaux

5.1.1 Définitions. Soit A un anneau commutatif unitaire. Soient x et y deux éléments de A. On dit que x est un *diviseur* de y dans A, ou encore que x *divise* y dans A, ou encore que y est un *multiple* de x dans A, lorsqu'il existe $a \in A$ tel que $y = xa$. On note alors : $x \mid y$.

5.1.2 Proposition. *Soit A un anneau commutatif unitaire. Pour tous $x, y \in A$, on a :*

$$(x \mid y) \Leftrightarrow (y \in xA) \Leftrightarrow (yA \subseteq xA).$$

Preuve. Supposons $x \mid y$. Il existe $a \in A$ tel que $y = xa$. Donc $y \in xA$. Or yA est le plus petit idéal de A contenant y comme on l'a vu en 3.2.1, d'où $yA \subseteq xA$. La réciproque est claire. □

5.1.3 Corollaire. *Soit A un anneau commutatif unitaire. On a :*

(i) *Pour tous $x, y, z \in A$,* $(x \mid y$ et $y \mid z) \Rightarrow (x \mid z)$.

(ii) *Pour tout $u \in A$,* $(u \in U(A)) \Leftrightarrow (uA = A) \Leftrightarrow (u \mid y$ quel que soit $y \in A)$.

(iii) *Pour tous $x, u \in A$,* $(u \in U(A)$ et $x \mid u) \Rightarrow (x \in U(A))$.

Preuve. Résulte immédiatement de la proposition précédente. □

5.2 Eléments associés

5.2.1 Définition. Soit A un anneau commutatif unitaire *intègre*. Soient x et y deux éléments de A. On dit que x et y sont *associés* lorsqu'on a à la fois $x \mid y$ et $y \mid x$. On note alors $x \sim y$.

5.2.2 Proposition. *Soit A un anneau commutatif unitaire intègre. Pour tous $x, y \in A$, on a :*

$$(x \sim y) \Leftrightarrow (x \mid y \text{ et } y \mid x) \Leftrightarrow (xA = yA) \Leftrightarrow (\text{il existe } u \in U(A) \text{ tel que } x = uy).$$

Preuve. La première équivalence est vraie par définition, la seconde découle de 5.1.2. Pour la dernière, supposons que $x \sim y$. Il existe $u, v \in A$ tels que $x = uy$ et $y = vx$, donc $x = uvx$. Si $x = 0$, alors $y = 0$, et on a $x = uy$ pour tout $u \in U(A)$. Si $x \neq 0$, on écrit $x(1 - uv) = 0$; l'intégrité de A implique que $uv = 1$, d'où $u \in U(A)$, ce qui montre le résultat voulu. Réciproquement, supposons $x = uy$ avec $u \in U(A)$; on a $y \mid x$ et, puisque $y = u^{-1}x$ avec $u^{-1} \in A$, on a aussi $x \mid y$. On conclut que $x \sim y$. □

5.2.3 Corollaire. Deux éléments associés ont les mêmes multiples et les mêmes diviseurs.

Preuve. Supposons $x \sim y$. On a donc $xA = yA$. Tout diviseur z de y vérifie $yA \subseteq zA$, donc $xA \subseteq zA$, c'est-à-dire que z divise x. □

5.2.4 Exemples.

(a) Dans $\mathbb{Z}$, deux entiers m et n sont associés si et seulement si $m = \pm n$; voir 2.1.3.(a).

(b) Pour tout anneau intègre A, deux polynômes P et Q de $A[X]$ sont associés si et seulement s'il existe $c \in U(A)$ tel que $P = cQ$, et l'on a alors $Q = c^{-1}P$; (voir corollaire 2.3.5).

(c) En particulier, si K est un corps, deux polynômes P et Q de $K[X]$ sont associés si et seulement s'il existe $c \in K^*$ tel que $P = cQ$.

5.3 Eléments premiers entre eux, pgcd et ppcm

5.3.1 Définition. Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On dit que x et y sont *premiers entre eux dans A*, ou *étrangers dans A*, lorsque les seuls éléments de A qui divisent à la fois x et y sont les éléments de $U(A)$.

Remarque. Si x est premier avec y, alors x est premier avec tout élément associé à y.

5.3.2 Définition. Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On dit que x et y *admettent un plus grand commun diviseur* dans A lorsqu'il existe un élément $d \in A$ tel que : d divise x, d divise y, et tout élément qui divise à la fois x et y divise aussi d. On dit alors que d est *un pgcd* de x et y.

5.3.3 Proposition. *Soit A un anneau commutatif unitaire intègre. Soient $x, y \in A$.*

(i) *Si x et y admettent un pgcd d, alors un élément quelconque $d' \in A$ est un pgcd de x et y si et seulement si d' est associé à d.*

(ii) *Les éléments x et y sont premiers entre eux si et seulement si 1 est un pgcd de x et y, c'est-à-dire encore si et seulement si $U(A)$ est l'ensemble des pgcd de x et y.*

(iii) *Si x et y sont non nuls et admettent un pgcd d, alors les deux éléments x' et y' tels que $x = dx'$ et $y = dy'$ sont premiers entre eux dans A.*

Preuve. Montrons (i). Si d' est un pgcd de x et y, il divise x et y, et donc puisque d est un pgcd de x et y, on a $d' \mid d$. De même, $d \mid d'$, et donc $d \sim d'$. Comme deux éléments associés ont les mêmes multiples et les mêmes diviseurs, la réciproque est claire. Le point (ii) se déduit immédiatement de (i). Pour le point (iii), considérons z un diviseur commun à x' et y'. Il existe $a, b \in A$ tels que $x' = za$ et $y' = zb$. Donc $x = dza$ et $y = dzb$. Ceci prouve que dz est un diviseur commun à x et y, donc un diviseur de leur pgcd d. Il existe donc $u \in A$ tel que $d = dzu$, ou encore $d(1 - zu) = 0$. Comme A est intègre et $d \neq 0$ (car x et y sont non nuls), on a $zu = 1$. On conclut que $z \in U(A)$. □

5.3.4 Définition. Soit A un anneau commutatif unitaire intègre. Soient x et y deux éléments de A. On dit que x et y *admettent un plus petit commun multiple* dans A lorsqu'il existe un élément $m \in A$ tel que : m est un multiple de x, m est un multiple de y, et tout élément qui est un multiple à la fois de x et de y est aussi un multiple de m. On dit que m est *un ppcm* de x et y.

Remarque et notations. Il est clair que, comme la notion de pgcd, la notion de ppcm est définie à la relation d'association près. Dans toute la suite, on notera $\mathrm{pgcd}(x, y)$ un pgcd quelconque que x et y, et $\mathrm{ppcm}(x, y)$ un ppcm quelconque de x et de y.

5.3.5 Proposition. *Soit A un anneau commutatif unitaire intègre. Si deux éléments non nuls $x, y \in A$ admettent un ppcm dans A, alors ils admettent un pgcd dans A, et on a alors la relation :*

$$xy \sim \mathrm{pgcd}(x, y)\,\mathrm{ppcm}(x, y).$$

Preuve. Supposons que x et y admettent un ppcm m. Comme m est un multiple de x et de y, il existe $x', y' \in A$ tel que $m = xx' = yy'$. Le produit xy est aussi un multiple de x et de y donc de m, donc il existe $d \in A$ tel que $xy = md$. Ainsi $xy = xx'd$, donc par intégrité de A, $y = x'd$. De même $x = y'd$, ce qui prouve que d est un diviseur commun de x et y.

Supposons maintenant que e est un diviseur commun de x et de y. Il existe $x'', y'' \in A$ tels que $x = ex''$ et $y = ey''$. L'élément $n = ex''y'' = xy'' = x''y$ apparaît comme un multiple commun de x et y. C'est donc un multiple de m par définition du ppcm. Il existe $k \in A$ tel que $n = km$. Donc $kme = ne = e^2x''y'' = xy = md$ d'où $ke = d$ par intégrité de A, c'est-à-dire que e divise d. On conclut que d est un pgcd de x et y. □

5.4 *Complément* : notion d'élément irréductible

5.4.1 Définition. Soit A un anneau commutatif unitaire *intègre*. Soit x un élément de A. On dit que x est *irréductible* dans A lorsqu'il n'est pas inversible dans A, et vérifie :

$$\text{si } x = ab \text{ avec } a, b \in A, \text{ alors } a \in U(A) \text{ ou } b \in U(A).$$

Remarques.

1. 0 n'est pas irréductible dans A.
2. Un élément de A peut être irréductible dans A mais ne plus l'être dans un anneau contenant A. Par exemple, 3 est irréductible dans $\mathbb{Z}$, mais pas dans $\mathbb{Q}$ puisqu'il est inversible dans $\mathbb{Q}$.

Exemples.

1. Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.
2. Pour tout corps K, les polynômes de degré un sont toujours irréductibles dans $K[X]$ (par un simple argument de degré).
3. Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un. Cela résulte du théorème de d'Alembert-Gauss (hautement non trivial) qui établit que tout polynôme non constant à coefficients complexes admet au moins un zéro dans $\mathbb{C}$, et se décompose alors en produit de facteurs de degré 1.
4. Si $K = \mathbb{R}$, les éléments irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un, et les polynômes de degré deux de discriminant strictement négatif. C'est une conséquence du résultat précédent et du fait qu'un polynôme de $\mathbb{R}[X]$ admettant un zéro complexe admet aussi son conjugué pour zéro.

5.4.2 Proposition. *Soit A un anneau commutatif unitaire intègre.*

(i) *Un élément x de A est irréductible dans A si et seulement si l'idéal principal xA est maximal parmi les idéaux principaux de A distincts de A.*

(ii) *Tout élément de A associé à un élément irréductible dans A est irréductible dans A.*

Preuve. Supposons x irréducible. L'idéal principal $M = xA$ est distinct de A car $x \notin U(A)$. Soit $J = aA$ un idéal principal de A distinct de A, c'est-à-dire tel que $a \notin U(A)$, et supposons que $M \subseteq J$. Alors en particulier $x \in J$, donc il existe $b \in A$ tel que $x = ab$. Puisque $a \notin U(A)$, l'irréductibilité de x implique que $b \in U(A)$. Donc $x \sim a$, d'où $M = J$. Ceci prouve que M est maximal parmi les idéaux principaux distincts de A.

Réciproquement soit $x \in A$ tel que xA soit maximal parmi les idéaux principaux distincts de A. Soient $a, b \in A$ tels que $x = ab$. Alors $x \in aA$, et donc $xA \subseteq aA$. Si $a \in U(A)$, alors $aA = A$. Sinon, $aA \neq A$ et la maximalité de xA implique alors que $xA = aA$, donc $x \sim a$, d'où l'existence de $u \in U(A)$ tel que $x = ua$. Ainsi $x = ua = ba$ avec $a \neq 0$ (car $x \neq 0$), ce qui implique par intégrité de A que $b = u$, et donc $b \in U(A)$. L'assertion (i) est ainsi établie.

L'assertion (ii) découle de (i) puisque deux éléments associés engendrent le même idéal principal. □

5.4.3 Proposition. *Dans un anneau commutatif unitaire intègre A, tout élément irréductible de A est premier avec tout élément qu'il ne divise pas.*

Preuve. Soit x irréductible dans A. Soit $y \in A$ tel que x ne divise pas y. Par l'absurde, supposons que u soit un diviseur commun de x et y non inversible dans A. On aurait alors $x = ua$ et $y = ub$ avec $a, b \in A$. Comme $x = ua$ et $u \notin U(A)$, l'irréductibilité de x impliquerait que $a \in U(A)$. On obtiendrait $u = xa^{-1}$ avec $a^{-1} \in A$, de sorte que $y = xa^{-1}b$, ce qui contredit le fait que x ne divise pas y.

5.5 *Complément* : notion d'élément premier

5.5.1 Définition. Soit A un anneau commutatif unitaire *intègre*. Soit x un élément de A. On dit que x est dit *premier* dans A lorsqu'il est non nul et non inversible dans A, et vérifie : :

si x divise ab avec $a, b \in A$, alors x divise a ou x divise b.

5.5.2 Proposition. *Soit A un anneau commutatif unitaire intègre. Pour tout $x \in A$, on*

(i) *(x premier dans A) $\Leftrightarrow$ (xA idéal premier non nul de A).*

(ii) *Tout élément de A associé à un élément premier dans A est premier dans A.*

Preuve. L'équivalence (i) est évidente par définition même d'un idéal premier et par la proposition 5.1.2. L'assertion (ii) en découle puisque deux éléments associés engendrent le même idéal principal. □

5.5.3 Proposition. *Soit A un anneau commutatif unitaire intègre.*

(i) *Tout élément premier dans A est irréductible dans A.*

(ii) *Si A est principal, tout élément irréductible dans A est premier dans A ; donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.*

Preuve. Soit $x \in A$ premier dans A. On a $x \notin U(A)$. Supposons que $x = ab$ avec $a, b \in A$. En particulier $x \mid ab$, donc puisque x est premier, $x \mid a$ ou $x \mid b$. Supposons que $x \mid a$. Il existe $y \in A$ tel que $a = xy$, d'où $x = xyb$, ou encore $x(1 - yb) = 0$. Comme x est non nul car premier, et que A est intègre, on conclut que $yb = 1$, et donc que $b \in U(A)$. On prouve de même que $a \in U(A)$ si $x \mid b$. On a ainsi montré que x est irréductible dans A.

Supposons maintenant que A est principal. Soit x un élément irréductible de A. Il est non inversible (par définition), non nul (voir la première remarque de 5.4.1), et l'idéal $M = xA$ est maximal parmi les idéaux principaux de A distincts de A (voir proposition de 5.4.2). Mais ici tout idéal de A est par hypothèse principal. Donc M est tout simplement un idéal maximal de A. Donc M est un idéal premier de A (voir théorème 4.3.2), et comme il est non nul, on déduit de la proposition de 5.5.2 que x est un élément premier dans A. □

5.5.4 Contre-exemple. La réciproque de l'assertion (i) peut être fausse dans certains anneaux. Par exemple dans l'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}\,; a, b \in \mathbb{Z}\}$, l'élément 3 est irréductible, mais non premier.

Preuve. Posons $A = \mathbb{Z}[i\sqrt{5}]$. D'après le dernier résultat de 1.2.4 pour $\omega = -5$, A est un anneau commutatif unitaire intègre, qui contient $\mathbb{Z}$ comme sous-anneau, et l'application $N : A \to \mathbb{N}$ définie par $N(x) = |x|^2 = a^2 + 5b^2$ pour tout $x = a + ib\sqrt{5}$ est multiplicative. Il en résulte en particulier que $U(A) = \{x \in A\,;\, N(x) = 1\} = \{-1; +1\}$.

Montrons que 3 n'est pas premier dans A. Observons d'abord que 3 ne divise pas $2 + i\sqrt{5}$ dans A (en effet, on aurait sinon $(2+i\sqrt{5}) = 3(a+ib\sqrt{5})$ avec $a, b \in \mathbb{Z}$, d'où $3a = 2$ et $1 = 3b$, ce qui est impossible). De même 3 ne divise pas $2 - i\sqrt{5}$. Et pourtant 3 divise $9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ dans A. On conclut que 3 n'est pas premier dans A.

Montrons maintenant que 3 est irréductible dans A. Il est clair que 3 n'est pas inversible dans A. Supposons que $3 = xy$ avec $x = a+ib\sqrt{5}$ et $y = c+id\sqrt{5}$, où $a, b, c, d \in \mathbb{Z}$. On a $N(x)N(y) = N(xy) = 9$ dans $\mathbb{N}^*$, donc trois cas seulement sont possibles: $N(x) = N(y) = 3$, ou $N(x) = 1$ et $N(y) = 9$, ou $N(x) = 9$ et $N(y) = 1$. Or le premier cas est impossible (car $a^2 + 5b^2 = 3$ n'a pas de solutions entières), le second implique que $x \in U(A)$, et le troisième implique de même que $y \in U(A)$. On conclut que 3 est irréductible dans A. □

Ceci montre en particulier que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

6 – Divisibilité dans les anneaux principaux

6.1 Pgcd dans les anneaux principaux, théorème de Bézout et lemme de Gauss

6.1.1 Théorème. *Soit A un anneau principal. Deux éléments quelconques de A admettent toujours des pgcd et des ppcm dans A. Plus précisément, quels que soient a et b dans A :*

(i) *tout générateur de l'idéal principal $aA + bA$ est un pgcd de a et b :*

$$(\ d \text{ est un pgcd de } a \text{ et } b\ ) \Leftrightarrow (\ aA + bA = dA\ )\ ;$$

(ii) *tout générateur de l'idéal principal $aA \cap bA$ est un ppcm de a et b :*

$$(\ m \text{ est un ppcm de } a \text{ et } b\ ) \Leftrightarrow (\ aA \cap bA = mA\ ).$$

Preuve. Comme A est principal, l'idéal $aA + bA$ est principal. Il existe $d \in A$ tel que $aA + bA = dA$. Montrons que d est un pgcd de a et b. On a d'abord $aA \subseteq aA + bA$, donc $aA \subseteq dA$, donc $d \mid a$. De même, $d \mid b$. Soit maintenant $c \in A$ tel que $c \mid a$ et $c \mid b$. Alors $aA \subseteq cA$ et $bA \subseteq cA$, donc, puisque cA est stable par addition, $aA + bA \subseteq cA$, c'est-à-dire $dA \subseteq cA$, et donc $c \mid d$. Ceci prouve que d est un pgcd de a et b. Réciproquement, soit d' un pgcd de a et b. D'après 5.3.3, on a $d' \sim d$, donc $dA = d'A$, c'est-à-dire $d'A = aA + bA$.

Comme A est principal, l'idéal $aA \cap bA$ est principal. Il existe $m \in A$ tel que $aA \cap bA = mA$. Montrons que m est un ppcm de a et b. On a d'abord $aA \supseteq aA \cap bA$, donc $aA \supseteq mA$, donc $a \mid m$. De même, $b \mid m$. Soit maintenant $c \in A$ tel que $a \mid c$ et $b \mid c$. Alors $aA \supseteq cA$ et $bA \supseteq cA$, donc $aA \cap bA \supseteq cA$, c'est-à-dire $mA \supseteq cA$, et donc $m \mid c$. Ceci prouve que m est un ppcm de a et b. Réciproquement, soit m' un ppcm de a et b. D'après 5.3.4, on a $m' \sim m$, donc $mA = m'A$, c'est-à-dire $m'A = aA \cap bA$. □

6.1.2 Théorème de Bézout. *Soit A un anneau principal. Pour tous a et b dans A, on a :*

$$(\ a \text{ et } b \text{ premiers entre eux dans } A\ ) \Leftrightarrow (\ \text{il existe } u, v \in A \text{ tels que } au + bv = 1\ ).$$

Preuve. Soient $a, b \in A$ fixés. Supposons a et b premiers entre eux ; 1 est donc un pgcd de a et b. Il résulte alors du théorème précédent que $aA + bA = A$. En particulier $1 \in aA + bA$, et donc il existe $(u, v) \in A^2$ tel que $au + bv = 1$. Supposons réciproquement qu'il existe $u, v \in A$ tels que $au + bv = 1$; alors 1 appartient à $aA + bA$, donc $aA + bA = A$. Or, si d est un pgcd de a et b, on a $dA = aA + bA$. On déduit que $dA = A$, donc $d \in U(A)$, c'est-à-dire a et b premiers entre eux. □

6.1.3 Lemme de Gauss. *Soit A un anneau principal. Pour tous a, b, c dans A, on a :*

$$(\ a \text{ divise } bc, \text{ et } a \text{ premier avec } b\ ) \Rightarrow (\ a \text{ divise } c\ ).$$

Preuve. Comme a et b sont premiers entre eux, il existe d'après le théorème de Bézout $u, v \in A$ tels que $au + bv = 1$. Donc $c = cau + cbv$. Comme a divise bc, on a $bc \in aA$, donc $bcv \in aA$. Par ailleurs il est clair que $acu \in aA$. Par stabilité de l'idéal aA pour l'addition, on conclut que $c = acu + bcv \in aA$. □

6.1.4 Corollaire. *Soit A un anneau principal. Soient a et b deux éléments non nuls de A. Soient $d = \mathrm{pgcd}(a, b)$ et a', b' les éléments de A tels que $a = da'$ et $b = db'$. Alors, il existe des éléments $u, v \in A$ tels que $au + bv = d$, et l'ensemble de tous les couples $(x, y) \in A^2$ tels que $ax + by = d$ est alors égal à $\{(u, v) + c(-b', a')\,;\, c \in A\}$.*

Preuve. D'après le point (iii) de la proposition 5.3.3, les éléments a' et b' sont premiers entre eux dans A. Il existe donc d'après le théorème de Bézout des éléments $u, v \in A$ tels que $a'u + b'v = 1$, ce qui implique $au + bv = d$. Pour tout $c \in A$, le couple $(x, y) = (u, v) + c(-b', a') = (u - cb', v + ca')$ vérifie $a'x + b'y = a'(u - cb) + b'(v + ca) = a'u - a'cb' + b'v + b'ca' = a'u + b'v = 1$, et donc $ax + by = d$.

Réciproquement, quel que soit $(x, y) \in A^2$ tel que $ax + by = d$, on a $a'x + b'y = 1 = a'u + b'v$, d'où $a'(u - x) = b'(y - v)$. Comme a' et b' sont premiers entre eux, il résulte du théorème de Gauss que a' divise $y - v$. Il existe donc $c \in A$ tel que $y - v = ca'$. On a alors $ca'b' = b'(y - v) = a'(u - x)$. Comme $a' \neq 0$, on déduit par intégrité de A que $u - x = cb'$; on obtient donc bien $x = u - cb'$ et $y = v + ca'$. □

Ce corollaire appliqué au cas particulier où $d = 1$ souligne en particulier que, dans le théorème de Bézout, il n'y a pas unicité du couple (u, v).

6.2 Anneaux euclidiens

6.2.1 Proposition (exemple préliminaire de l'anneau $\mathbb{Z}$). *Quels que soient des entiers a et b, avec $b \neq 0$, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ uniques tels que $a = bq + r$ et $0 \leq r < |b|$.*

Preuve. Montrons d'abord l'unicité. Supposons l'existence de deux couples (q, r) et (q', r') dans $\mathbb{Z} \times \mathbb{N}$ satisfaisant aux conditions $a = bq + r$ avec $0 \leq r < |b|$, et $a = bq' + r'$ avec $0 \leq r' < |b|$. On a alors $b(q - q') = r' - r$ et $-|b| < r' - r < |b|$. Donc $-|b| < b(q - q') < |b|$. Comme $b \neq 0$, on en déduit que $-1 < q - q' < 1$, ce qui, puisque $q - q'$ est un entier, implique $q - q' = 0$. Ainsi $q = q'$, d'où $r = r'$.

Pour montrer maintenant l'existence, supposons d'abord $b > 0$. Posons $E = \{k \in \mathbb{Z}\,;\, kb \leq a\}$. C'est une partie de $\mathbb{Z}$ qui est non vide (car $0 \in E$ si $a \geq 0$ et $a \in E$ si $a < 0$) et qui est majorée (par le maximum des entiers a et 0). Donc elle admet un plus grand élément. Notons-le q. On a par définition de q la double inégalité $qb \leq a < (q + 1)b$, de sorte que l'entier $r = a - qb$ vérifie $0 \leq r < b$. Supposons maintenant $b < 0$. D'après ce qui précède, il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = (-b)q + r$ et $0 \leq r < |b|$. Le couple $(-q, r) \in \mathbb{Z} \times \mathbb{N}$ vérifie alors $a = b(-q) + r$ et $0 \leq r < |b|$. □

6.2.2 Proposition (exemple préliminaire de l'anneau $K[X]$). *Soit K un corps commutatif. Quels que soient des polynômes F et G dans $K[X]$, avec $G \neq 0$, il existe $Q \in K[X]$ et $R \in K[X]$ uniques tels que $F = GQ + R$ et $\deg R < \deg G$.*

Preuve. On montre d'abord l'unicité. Supposons que deux couples (Q, R) et (Q', R') dans $K[X] \times K[X]$ satisfassent aux conditions $F = GQ + R = GQ' + R'$ avec $\deg R < \deg G$ et $\deg R' < \deg G$. On a alors $G(Q - Q') = R' - R$. Comme K est un corps (en particulier intègre), on a d'après la proposition 2.3.4 l'égalité $\deg G + \deg(Q - Q') = \deg(R' - R)$. Or $\deg R < \deg G$ et $\deg R' < \deg G$ impliquent que $\deg(R' - R) < \deg G$. Donc $\deg G + \deg(Q - Q') < \deg G$, ce qui n'est possible que si $\deg(Q - Q') = -\infty$, c'est-à-dire $Q = Q'$. On a alors forcément aussi $R = R'$.

Pour montrer maintenant l'existence, notons $n = \deg F$ et $m = \deg G \in \mathbb{N}$. Si $n < m$, on a le résultat voulu en prenant $Q = 0$ et $R = F$. On suppose donc désormais que $n \geq m \geq 0$ (en particulier $F \neq 0$). Notons :

$$\mathcal{E} = \{P \in K[X]\,;\, P = F - SG \text{ avec } S \in K[X]\}.$$

Si $\mathcal{E}$ contient le polynôme nul, il existe $S \in K[X]$ tel que $F = SG$ et on a le résultat voulu en prenant $Q = S$ et $R = 0$. On peut donc supposer dans la suite que $\mathcal{E}$ ne contient pas le polynôme nul.

L'ensemble $\mathcal{E}$ est non-vide (il contient par exemple le polynôme F en prenant $S = 0$). Il en résulte que l'ensemble $E = \{\deg P\,;\, P \in \mathcal{E}\}$ est une partie non-vide de $\mathbb{N}$. L'ensemble E admet donc un plus petit élément n_0. D'une part tout polynôme $P \in \mathcal{E}$ vérifie $\deg P \geq n_0$. D'autre part il existe un polynôme $P_0 \in \mathcal{E}$ tel que $\deg P_0 = n_0$. Ce polynôme P_0 est de la forme $P_0 = F - S_0G$ pour un certain $S_0 \in K[X]$. On obtient ainsi l'égalité $F = S_0G + P_0$. Si $n_0 < m = \deg G$, on a le résultat voulu en prenant $Q = S_0$ et $R = P_0$. On suppose donc maintenant que $n_0 \geq m$. Notons :

$$P_0 = a_{n_0}X^{n_0} + \cdots + a_1X + a_0 \quad \text{et} \quad G = b_mX^m + \cdots + b_1X + b_0$$

avec les $a_i, b_j \in K$ pour tout $1 \leq i \leq n_0$ et $1 \leq j \leq m$, tels que $a_{n_0} \neq 0$ et $b_m \neq 0$. On peut écrire $P_0 = a_{n_0}b_m^{-1}X^{n_0-m}G + P_1$ avec $\deg P_1 \leq n_0 - 1 < n_0$. On a donc :

$$P_1 = P_0 - a_{n_0}b_m^{-1}X^{n_0-m}G = F - [S_0 + a_{n_0}b_m^{-1}X^{n_0-m}]G,$$

ce qui prouve que $P_1 \in \mathcal{E}$. Puisque $\deg P_1 < n_0$, ceci contredit la définition de n_0. C'est donc que le cas où $n_0 \geq m$ est impossible, ce qui achève la preuve. □

▶ *Remarque.* La preuve utilise de façon essentielle le fait que les coefficients des polynômes sont dans un corps, ce qui permet d'inverser le coefficient dominant b_m. De fait, le résultat de cette proposition n'est plus vrai si K n'est pas un corps.

Par exemple, prenons dans $\mathbb{Z}[X]$ les polynômes $F = X^2+1$ et $G = 3X+1$. S'il existait $Q, R \in \mathbb{Z}[X]$ tel que $F = GQ + R$ avec $\deg R < \deg G$, on aurait nécessairement $R = r \in \mathbb{Z}$ et $Q = aX + b$ avec $a, b \in \mathbb{Z}$, d'où $X^2 + 1 = (3X + 1)(aX + b) + r$, et en particulier $3a = 1$, ce qui est impossible dans $\mathbb{Z}[X]$.

6.2.3 Définition. On appelle *anneau euclidien* un anneau commutatif unitaire qui est intègre, et pour lequel il existe une application $\delta : A^* \to \mathbb{N}$ vérifiant les deux conditions suivantes:

1. pour tous $a, b \in A^*$, $(\ a \mid b\ ) \Rightarrow (\ \delta(a) \leq \delta(b)\ )$;
2. pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que:
$$(\ a = bq + r\ ) \quad \text{et} \quad (\ r = 0 \ \text{ ou } \ \delta(r) < \delta(b)\ ).$$

Une application δ vérifiant ces deux conditions s'appelle un *stathme* euclidien. Dans la condition 2, on dit que q est un *quotient* et r un *reste* dans la *division euclidienne* de a par b.

6.2.4 Exemples.

(a) L'anneau $\mathbb{Z}$ est euclidien, pour le stathme défini par $\delta(x) = |x|$ pour tout $x \in \mathbb{Z}$ non nul.

(b) Si K est un corps, l'anneau $K[X]$ est euclidien, pour le stathme défini par $\delta(F) = \deg F$ pour tout $F \in K[X]$ non nul.

(c) L'anneau $\mathbb{Z}[i]$ est euclidien, pour le stathme défini par $\delta(z) = z\,\overline{z}$ pour tout $z \in \mathbb{Z}[i]$ non nul.

Les preuves des exemples (a) et (b) découlent directement des deux propositions préliminaires précédentes. L'exemple (c) est laissé en exercice.

Remarque. La définition d'un stathme n'impose pas de conditions d'unicité de q et r.

Et effectivement, ils ne sont pas forcément uniques. Par exemple, dans $\mathbb{Z}$, pour $a = 19$ et $b = 3$, on a : $19 = 6\times3+1 = 7\times3+(-2)$ avec $r = 1$ et $r' = -2$ qui vérifient tous les deux $\delta(r) = |1| = 1 < \delta(3) = 3$ et $\delta(r') = |-2| = 2 < \delta(3) = 3$. De fait, l'unicité de q et r qui apparaît dans la première proposition préliminaire ci-dessus tient au fait qu'on y a remplacé la condition ($r = 0$ ou $|r| < |b|$), qui correspond à la définition du stathme, par la condition plus forte $0 \leq r < |b|$.

6.2.5 Théorème. *Tout anneau euclidien est principal.*

Preuve. Soit A un anneau euclidien, de stathme δ. Il est intègre, et il s'agit donc de montrer que tout idéal I de A est principal. C'est clair si $I = \{0\}$ (alors $I = 0A$) ou si $I = A$ (alors $I = 1A$). On suppose donc $I \neq \{0\}$ et $I \neq A$. On considère $E = \{\delta(x)\,;\, x \in I, x \neq 0\}$. C'est une partie non vide de $\mathbb{N}$, elle admet donc un plus petit élément n. Il existe $x \in I$, $x \neq 0$ tel que $n = \delta(x)$. Soit alors $a \in I$ quelconque; par division euclidienne de a par x, il existe $q, r \in A$ tels que $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x) = n$. Or $r = a - xq$ avec $a \in I$ et $x \in I$, donc $r \in I$ par définition d'un idéal. Par minimalité de n, on ne peut donc pas avoir $\delta(r) < n$, et donc nécessairement $r = 0$, d'où $a = xq$. Ceci prouve que tout $a \in I$ appartient à xA. On conclut que $I \subseteq xA$, et donc $I = xA$. □

6.2.6 Exemples, contre-exemples, remarques.

(a) Il en résulte que : $\mathbb{Z}$, $K[X]$ *lorsque* K *est un corps, et* $\mathbb{Z}[i]$ *sont des anneaux principaux.*

(b) La réciproque du théorème 6.2.5 est fausse ; il existe des anneaux principaux qui ne sont pas euclidiens. C'est par exemple un exercice classique (mais non trivial) que de monter que :

l'anneau $\mathbb{Z}[\omega] = \{a + \omega b\,;\, a, b \in \mathbb{Z}\}$ *pour* $\omega = \frac{1+i\sqrt{19}}{2}$ *est principal et non euclidien.*

(c) On a déjà observé précédemment (en 3.2.5 et en 4.3.5) que l'anneau $\mathbb{Z}[X]$ n'est pas principal. Ceci montre que, pour un anneau commutatif unitaire intègre A :

$$(\ A \text{ euclidien} \not\Rightarrow A[X] \text{ euclidien}\ ) \quad \text{et} \quad (\ A \text{ principal} \not\Rightarrow A[X] \text{ principal}\ ).$$

On a en fait le résultat général suivant :

6.2.7 Théorème. *Soit A un anneau commutatif unitaire. Les trois conditions suivantes sont équivalentes :* (i) *A est un corps ;* (ii) *$A[X]$ est euclidien ;* (iii) *$A[X]$ est principal.*

Preuve. On a vu que (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Supposons donc maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, donc A est intègre. L'application $f : A[X] \to A$ qui, à tout polynôme $P = \sum_{i=0}^{n} a_i X^i$, associe le coefficient a_0 est un morphisme d'anneaux, clairement surjectif. Donc le premier théorème d'isomorphisme conduit à $A[X]/\operatorname{Ker} f \simeq A$. L'intégrité de A implique ainsi que $A[X]/\operatorname{Ker} f$ est intègre. Donc d'après 4.3.2, $\operatorname{Ker} f$ est un idéal premier non nul de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors, d'après la proposition 4.3.5, un idéal maximal de $A[X]$. Donc $A[X]/\operatorname{Ker} f$ est un corps en réappliquant 4.3.2. On conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

6.3 Pgcd dans les anneaux euclidiens, lemme d'Euclide et application.

6.3.1 Lemme (fondamental de l'algorithme d'Euclide). *Soit A un anneau euclidien. Soient $a, b \in A$ tels que $b \neq 0$. Alors, pour tout reste r d'une division euclidienne de a par b, tout pgcd de a et b est associé à tout pgcd de b et r. En d'autres termes, en notant δ le stathme de A :*

$$(\ a = bq + r,\ \text{ avec } r = 0 \ \text{ ou } \ \delta(r) < \delta(b)\ ) \ \Rightarrow\ (\ \operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(b, r)\ ).$$

Preuve. Il résulte de l'égalité $a = bq + r$ que $a \in bA + rA$; on en déduit que $aA \subset bA + rA$. Comme par ailleurs $bA \subset bA + rA$, la stabilité de $bA + rA$ pour l'addition implique alors $aA + bA \subset bA + rA$. En écrivant ensuite $r = a - bq$, on montre de même que $bA + rA \subset aA + bA$. Finalement $aA + bA = bA + rA$. Donc, en notant d un pgcd de a et b, et d' un pgcd de b et r, on a $dA = d'A$, c'est-à-dire $d \sim d'$. □

6.3.2 Théorème (algorithme d'Euclide). *Soit A un anneau euclidien. Soient $a, b \in A$ non nuls.*

(i) *il existe $k \in \mathbb{N}^*$ et des éléments $q_1, \ldots, q_k, r_0, r_1, \ldots, r_k \in A$, avec*

$$r_0 = b \neq 0,\ \ r_1 \neq 0,\ \ r_2 \neq 0,\ \ \ldots\ \ \ r_{k-2} \neq 0,\ \ r_{k-1} \neq 0,\ \ r_k = 0,$$

vérifiant la condition:

$$\delta(r_{k-1}) < \delta(r_{k-2}) < \cdots < \delta(r_2) < \delta(r_1) < \delta(r_0) = \delta(b),$$

et les égalités:

$$\begin{aligned} &a = bq_1 + r_1 = r_0 q_1 + r_1, \quad r_0 = r_1 q_2 + r_2, \quad r_1 = r_2 q_3 + r_3, \\ &\cdots\cdots\cdots \\ &r_{k-3} = r_{k-2} q_{k-1} + r_{k-1}, \quad r_{k-2} = r_{k-1} q_k + r_k = r_{k-1} q_k. \end{aligned}$$

(ii) *On a alors :* $\operatorname{pgcd}(a, b) \sim r_{k-1}$.

Preuve. On effectue la division euclidienne de a par b. Notons $a = bq_1 + r_1$ avec $r_1 = 0$ ou $\delta(r_1) < \delta(b)$.
Si $r_1 = 0$, on arrête.
Si $r_1 \neq 0$, on a $\delta(r_1) < \delta(b)$, et on effectue la division euclidienne de b par r_1.
Notons $b = r_1q_2 + r_2$ avec $r_2 = 0$ ou $\delta(r_2) < \delta(r_1)$.
Si $r_2 = 0$, on arrête.
Si $r_2 \neq 0$, on a $\delta(r_2) < \delta(r_1) < \delta(b)$, et on effectue la division euclidienne de r_1 par r_2.
Notons $r_1 = r_2q_3 + r_3$ avec $r_3 = 0$ ou $\delta(r_3) < \delta(r_2)$.
Si $r_3 = 0$, on arrête.
Si $r_3 \neq 0$, on a $\delta(r_3) < \delta(r_2) < \delta(r_1) < \delta(b)$, et on effectue la division euclidienne de r_2 par r_3.
On itère ainsi le processus. Comme il n'existe pas de suite infinie strictement décroissante dans $\mathbb{N}$, il existe un rang $k \in \mathbb{N}^*$ tel que $r_{k-1} \neq 0$ et $r_k = 0$. En notant $r_0 = b$ pour la cohérence des notations, ceci prouve le point (i).

Pour (ii), remarquons que le lemme 6.3.1 appliqué dans la première égalité de (i) donne $\text{pgcd}(a, b) \sim \text{pgcd}(b, r_1) \sim \text{pgcd}(r_0, r_1)$. De même dans la deuxième égalité, on obtient $\text{pgcd}(r_0, r_1) \sim \text{pgcd}(r_1, r_2)$. Puis $\text{pgcd}(r_1, r_2) \sim \text{pgcd}(r_2, r_3)$, et par une récurrence évidente, $\text{pgcd}(a, b) \sim \text{pgcd}(r_{k-1}, r_k)$. Or puisque r_k est nul, $\text{pgcd}(r_{k-1}, r_k) \sim r_{k-1}$, ce qui achève la preuve. □

On traduit le point (ii) en disant que les pgcd de a et b sont les éléments associés au dernier reste non nul dans la suite des divisions euclidiennes successives de a par b.

6.3.3 Exemple et remarque. Dans l'anneau euclidien $\mathbb{Z}$, soient $a = 33810$ et $b = 4116$. La suite des divisions successives donne :

$$\underbrace{33810}_{a} = \underbrace{4116}_{b=r_0} \times 8 + \underbrace{882}_{r_1} \quad ; \quad \underbrace{4116}_{r_0} = \underbrace{882}_{r_1} \times 4 + \underbrace{588}_{r_2} \quad ; \quad \underbrace{882}_{r_1} = \underbrace{588}_{r_2} \times 1 + \underbrace{294}_{r_3} \quad ; \quad \underbrace{588}_{r_2} = \underbrace{294}_{r_3} \times 2 + 0.$$

On conclut que $\text{pgcd}(a, b) \sim r_3$ donc $\text{pgcd}(33810, 4116) \sim 294$.

A noter que l'on a alors :
$294 = 882 - 588 = 882 + (4 \times 882) - 4116 = 5 \times (33810 - 8 \times 4116) - 4116 = 5 \times 33810 - 41 \times 4116$,
ce qui fournit un couple d'entiers (u, v) prévu au corollaire 6.1.4, c'est-à-dire vérifiant $d = au + bv$.

6.4 *Complément* : décomposition en produit de facteurs irréductibles

6.4.1 Exemple préliminaire (décomposition d'un entier en produits de facteurs premiers). On commence par rappeler le résultat suivant fondamental en arithmétique élémentaire, en notant que les nombres premiers et leurs opposés sont les éléments irréductibles de l'anneau $\mathbb{Z}$.

Lemme. *Dans l'anneau $\mathbb{Z}$:*

(i) *Tout entier différent de 1 et de -1 admet au moins un diviseur premier.*
(ii) *Si un nombre premier divise un produit d'entiers, alors il divise l'un des facteurs de ce produit.*
(ii) *En particulier, si un nombre premier divise un produit de nombres premiers, alors il est égal à l'un d'entre eux.*

Preuve. Il est clair qu'il suffit de prouver (i) pour un entier naturel n supérieur ou égal à 2. Notons $D(n)$ l'ensemble des diviseurs de n supérieurs ou égaux à 2. Il est non vide car il contient n. Comme $\mathbb{N}$ est bien ordonné, $D(n)$ admet un plus petit élément p. C'est un diviseur de n, supérieur ou égal à 2 ; montrons qu'il est premier. Pour cela, considérons un entier naturel a divisant p. Par transitivité de la divisibilité, a divise n. Si $a \geq 2$, alors $a \in D(n)$, donc $p \leq a$ par minimalité de p; ainsi a divise p et $p \leq a$, donc $a = p$. Sinon, $a = 1$. Ceci prouve (i).

Soit p un nombre premier. Supposons que p divise le produit bc de deux entiers b et c. Supposons que p ne divise pas b. Alors, d'après 5.4.3, p est premier avec b. Ce qui, d'après lemme de Gauss, implique que p divise c. Ceci prouve l'assertion (ii) ; le point (iii) s'en déduit immédiatement. □

Théorème. *Soit n un entier supérieur ou égal à 2. Il existe, et ceci de façon unique, un entier $s \geq 1$, des nombres premiers $p_1, p_2, \ldots, p_s$ vérifiant $p_1 < p_2 < \cdots < p_s$, et des entiers naturels non nuls $\alpha_1, \alpha_2, \ldots, \alpha_s$ tels que:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}.$$

Preuve. Montrons l'existence d'une telle décomposition par récurrence sur n. C'est clair si $n = 2$. Fixons $n \geq 3$ quelconque et supposons vraie l'existence d'une décomposition pour tout entier strictement inférieur à n. Soit p un diviseur premier de n (il en existe d'après le point (i) du lemme précédent). Si $n = p$, il n'y a rien à démontrer. Sinon, il existe $2 \leq n_0 \leq n-1$ tel que que $n = pn_0$. En appliquant l'hypothèse de récurrence à n_0, on a $n = pp_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$. S'il existe $1 \leq j \leq s$ tel que $p = p_j$, alors $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_j^{\alpha_j+1} \ldots p_s^{\alpha_s}$, d'où le résultat. Sinon, on obtient une décomposition du type voulu (en ordonnant p relativement aux p_i), avec $s+1$ facteurs, et un exposant 1 pour le facteur p.

Montrons l'unicité. Supposons pour cela que $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_t^{\beta_t}$, avec $s \in \mathbb{N}^*$, $p_1 < p_2 < \cdots < p_s$ premiers, $\alpha_i \in \mathbb{N}^*$ pour tout $1 \leq i \leq s$, et $t \in \mathbb{N}^*$, $q_1 < q_2 < \cdots < q_t$ premiers, $\beta_j \in \mathbb{N}^*$ pour tout $1 \leq j \leq t$. D'après le point (iii) du lemme précédent, chaque p_i ($1 \leq i \leq s$) est égal à un des q_j ($1 \leq j \leq t$), et chaque q_j est égal à l'un des p_i. Comme les p_i sont deux à deux distincts, ainsi que les q_j, on a nécessairement $s = t$. De plus la condition de croissance sur les p_i et les q_j implique que l'on a précisément $p_1 = q_1, p_2 = q_2, \ldots, p_s = q_s$. Donc finalement: $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$. Si $\beta_1 > \alpha_1$, on en déduit l'égalité $p_2^{\alpha_2} \ldots p_s^{\alpha_s} = p_1^{\beta_1 - \alpha_1} p_2^{\beta_2} \ldots p_s^{\beta_s}$; celle-ci implique que p_1 divise le produit $p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, ce qui est impossible d'après le point (ii) du lemme précédent. De même $\beta_1 < \alpha_1$ conduit à une contradiction. C'est donc que $\alpha_1 = \beta_1$. On prouve de façon analogue que $\alpha_i = \beta_i$ pour tout $1 \leq i \leq s$. □

Quitte à multiplier par ± 1, le théorème s'applique à tout entier différent de 0, 1 et -1. Ainsi, tout entier non nul et non inversible s'écrit au signe près comme un produit de nombres premiers, de façon unique à l'ordre près des facteurs. C'est un cas particulier du théorème général suivant, que l'on cite ici pour mémoire mais que l'on ne démontre pas au niveau de ce cours de licence.

6.4.2 Théorème. *Soit A un anneau principal. Tout élément de A non nul et non inversible dans A se décompose en un produit d'un nombre fini d'éléments irréductibles dans A. Cette décomposition est unique à l'ordre près des facteurs et au produit par un élément inversible près.*

Explicitement, cela signifie que, dans tout anneau principal A, on a :

(1) tout élément $a \in A$ tel que $a \neq 0$ et $a \notin U(A)$ s'écrit $a = r_1 r_2 \ldots r_n$, avec $r_1, r_2, \ldots, r_n$ des éléments de A irréductibles dans A ;

(2) si $r_1 r_2 \ldots r_n = s_1 s_2 \ldots s_m$, avec $r_1, \ldots, r_n, s_1, \ldots, s_m$ irréductibles dans A, alors $m = n$, et il existe une permutation $\sigma \in S_n$ telle que $s_i \sim r_{\sigma(i)}$ pour tout $1 \leq i \leq n$.

6.4.3 Terminologie et notations. Soit A un anneau principal.

(a) – Dans l'ensemble des éléments irréductibles de A, l'association définit d'après 5.4.2.(ii) une relation d'équivalence. En choisissant dans chaque classe d'équivalence un représentant particulier, on définit un *système de représentants* $\mathcal{R}$ des éléments irréductibles. En d'autres termes, tout élément irréductible de A est équivalent à un unique élément irréductible de la famille $\mathcal{R}$:

quel que soit r irréductible dans A, il existe $r' \in \mathcal{R}$ et $u \in U(A)$ uniques tels que $r = ur'$.

1. Dans l'anneau $\mathbb{Z}$, on choisit comme système de représentants des éléments irréductibles l'ensemble $\mathcal{P}$ des nombres premiers positifs. Tout élément irréductible de $\mathbb{Z}$ est alors de la forme εp avec $p \in \mathcal{P}$ et $\varepsilon \in U(\mathbb{Z}) = \{-1, +1\}$.

2. Dans l'anneau $\mathbb{C}[X]$, on choisit comme système de représentants des éléments irréductibles l'ensemble $\mathcal{R}$ des polynômes de degré 1 unitaires (c'est-à-dire de coefficient dominant égal à 1). Tout élément irréductible est alors de la forme $\alpha(X-\beta)$ avec $X-\beta \in \mathcal{R}$ et $\alpha \in U(\mathbb{C}[X]) = \mathbb{C}^*$.

(b) – Soit $\mathcal{R}$ un système de représentants des éléments irréductibles dans A. Soit $a \in A$ non nul et non inversible. Il résulte de 6.4.2 que a s'écrit de façon unique, à l'ordre près des facteurs :

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}, \quad \text{où } u \in U(A),\ r_i \in \mathcal{R} \text{ (avec } r_i \neq r_j \text{ si } i \neq j),\ n_i \in \mathbb{N}^*.$$

1. Dans $\mathbb{Z}$, tout élément a non nul et distinct de ± 1 s'écrit de façon unique $a = \varepsilon\, p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, où $\varepsilon = \pm 1$, $n_i \in \mathbb{N}^*$, $p_i \in \mathcal{P}$ (avec $p_i \neq p_j$ si $i \neq j$) pour tout $1 \leq i \leq s$.

2. Dans $\mathbb{C}[X]$, tout polynôme $P(X)$ de degré ≥ 1 s'écrit de façon unique:
$$P(X) = \alpha(X-\beta_1)^{n_1}(X-\beta_2)^{n_2} \dots (X-\beta_s)^{n_s},$$
où $\alpha \in \mathbb{C}^*$, $n_i \in \mathbb{N}^*$, $\beta_i \in \mathbb{C}$ (avec $\beta_i \neq \beta_j$ si $i \neq j$) pour tout $1 \leq i \leq s$.

(c) – Soit $\mathcal{R}$ un système de représentants des éléments irréductibles dans A. Soient $a, b \in A$ non nuls et non inversibles. En réunissant les facteurs irréductibles intervenant dans l'écriture ci-dessus de a et dans celle de b, et en autorisant alors des exposants nuls, a et b s'écrivent de façon unique :

$$a = u\, r_1^{n_1} r_2^{n_2} \dots r_q^{n_q} \quad \text{et} \quad b = v\, r_1^{m_1} r_2^{m_2} \dots r_q^{m_q}, \quad \text{où } u, v \in U(A),$$
$$r_i \in \mathcal{R} \text{ (avec } r_i \neq r_j \text{ si } i \neq j),\ \ n_i \in \mathbb{N},\ \ m_i \in \mathbb{N},\ \ (n_i, m_i) \neq (0,0) \ \text{ pour tout } 1 \leq i \leq q.$$

6.4.4 Première application : expression des diviseurs d'un élément. *Soit A un anneau principal. Soit a un élément de A non nul et non inversible dans A. Avec la notation du* (b) *ci-dessus, les diviseurs de a dans A sont tous les éléments de la forme:*

$$w r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}, \ \textit{avec } 0 \leq p_i \leq n_i \textit{ pour tout } 1 \leq i \leq s, \textit{ et } w \in U(A).$$

Preuve. Soit b un diviseur de a. Si $b \in U(A)$, le résultat est clair avec $b = w$ et $p_1 = p_2 = \dots = p_s = 0$. Supposons donc maintenant que $b \notin U(A)$. Soit r l'un des facteurs irréductibles intervenant dans la décomposition de b. Comme $b \mid a$, on a $r \mid a$, c'est-à-dire que r divise $r_1^{n_1} r_2^{n_2} \dots r_s^{n_s}$. Puisque r est premier (car irréductible, voir 5.5.3), on en tire que r est associé à l'un des r_i. Ceci prouve que b est de la forme $b = w\, r_1^{p_1} r_2^{p_2} \dots r_s^{p_s}$, avec $w \in U(A)$ et $p_i \geq 0$ pour tout $1 \leq i \leq s$.

Pour montrer que $p_i \leq n_i$ pour tout $1 \leq i \leq s$, raisonnons par l'absurde. Supposons par exemple (pour fixer les idées) que $p_1 > n_1$. En notant $a = xb$ avec $x \in A$, on aurait donc: $u\, r_2^{n_2} \dots r_s^{n_s} = xw\, r_1^{p_1 - n_1} r_2^{p_2} \dots r_s^{p_s}$, avec $p_1 - n_1 > 0$, ce que contredirait la condition (2) de 6.4.2. □

6.4.5 Seconde application : expression du pgcd et du ppcm. *Soit A un anneau principal. Si a et b sont deux éléments de A non nuls et non inversibles. Avec la notation du* (c)*, on a :*

$$\operatorname{pgcd}(a,b) \sim r_1^{h_1} r_2^{h_2} \dots r_q^{h_q} \quad \textit{et} \quad \operatorname{ppcm}(a,b) \sim r_1^{\ell_1} r_2^{\ell_2} \dots r_q^{\ell_q},$$

avec $h_i = \min(n_i, m_i)$ et $\ell_i = \max(n_i, m_i)$ pour tout $1 \leq i \leq q$.

Preuve. Soient $a, b \in A$. Si $a = 0$, on a $\operatorname{pgcd}(a,b) \sim b$. Si $a \in U(A)$, on a $\operatorname{pgcd}(a,b) \sim a \sim 1$. De même si $b = 0$ ou $b \in U(A)$. Sinon, a et b sont non nuls et non inversibles: le résultat résulte alors de 6.4.4 et de la définition des pgcd et ppcm. □

► *Exemples élémentaires d'illustration*

1. Considérons dans l'anneau $\mathbb{Z}$ les éléments $a = 60$ et $b = -378$. Leurs décompositions en produits de facteurs irréductibles dans $\mathbb{Z}$ sont : $a = 2^2 \times 3 \times 5$ et $b = -2 \times 3^3 \times 7$.
Leurs pgcd sont $\pm 2 \times 3 = \pm 6$. Leurs ppcm sont $\pm 2^2 \times 3^3 \times 5 \times 7 = \pm 3780$

2. Considérons dans l'anneau $\mathbb{R}[X]$ les éléments $P = X^4 - 1$ et $Q = 2X^3 - 2$. Leurs décompositions en produits de facteurs irréductibles dans $\mathbb{R}[X]$ sont :
$$P = (X-1)(X+1)(X^2+1) \quad \text{et} \quad Q = 2(X-1)(X^2+X+1).$$
Leurs pgcd sont $\lambda\,(X-1)$ avec $\lambda \in \mathbb{R}^*$. Leurs ppcm sont $\mu(X-1)(X+1)(X^2+1)(X^2+X+1)$ avec $\mu \in \mathbb{R}^*$.

3. Considérons dans l'anneau $\mathbb{C}[X]$ les mêmes éléments $P = X^4 - 1$ et $Q = 2X^3 - 2$. Leurs décompositions en produits de facteurs irréductibles dans $\mathbb{C}[X]$ sont :
$$P = (X-1)(X+1)(X-i)(X+i) \quad \text{et} \quad Q = 2(X-1)(X-j)(X-j^2).$$

6.5 *Complément* : et si A n'est pas principal ?

Dans les situations que l'on connaît bien de l'arithmétique dans $\mathbb{Z}$ ou $K[X]$ avec K un corps, deux éléments quelconques ont toujours des pgcd et des ppcm, avec des résultats importants dans la pratique qui leur sont liés (théorèmes de Bézout, de Gauss, décomposition canonique en produit de facteurs irréductibles,...). On a vu dans ce chapitre que tout cela reste vrai dans le cadre général des anneaux principaux, avec même quelques propriétés algorithmiques supplémentaires dans le cas particulier des anneaux euclidiens.

On étudiera plus tard (en master) une classe d'anneaux encore plus générale (les anneaux factoriels), qui englobent strictement les anneaux principaux, et où, là encore, l'existence de pgcd et de ppcm pour tous les couples d'éléments permet de faire de l'arithmétique (on n'a plus de propriété de Bézout, mais on a encore le lemme de Gauss et la décomposition canonique en produit d'éléments irréductibles).

Mais on peut garder à l'esprit qu'il existe aussi des anneaux commutatifs unitaires dans lequels l'existence de pgcd ou de ppcm n'est plus assurée. L'exemple que nous donnons ici pour mémoire a déjà été considéré en 5.5.4.

(i) Plaçons-nous dans l'anneau $A = \mathbb{Z}[i\sqrt{5}]$. Considérons les éléments $x = 3$ et $y = 2 + i\sqrt{5}$. Les seuls diviseurs non inversibles de x sont ± 3 et comme ± 3 ne divisent pas y, on déduit que x et y admettent ± 1 comme pgcd. Si x et y admettaient un ppcm, il résulte de la proposition 5.3.5 que ce dernier serait $m = \pm xy = \pm 3(2 + i\sqrt{5})$. Or comme $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ est un multiple commun de x et de y, ce serait un mutiple de leur ppcm $m = 3(2 + i\sqrt{5})$, et donc 3 serait un multiple de $2 + i\sqrt{5}$, ce qui est clairement impossible dans A. Ainsi :

► x et y admettent un pgcd dans A mais n'admettent pas de ppcm dans A.

(ii) Plaçons-nous encore dans l'anneau $A = \mathbb{Z}[i\sqrt{5}]$. Considérons les éléments $x = 9$ et $y = 6 + 3i\sqrt{5}$. En écrivant $x = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ et $y = 3(2 + i\sqrt{5})$, il apparaît que 3 et $2 + i\sqrt{5}$ sont des diviseurs communs de x et y. Supposons que x et y admettent un pgcd d. Ce dernier serait divisible par 3 et par $2 + i\sqrt{5}$. Il existerait $a, b \in A$ tel que $d = 3a$ et $d = b(2 + i\sqrt{5})$. Mais d'autre part il existerait $x', y' \in A$ tels que $9 = dx'$ et $6 + 3i\sqrt{5} = dy'$. D'où en particulier $9 = 3ax'$ donc a diviserait 3 dans A, c'est-à-dire $a = \pm 3$ ou $a = \pm 1$. Le cas $a = \pm 3$ est impossible car $d = \pm 9$ ne divise pas $y = 6 + 3i\sqrt{5}$. Le cas $a = \pm 1$ est aussi impossible car on aurait $d = \pm 3 = b(2 + i\sqrt{5})$ qui n'a pas de solution dans A. Ainsi :

► x et y n'admettent pas de pgcd dans A.

7 – Applications aux polynômes d'endomorphismes

Dans tout ce qui suit, on fixe un corps K et un K-espace vectoriel E de dimension finie $n \geq 1$.

7.1 Polynômes d'endomorphismes, polynômes de matrices

7.1.1 Algèbre d'endomorphismes. Considérons le K-espace vectoriel $(\operatorname{End} E, +, .)$ des endomorphismes de l'espace vectoriel E. On a vu en 1.1.2.b) que $\operatorname{End} E$ est aussi un anneau (non commutatif) unitaire pour les lois $+$ et $\circ$. Cette double structure de K-espace vectoriel et d'anneau, avec de plus la propriété de cohérence (évidente à vérifier) :

$$\lambda.(u \circ v) = (\lambda.u) \circ v = u \circ (\lambda.v) \text{ pour tous } u, v \in \operatorname{End} E, \lambda \in K$$

correspond à ce l'on appelle une structure de K-algèbre. On retiendra que:

$(\operatorname{End} E, +, \circ, .)$ *est une K-algèbre, non commutative, unitaire.*

En particulier l'élément neutre pour le produit interne dans $\operatorname{End} E$ est id_E, et l'on note $u^m = u \circ u \circ \ldots \circ u$, avec m facteurs.

7.1.2 Algèbre de matrices carrées. De même, en notant $\mathcal{M}_n(K)$ l'ensemble des matrices carrées d'ordre n à coefficients dans K, on a:

$(\mathcal{M}_n(K), +, \times, .)$ *est une K-algèbre, non commutative, unitaire, isomorphe à* $\operatorname{End} E$.

En effet, tout choix d'une base $\mathcal{B}$ de E permet de considérer la bijection $m : \operatorname{End} E \to \mathcal{M}_n(K)$ associant à tout endomorphisme u sa matrice $m(u)$ par rapport à la base $\mathcal{B}$, qui vérifie $m(u+v) = m(u) + m(v)$, $m(u \circ v) = m(u) \times m(v)$, $m(\lambda.u) = \lambda.m(u)$ pour tous $u, v \in \operatorname{End} E, \lambda \in K$, et réalise donc un *isomorphisme d'algèbres unitaires.* En particulier on a bien $m(\mathrm{id}_E) = I_n$.

7.1.3 Algèbre de polynômes. En considérant sur $K[X]$ à la fois sa structure d'anneau commutatif unitaire et sa structure usuelle de K-espace vectoriel de $K[X]$, on vérifie aisément que:

$K[X]$ *est une K-algèbre, commutative, unitaire.*

7.1.4 Théorème.

(i) *Pour tout $u \in \operatorname{End} E$ fixé, il existe un unique morphisme d'algèbres $\varphi_u : K[X] \to \operatorname{End} E$ tel que $\varphi_u(X) = u$. Il est défini par $P \mapsto P(u)$ où l'on pose :*

$$P(u) = \alpha_m.u^m + \alpha_{m-1}.u^{m-1} + \cdots + \alpha_1.u + \alpha_0.\,\mathrm{id}_E \quad \textit{lorsque } P = \textstyle\sum_{i=0}^m \alpha_i X^i \textit{ où } \alpha_i \in K.$$

(ii) *Pour tout $A \in \mathcal{M}_n(K)$ fixé, il existe un unique morphisme d'algèbres $\psi_A : K[X] \to \mathcal{M}_n(K)$ tel que $\psi_A(X) = A$. Il est défini par $P \mapsto P(A)$ où l'on pose:*

$$P(A) = \alpha_m.A^m + \alpha_{m-1}.A^{m-1} + \cdots + \alpha_1.A + \alpha_0.I_n \quad \textit{lorsque } P = \textstyle\sum_{i=0}^m \alpha_i X^i \textit{ où } \alpha_i \in K.$$

Preuve. Montrons d'abord l'unicité. Supposons que φ soit un morphisme d'algèbres $K[X] \to \operatorname{End} E$ tel que $\varphi(X) = u$. Si $P = \sum_{i=1}^m \alpha_i X^i$ est un élément de $K[X]$ quelconque, alors $\varphi(P) = \sum_{i=1}^m \varphi(\alpha_i X^i) = \sum_{i=1}^m \alpha_i \varphi(X)^i = \sum_{i=1}^m \alpha_i u^i$, ce qui prouve que $\varphi = \varphi_u$. Il est clair réciproquement que φ_u est bien un morphisme d'algèbre $K[X] \to \operatorname{End} E$ tel que $\varphi_u(X) = u$, ce qui prouve (i). Le (ii) est analogue. □

Avec les notations de 7.1.2, on a $\psi_A = m \circ \varphi_u$ pour tout choix d'une base de E avec $m(u) = A$.

► *Attention* au fait que $\varphi_u(\alpha_0) = \varphi_u(\alpha_0.1_K) = \alpha_0.\varphi_u(1_K) = \alpha_0.\,\mathrm{id}_E$, et de même $\psi_A(\alpha_0) = \alpha_0.I_n$.

7.2 Idéal d'annulation et polynôme minimal

7.2.1 Proposition et définition. *On note O l'endomorphisme nul de E et O_n la matrice nulle dans $\mathcal{M}_n(K)$.*

(i) *Pour tout endomorphisme $u \in \operatorname{End} E$, l'ensemble N_u des polynômes $P \in K[X]$ tels que $P(u) = O$ est un idéal non nul de $K[X]$, appelé l'idéal d'annulation de l'endomorphisme u.*

(ii) *Pour toute matrice $A \in \mathcal{M}_n(K)$, l'ensemble N_A des polynômes $P \in K[X]$ tels que $P(A) = O_n$ est un idéal non nul de $K[X]$, appelé l'idéal d'annulation de la matrice A.*

Preuve. Avec les notations de 7.1.4, on a $N_u = \operatorname{Ker} \varphi_u$. Comme φ_u est un morphisme d'anneaux, son noyau N_u est un idéal de $K[X]$. En tant que K-espaces vectoriels, $K[X]$ n'est pas de dimension finie alors que $\operatorname{End} E$ est de dimension n^2, donc φ_u n'est pas injectif, et donc l'idéal N_u n'est pas nul. La preuve est identique pour une matrice A. □

7.2.2 Proposition et définition.

(i) *Pour tout endomorphisme $u \in \operatorname{End} E$, il existe un unique polynôme unitaire $Q_u \in K[X]$ tel que N_u soit l'idéal principal engendré par Q_u dans $K[X]$. Le polynôme unitaire Q_u est appelé le polynôme minimal de l'endomorphisme u.*

(ii) *Pour toute matrice $A \in \mathcal{M}_n(K)$, il existe un unique polynôme unitaire $Q_A \in K[X]$ tel que N_A soit l'idéal principal engendré par Q_A dans $K[X]$. Le polynôme unitaire Q_A est appelé le polynôme minimal de la matrice A.*

Preuve. Comme K est un corps, l'anneau $K[X]$ est principal, donc l'idéal N_u est principal non nul. D'après 5.2.2 et 5.2.4.(b), il existe un unique polynôme unitaire Q_u tel que $N_u = Q_u K[X]$. La preuve est identique pour une matrice A. □

7.2.3 Remarques

(1) Tout endomorphisme u de E annule son polynôme minimal Q_u, et un polynôme $P \in K[X]$ est annulé par u si et seulement s'il est multiple dans $K[X]$ du polynôme minimal Q_u de u :

$$\begin{cases} Q_u(u) = O, \\ \text{et} \\ \text{pour tout } P \in K[X],\ (P(u) = O) \Leftrightarrow (\text{ il existe } R \in K[X] \text{ tel que } P = RQ_u), \end{cases}$$

avec une formulation analogue en termes de matrices.

(2) Pour tout choix d'une base de E, si l'on a $u \in \operatorname{End} E$ et $A \in \mathcal{M}_n(K)$ avec $m(u) = A$, alors $N_u = N_A$ et $Q_u = Q_A$ d'après la dernière remarque de 7.1.4.

Exemples.

(1) Soient F et H deux sous-espaces vectoriels non nuls de E tels que $E = F \oplus H$. Soit s la symétrie par rapport à F parallèlement à H. On sait que l'on a $s \circ s = \mathrm{id}_E$ dans $\operatorname{End} E$, donc s annule $X^2 - 1$, d'où $X^2 - 1 \in N_s$, et donc Q_s divise $X^2 - 1$. Mais ici $s \neq \mathrm{id}_E$ puisque $H \neq \{0_E\}$ et $s \neq -\mathrm{id}_E$ puisque $F \neq \{0_E\}$, d'où $X - 1 \notin N_s$ et $X + 1 \notin N_s$, et donc Q_s ne divise pas $X - 1$ ni $X + 1$. On conclut que *le polynôme minimal de la symétrie s est* $Q_s = X^2 - 1$.

(2) En supposant toujours que $E = F \oplus H$ avec F et H non nuls, et en considérant cette fois la projection p de E sur F parallèlement à H, qui vérifie $p \circ p = p$, $p \neq \mathrm{id}_E$ et $p \neq O$, on montre de même que *le polynôme minimal de la projection p est* $Q_p = X^2 - X$.

(3) Si u est un endomorphisme nilpotent d'ordre p (ie. $u^p = O$ et $u^k \neq O$ pour $1 \leq k \leq p - 1$), alors le polynôme minimal de u est X^p. (On peut montrer que nécessairement $p \leq \dim E$).

7.3 Polynôme minimal et valeurs propres

Quelques rappels d'algèbre linéaire. Soit u un endomorphisme de E.

Une *valeur propre* de u dans K est un scalaire $\lambda \in K$ tel qu'il existe un vecteur $x \in E$ non nul vérifiant $u(x) = \lambda.x$. Un tel vecteur non nul x est alors appelé un *vecteur propre* associé à la valeur propre λ.

Si λ est une valeur propre de u dans K, le sous-espace vectoriel $E_\lambda = \mathrm{Ker}(u - \lambda\,\mathrm{id}_E)$ de E est appelé le *sous-espace propre* associé à la valeur propre λ. C'est donc l'ensemble des vecteurs $x \in E$ tels que $u(x) = \lambda x$, c'est-à-dire l'ensemble des vecteurs propres associés à λ auquel on adjoint le vecteur nul 0_E.

On appelle *polynôme caractéristique* de u le polynôme $P_u = \det(u - X.\,\mathrm{id}_E) \in K[X]$. Son degré est égal à la dimension n de E. Les zéros de P_u dans K sont exactement les valeurs propres de u dans K. La multiplicité d'une valeur propre λ dans K est l'exposant avec lequel le facteur $(X - \lambda)$ apparaît dans la décomposition du polynôme P_u en produit de facteurs irréductibles dans $K[X]$.

7.3.1 Théorème. *Pour tout endomorphisme u de E :*

(i) *le polynôme caractéristique P_u est un multiple du polynôme minimal Q_u dans $K[X]$,*

(ii) *les zéros dans K du polynôme minimal Q_u sont exactement les valeurs propres de u dans K.*

Preuve. D'après le théorème de Cayley-Hamilton, u annule son polynôme caractéristique P_u, c'est-à-dire $P_u(u) = O$. Ceci signifie que P_u appartient à l'idéal d'annulation N_u de u. Comme N_u est l'idéal principal engendré par Q_u dans $K[X]$, il existe un polynôme R tel que $P_u = RQ_u$ dans $K[X]$, ce qui prouve (i).

Si $\lambda \in K$ un zéro de Q_u, on a $Q_u(\lambda) = 0$, donc $P_u(\lambda) = R(\lambda)Q_u(\lambda) = 0$, et donc λ est une valeur propre de u. Réciproquement, soit λ une valeur propre de u. Il existe donc un vecteur non nul x de E tel que $u(x) = \lambda.x$. En composant par u, on en déduit $u^2(x) = u(\lambda.x) = \lambda.u(x) = \lambda^2.x$, puis $u^3(x) = \lambda^3.x$ et finalement $u^j(x) = \lambda^j.x$ pour tout $j \geq 0$.

Posons $Q_u = X^m + \beta_{m-1}X^{m-1} + \cdots + \beta_1 X + \beta_0$, où $m = \deg Q_u \leq \deg P_u = n$ et où les β_i appartiennent à K. Par définition du polynôme minimal, $Q_u(u)$ est l'endomorphisme nul O de E. Donc :

$$\begin{aligned} 0_E = Q_u(u)(x) &= \left(u^m + \beta_{m-1}u^{m-1} + \cdots + \beta_1 u + \beta_0\,\mathrm{id}_E\right)(x) \\ &= u^m(x) + \beta_{m-1}u^{m-1}(x) + \cdots + \beta_1 u(x) + \beta_0 x = \lambda^m.x + \beta_{m-1}\lambda^{m-1}.x + \cdots + \beta_1\lambda.x + \beta_0.x \\ &= Q_u(\lambda).x. \end{aligned}$$

Comme le vecteur x est non nul, on conclut que $Q_u(\lambda)$ est nul dans K. □

7.3.2 Remarque. *P_u et Q_u ont exactement les mêmes zéros dans K, qui sont les valeurs propres de u dans K.* En outre, P_u étant un multiple de Q_u, on a pour toute valeur propre λ de u:

$$1 \;\leq\; \begin{pmatrix}\text{la multiplicité de } \lambda \text{ en}\\ \text{tant que zéro de } Q_u\end{pmatrix} \;\leq\; \begin{pmatrix}\text{la multiplicité de } \lambda \text{ en}\\ \text{tant que zéro de } P_u\end{pmatrix}.$$

Notons enfin que tout ce que l'on vient de formuler en termes de polynôme minimal et de valeurs propres d'un endomorphisme peut être exprimé de façon analogue en termes de polynôme minimal et de valeurs propres d'une matrice carrée.

Exemple. Si une matrice $A \in \mathcal{M}_5(K)$ vérifie $P_A = -(X-2)^3(X+1)^2$. A priori, Q_A peut valoir :

$$\begin{array}{ccccccc} & (X-2)(X+1), & \text{ou} & (X-2)^2(X+1), & \text{ou} & (X-2)^3(X+1), \\ \text{ou} & (X-2)(X+1)^2, & \text{ou} & (X-2)^2(X+1)^2, & \text{ou} & (X-2)^3(X+1)^2. \end{array}$$

Pour déterminer ce que vaut effectivement Q_A, on peut calculer successivement tous les produits matriciels correspondants $(A - 2I_5)(A + I_5)$, $(A - 2I_5)^2(A + I_5)$..., jusqu'à obtenir un produit nul (sachant que de toute façon $(A - 2I_5)^3(A + I_5)^2$ est nul d'après le théorème de Cayley-Hamilton). On conçoit que de tels calculs directs sont vite fastidieux, voire inextricables à la main pour des matrices un peu grandes. D'où l'importance d'arguments théoriques plus généraux.

7.4 Lemme des noyaux et diagonalisabilité

Remarquons tout d'abord que, bien qu'en général la loi $\circ$ ne soit pas commutative dans $\operatorname{End} E$, on a pour tout endomorphisme u de E et tous polynômes P et Q dans $K[X]$ les égalités :

$$P(u)\circ Q(u) = PQ(u) = QP(u) = Q(u)\circ P(u),$$

ceci étant directement lié au fait que les différentes puissance de u commutent entre elles.

7.4.1 Lemme fondamental (dit "lemme des noyaux").

Soit u un endomorphisme de E.

(i) *Soient P et Q deux polynômes premiers entre eux dans $K[X]$, alors on a :*

$$\operatorname{Ker}(P(u)\circ Q(u)) = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u).$$

(ii) *Soient plus généralement $m \geq 2$ un entier et $P_1, P_2, \ldots, P_m$ des polynômes deux à deux premiers entre eux dans $K[X]$, alors on a :*

$$\operatorname{Ker}\Big(P_1(u)\circ P_2(u)\circ\cdots\circ P_m(u)\Big) = \operatorname{Ker} P_1(u) \,\oplus\, \operatorname{Ker} P_2(u) \,\oplus\cdots\oplus\, \operatorname{Ker} P_m(u)$$

Preuve. Si $x \in \operatorname{Ker} Q(u)$, alors $Q(u)(x) = 0_E$, donc $P(u)\big(Q(u)(x)\big) = 0_E$, c'est-à-dire $(P(u)\circ Q(u))(x) = 0_E$, ou encore $(PQ)(u)(x) = 0_E$, c'est-à-dire $x \in \operatorname{Ker}(PQ)(u)$; ceci prouve que $\operatorname{Ker} Q(u) \subset \operatorname{Ker}(PQ)(u)$. On montre de même que $\operatorname{Ker} P(u) \subset \operatorname{Ker}(PQ)(u)$ en utilisant le fait que $P(u)\circ Q(u) = Q(u)\circ P(u)$. Ansi $\operatorname{Ker} P(u)$ et $\operatorname{Ker} Q(u)$ sont deux sous-espaces vectoriels de $\operatorname{Ker}(PQ)(u)$, d'où :

$$\operatorname{Ker} P(u) + \operatorname{Ker} Q(u) \subseteq \operatorname{Ker}(PQ)(u).$$

Pour la réciproque, utilisons le fait que P et Q sont premiers entre eux dans $K[X]$. Par le théorème de Bézout, il existe $H, G \in K[X]$ tels que $HP + GQ = 1$ dans $K[X]$. Donc $H(u)\circ P(u) + G(u)\circ Q(u) = \mathrm{id}_E$ dans $\operatorname{End} E$, et donc $x = H(u)(P(u)(x)) + G(u)(Q(u)(x))$ pour tout $x \in E$. Considérons un vecteur $x \in \operatorname{Ker}(PQ)(u)$. Il s'écrit comme on vient de le voir $x = y + z$ avec $y = H(u)(P(u)(x))$ et $z = G(u)(Q(u)(x))$. D'une part le vecteur y vérifie :

$$Q(u)(y) = (Q(u)\circ H(u)\circ P(u))(x) = (H(u)\circ P(u)\circ Q(u))(x) = H(u)\big((PQ)(u)(x)\big) = H(u)(0_E) = 0_E,$$

et donc $y \in \operatorname{Ker} Q(u)$. D'autre part, le vecteur z vérifie :

$$P(u)(z) = (P(u)\circ G(u)\circ Q(u))(x) = (G(u)\circ P(u)\circ Q(u))(x) = G(u)\big((PQ)(u)(x)\big) = G(u)(0_E) = 0_E,$$

et donc $z \in \operatorname{Ker} P(u)$. On a ainsi montré que $\operatorname{Ker}(PQ)(u) \subseteq \operatorname{Ker} P(u) + \operatorname{Ker} Q(u)$, et finalement :

$$\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) + \operatorname{Ker} Q(u).$$

Il reste à montrer que la somme est directe. Pour cela, considérons $x \in \operatorname{Ker} P(u) \cap \operatorname{Ker} Q(u)$. On a $P(u)(x) = 0_E$ donc $H(u)(P(u)(x)) = H(u)(0_E) = 0_E$. De même $G(u)(x) = 0_E$ donc $G(u)(Q(u)(x)) = G(u)(0_E) = 0_E$. D'où $x = H(u)(P(u)(x)) + G(u)(Q(u)(x)) = 0_E + 0_E = 0_E$. Ceci prouve que $\operatorname{Ker} P(u) \cap \operatorname{Ker} Q(u) = \{0_E\}$. On conclut que :

$$\operatorname{Ker}(PQ)(u) = \operatorname{Ker} P(u) \oplus \operatorname{Ker} Q(u).$$

L'assertion (i) étant établie, l'assertion (ii) s'en déduit par récurrence sur m. Le résultat est vrai pour $m = 2$; supposons-le vrai jusqu'à un rang $m-1$. Soient $P_1, P_2, \ldots, P_m \in K[X]$ que l'on suppose deux à deux premiers entre eux. Alors P_m est premier avec $Q = P_1P_2\ldots P_{m-1}$ (en effet, il existerait sinon un facteur irréductible R commun à la décomposition de P_m et à celle de Q ; R apparaîtrait nécessairement dans la décomposition d'un P_{j_0} où $1 \leq j_0 \leq m-1$, ce qui contredirait le fait que P_m est premier avec P_{j_0}). L'assertion (i) montre alors que $\operatorname{Ker}(P_1P_2\ldots P_m)(u) = \operatorname{Ker} Q(u) \oplus \operatorname{Ker} P_m(u)$, et l'hypothèse de récurrence impliquant que $\operatorname{Ker} Q(u) = \operatorname{Ker} P_1(u) \oplus \operatorname{Ker} P_2(u) \oplus \cdots \oplus \operatorname{Ker} P_{m-1}(u)$, le résultat voulu à l'ordre m est établi. □

7.4.2 Théorème. *Un endomorphisme u de E est diagonalisable sur K si et seulement s'il existe dans l'idéal d'annulation de u dans $K[X]$ un polynôme de la forme $F = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_p)$ où les éléments $\lambda_1, \lambda_2, \ldots, \lambda_p$ de K sont deux à deux distincts.*

Preuve. Supposons que u est diagonalisable. Rappelons que cela signifie que u admet des valeurs propres $\lambda_1, \lambda_2, \ldots, \lambda_s$ (supposées par notation deux à deux distinctes) telles que $E = E_1 \oplus E_2 \oplus \cdots \oplus E_s$, où $E_j = \mathrm{Ker}(u - \lambda_j.\,\mathrm{id}_E)$ est le sous-espace propre associé à λ_j, pour tout $1 \leq j \leq s$. Introduisons dans $K[X]$ les polynômes $F = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_s)$ et $G_i = F/(X-\lambda_i) = \prod_{j\neq i}(X-\lambda_j)$ pour tout $1 \leq i \leq s$. On a $F(u) = G_i(u)\circ(u-\lambda_i.\,\mathrm{id}_E)$. Donc $F(u)(x) = 0_E$ pour tout $x \in E_i$. Donc $F(u)(x) = 0_E$ pour tout $x \in E$ puisque E est somme directe des E_i. On conclut que $F(u)$ est l'endomorphisme nul, ce qui prouve le résultat voulu (avec $p = s$).

Réciproquement, supposons satisfaite la condition de l'énoncé. Les polynômes $(X - \lambda_i)$ sont deux à deux premiers entre eux dans $K[X]$. On applique le lemme des noyaux pour déduire que $E = \bigoplus_{i=1}^{p} \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)$, donc u est diagonalisable, ses sous-espaces propres étant ceux des $\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)$ qui ne sont pas nuls (leur nombre s peut être a priori $\leq p$). □

7.4.3 Corollaire. *Un endomorphisme u de E est diagonalisable sur K si et seulement si son polynôme minimal est de la forme $Q_u = (X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_s)$, où $\lambda_1, \lambda_2, \ldots, \lambda_s$ sont les valeurs propres distinctes de u dans K.*

Preuve. Découle immédiatement du théorème précédent, du théorème 7.3.1, et de la définition du polynôme minimal. □

7.5 *Complément* : sous-espaces caractéristiques

7.5.1 Définition. Soit u un endomorphisme de E. Soit λ une valeur propre de u dans K. On note q la multiplicité de λ. Rappelons que cela signifie que le polynôme caractéristique P_u est divisible dans $K[X]$ par $(X-\lambda)^q$, mais pas par $(X-\lambda)^{q+1}$. En outre, on sait que la multiplicité q est supérieure ou égale à la dimension du sous-espace propre E_λ, et que u est diagonalisable sur K si et seulement si ces deux entiers coïncident pour chacune des valeurs propres de u.

On définit le *sous-espace caractéristique* associé à la valeur propre λ, noté F_λ, comme le noyau de l'endomorphisme $(u - \lambda.\,\mathrm{id}_E)^q$. Il est clair que, pour toute valeur propre λ de u dans K, on a:

$$F_\lambda = \mathrm{Ker}(u-\lambda.\,\mathrm{id}_E)^q \quad \supseteq \quad E_\lambda = \mathrm{Ker}(u-\lambda.\,\mathrm{id}_E) \quad \neq \quad \{0_E\}.$$

7.5.2 Proposition. *Soient u un endomorphisme de E. Pour toute valeur propre λ de u dans K, la multiplicité q de λ et égale à la dimension du sous-espace caractéristique F_λ.*

Preuve. Par définition de q, le polynôme caractéristique de u est de la forme $P_u = (X-\lambda)^q F$ avec $F \in K[X]$ tel que $F(\lambda) \neq 0$. Introduisons le sous-espace vectoriel $H = \mathrm{Ker}\,F(u)$ de E. Les polynômes $(X-\lambda)^q$ et F étant premiers entre eux dans $K[X]$, il résulte du lemme des noyaux que $E = F_\lambda \oplus H$. Le sous-espace vectoriel H est stable par u ; en effet, si $x \in H$, alors $F(u)(x) = 0_E$, or $F(u)(u(x)) = u(F(u)(x)) = u(0_E) = 0_E$ donc $u(x) \in H$. De même F_λ est stable par u. On peut donc considérer la restriction v de u à F_λ et la restriction w de u à H, et l'on a (propriété classique du polynôme caractéristique, il suffit de choisir une base adaptée à la décomposition en somme directe et de faire la calcul des déterminants par blocs): $P_u = P_v P_w$ dans $K[X]$ (avec $P_w = 1$ dans le cas où $H = \{0_E\}$).

Notons $d = \dim F_\lambda$. Considérons $v' = v - \lambda.\,\mathrm{id}_{F_\lambda}$, qui est la restriction de $u - \lambda.\,\mathrm{id}_E$ à F_λ ; il est clair que c'est un endomorphisme nilpotent de F_λ, d'ordre $\leq q$, et donc $P_{v'} = (-1)^d X^d$, ce qui revient à dire que $P_v = (-1)^d(X-\lambda)^d$. Par ailleurs, par définition de H et de w, on a $F(w) = O$. Donc F est un multiple dans $K[X]$ du polynôme minimal Q_w de w. Comme $F(\lambda) \neq 0$, on a forcément $Q_w(\lambda) \neq 0$, ce qui prouve avec 7.3.1 que λ n'est pas une valeur propre de w, d'où $P_w(\lambda) \neq 0$. En résumé, $P_u = (-1)^d(X-\lambda)^d P_w$ avec $P_w(\lambda) \neq 0$, ce qui signifie que d est la multiplicité de la valeur propre λ. □

7.5.3 Données. On suppose que P_u se décompose sur K en produit de facteurs de degré 1 (c'est-à-dire que A est trigonalisable sur K, voir cours d'algèbre linéaire de deuxième année) ce qui est toujours possible si $K = \mathbb{C}$; on désigne par $\lambda_1, \lambda_2, \ldots, \lambda_s$ les valeurs propres *distinctes* de u dans K, on a donc :

$$P_u = (-1)^n (X-\lambda_1)^{q_1}(X-\lambda_2)^{q_2}\cdots(X-\lambda_s)^{q_s}, \quad n = \deg P_u = q_1+q_2+\cdots+q_s,$$
$$Q_u = \qquad (X-\lambda_1)^{p_1}(X-\lambda_2)^{p_2}\cdots(X-\lambda_s)^{p_s}, \quad m = \deg Q_u = p_1+p_2+\cdots+p_s,$$

avec $1 \leq p_i \leq q_i \leq n$ pour tout $1 \leq i \leq s$. De plus, pour tout $1 \leq i \leq s$, on note :

$E_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)$ le sous-espace propre associé à λ_i, qui vérifie $\dim E_i \leq q_i$,

$F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$ le sous-espace caractéristique associé à λ_i, qui vérifie $\dim F_i = q_i$.

7.5.4 Proposition. *Avec les notations précédentes, on a :*

(i) *E est somme directe des sous-espaces caractéristiques : $E = F_1 \oplus F_2 \oplus \cdots \oplus F_s$;*

(ii) *pour toute valeur propre λ_i de A, on a: $F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$.*

Preuve. D'après le théorème de Cayley-Hamilton, on a $P_u(u) = O$, donc $E = \mathrm{Ker}\, P_u(u)$. On applique alors le lemme des noyaux pour conclure que $E = \bigoplus_{i=1}^{s} \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$, ce qui prouve le point (i).

On a aussi $Q_u(u) = O$, donc de la même façon $E = \bigoplus_{i=1}^{s} \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$. Ainsi, en rappelant que $F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$ et en introduisant $H_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$ pour tout $1 \leq i \leq s$, on a $H_i \subseteq F_i$ puisque $p_i \leq q_i$, et $E = \bigoplus_{i=1}^{s} F_i = \bigoplus_{i=1}^{s} H_i$. On conclut que $F_i = H_i$ pour tout $1 \leq i \leq s$. □

7.5.5 Corollaire *Avec les notations précédentes, les conditions suivantes sont équivalentes:*

(i) *u est diagonalisable,*

(ii) *pour toute valeur propre λ_i de u, on a $F_i = E_i$,*

(iii) *pour toute valeur propre λ_i de u, on a $p_i = 1$,*

(iv) *le polynôme minimal de u n'a que des termes de degré 1 : $Q_u = (X-\lambda_1)\cdots(X-\lambda_s)$.*

Preuve. Il est clair que (iii) ⇔ (iv). Comme u diagonalisable signifie que $E = E_1 \oplus E_2 \oplus \cdots \oplus E_s$, et comme chaque E_i est inclus dans F_i, l'équivalence (i) ⇔ (ii) résulte du point (i) de la proposition précédente. L'implication (iii) ⇒ (ii) résulte du point (ii) de la proposition précédente. La réciproque (i) ⇒ (iv) découle de 7.4.2. □

7.5.6 Définition. Pour toute valeur propre λ_i de u, on appelle *suite des noyaux* associée à λ_i la suite croissante des sous-espaces vectoriels:

$$\underbrace{E_i}_{\dim = r_i} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E) \subseteq \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^2 \subseteq \cdots \subseteq \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i} = \underbrace{F_i}_{\dim = q_i}.$$

Cette suite est donc formée de q_i sous-espaces, mais d'après le point (ii) de la proposition 7.5.4, elle est stationnaire à partir de $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i} = \cdots = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i} = F_i$.

7.5.7 Lemme. *On reprend les hypothèses et données précédentes. Si pour un entier $\ell \geq 1$ on a $\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell+1} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell}$, alors $\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell}$ pour tout $s \geq \ell$.*

Preuve. On fait une récurrence sur s pour montrer que la propriété :

$$(P_s):\ \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{t} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell} \text{ pour tout } \ell \leq t \leq s$$

est vraie pour tout $s \geq \ell+1$. Elle l'est pour $s = \ell+1$ d'après l'hypothèse du lemme. Supposons par hypothèse de récurrence qu'il existe $s \geq \ell+1$ tel que P_s soit vérifiée. On a en particulier :

$$\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s-1}.$$

Soit $x \in \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s+1}$. On a : $(u-\lambda_i.\,\mathrm{id}_E)^{s}(u-\lambda_i.\,\mathrm{id}_E)(x) = (u-\lambda_i.\,\mathrm{id}_E)^{s+1}(x) = 0_E$, et donc $(u-\lambda_i.\,\mathrm{id}_E)(x) \in \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s}$. En appliquant l'égalité précédente, il en résulte que : $(u-\lambda_i.\,\mathrm{id}_E)(x) \in \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s-1}$, donc $(u-\lambda_i.\,\mathrm{id}_E)^{s}(x) = (u-\lambda_i.\,\mathrm{id}_E)^{s-1}(u-\lambda_i.\,\mathrm{id}_E)(x) = 0_E$, c'est-à-dire $x \in \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s}$. Ceci prouve que $\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s+1} \subset \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s}$. L'inclusion inverse étant évidente, on conclut que $\mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s+1} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u-\lambda_i.\,\mathrm{id}_E)^{\ell}$, ce qui montre (P_{s+1}) et achève la preuve du lemme. □

► **Premier exemple illustratif.** Soit $A = \begin{pmatrix} -4 & 1 & 0 & 1 \\ -2 & -1 & 0 & 1 \\ -12 & 6 & 3 & 1 \\ -2 & 1 & 0 & -1 \end{pmatrix}$. Soit u l'endomorphisme de $\mathbb{R}^4$ dont la matrice dans la base canonique est A. On calcule $P_u = P_A = (X-3)(X+2)^3$.

Par les méthodes habituelles, on détermine $E_1 = \mathrm{Ker}(u-3.\,\mathrm{id}_E)$ (on sait qu'il est de dimension 1) et $E_2 = \mathrm{Ker}(u+2.\,\mathrm{id}_E)$. On trouve que $\dim E_2 = 1$ ce qui, comme -2 est v.p. triple, prouve que A n'est pas diagonalisable. A priori, le polynôme minimal de A peut valoir :

$$(X-3)(X+2)^3, \text{ ou } (X-3)(X+2)^2, \text{ ou } (X-3)(X+2).$$

Mais ce dernier cas est exclu puisque A n'est pas diagonalisable (voir 7.5.5).

Donc $(A-3I_4)(A+2I_4)$ est non nulle. Comme par ailleurs on sait que $(A-3I_4)(A+2I_4)^3$ est nulle d'après le théorème de Cayley-Hamilton, c'est le calcul de $(A-3I_4)(A+2I_4)^2$ qui permet de trancher. On fait le calcul de ce produit matriciel :

$$\begin{pmatrix} -7 & 1 & 0 & 1 \\ -2 & -4 & 0 & 1 \\ -12 & 6 & 0 & 1 \\ -2 & 1 & 0 & -4 \end{pmatrix} \begin{pmatrix} -2 & 1 & 0 & 1 \\ -2 & 1 & 0 & 1 \\ -12 & 6 & 5 & 1 \\ -2 & 1 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} -7 & 1 & 0 & 1 \\ -2 & -4 & 0 & 1 \\ -12 & 6 & 0 & 1 \\ -2 & 1 & 0 & -4 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -50 & 25 & 25 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = O_4.$$

On trouve $(A-3I_4)(A+2I_4)^2 = O_4$; on conclut que le polynôme minimal est $Q_A = (X-3)(X+2)^2$.

► **Second exemple illustratif.** Soit $A = \begin{pmatrix} 1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 2 & -3 \end{pmatrix}$. Soit u l'endomorphisme de $\mathbb{R}^5$ dont la matrice dans la base canonique est A. On calcule $P_u = P_A = -(X-1)^3(X+1)^2$.

On détermine les sous-espaces propres; on obtient :

$\lambda_1 = 1$, $\quad E_1 = \mathrm{Ker}(u-\mathrm{id}_E)$, de dimension $r_1 = 2$ [une base est (e_1, e_2+e_3)];

$\lambda_2 = -1$, $\quad E_2 = \mathrm{Ker}(u+\mathrm{id}_E)$, de dimension $r_2 = 1$ [une base est $(e_1+e_2+e_3-2e_4-2e_5)$].

Donc A n'est pas diagonalisable. En particulier, $Q_A \neq (X+1)(X-1)$.

On forme la suite des noyaux :

$E_1 = \mathrm{Ker}(u-\mathrm{id}_E) \subseteq \mathrm{Ker}(u-\mathrm{id}_E)^2 \subseteq \mathrm{Ker}(u-\mathrm{id}_E)^3 = F_1$, avec $\dim E_1 = r_1 = 2$ et $\dim F_1 = q_1 = 3$,

$E_2 = \mathrm{Ker}(u+\mathrm{id}_E) \subseteq \mathrm{Ker}(u+\mathrm{id}_E)^2 = F_2$, avec $\dim E_2 = r_2 = 1$ et $\dim F_2 = q_2 = 2$.

Le seul noyau à déterminer est $\mathrm{Ker}(u-\mathrm{id}_E)^2$ qui, au vu des dimensions, est égal à E_1 ou à F_1. Pour trancher, on peut faire la calcul direct de $(A-I_5)^2$. On peut aussi sans calcul utiliser le lemme 7.5.7: si l'on avait $\mathrm{Ker}(u-\mathrm{id}_E) = \mathrm{Ker}(u-\mathrm{id}_E)^2$, on aurait aussi $\mathrm{Ker}(u-\mathrm{id}_E) = \mathrm{Ker}(u-\mathrm{id}_E)^3$, c'est-à-dire $E_1 = F_1$, ce qui est absurde. Donc $\mathrm{Ker}(u-\mathrm{id}_E)^2 = F_1$.

En résumé :

$$\underbrace{E_1}_{r_1=2} = \operatorname{Ker}(u-\mathrm{id}_E) \subsetneq \operatorname{Ker}(u-\mathrm{id}_E)^2 = \operatorname{Ker}(u-\mathrm{id}_E)^3 = \underbrace{F_1}_{q_1=3},$$
$$\underbrace{E_2}_{r_2=1} = \operatorname{Ker}(u+\mathrm{id}_E) \subsetneq \operatorname{Ker}(u+\mathrm{id}_E)^2 = \underbrace{F_2}_{q_2=2}.$$

D'après le lemme des noyaux, $\operatorname{Ker}\big[(u-\mathrm{id}_E)\circ(u+\mathrm{id}_E)^2\big] = \operatorname{Ker}(u-\mathrm{id}_E) \oplus \operatorname{Ker}(u+\mathrm{id}_E)^2 = E_1 \oplus F_2$. Ce noyau est donc de dimension $r_1 + q_2 = 4 < 5$, de sorte que l'endomorphisme $(u-\mathrm{id}_E)\circ(u+\mathrm{id}_E)^2$ n'est pas nul, ou encore $(A-I_5)(A+I_5)^2 \neq O_5$.

De même, $\operatorname{Ker}\big[(u-\mathrm{id}_E)^2\circ(u+\mathrm{id}_E)\big] = \operatorname{Ker}(u-\mathrm{id}_E)^2 \oplus \operatorname{Ker}(u+\mathrm{id}_E) = F_1 \oplus E_2$ est de dimension $q_1+r_2 = 4 < 5$, de sorte que l'endomorphisme $(u-\mathrm{id}_E)^2\circ(u+\mathrm{id}_E)$ n'est pas nul, ou encore $(A-I_5)^2(A+I_5) \neq O_5$.

En revanche, $\operatorname{Ker}\big[(u-\mathrm{id}_E)^2\circ(u+\mathrm{id}_E)^2\big] = \operatorname{Ker}(u-\mathrm{id}_E)^2 \oplus \operatorname{Ker}(u+\mathrm{id}_E)^2 = F_1 \oplus F_2 = \mathbb{R}^5$, de sorte que l'endomorphisme $(u-\mathrm{id}_E)^2\circ(u+\mathrm{id}_E)^2$ est nul, c'est-à-dire $(A-I_5)^2(A+I_5)^2 = O_5$.

On conclut que le polynôme minimal est $Q_A = (X-1)^2(X+1)^2$.