Chapitre 4 : ANNEAUX ET CORPS

Dans les classes antérieures, on a étudié les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition et de la multiplication ordinaires. On a montré que $\mathbb{Z}$ possédait une structure d'anneau et que $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ possédaient une structure de corps.

Dans ce chapitre, nous nous proposons de décrire les structures d'anneau et de corps d'une manière générale mais nous ne donnons ici que quelques définitions et quelques résultats élémentaires de la théorie des anneaux et des corps.

4.1. Structure d'anneaux

4.1.1. DÉFINITIONS. EXEMPLES

4.1.1.1. Définition

On appelle **anneau** *un ensemble A muni de deux lois de composition internes : une addition $(x, y) \longmapsto x + y$ et une multiplication $(x, y) \longmapsto xy$, satisfaisant aux axiomes suivants :*

(A_1) *L'addition est une loi de groupe abélien.*

(A_2) *La multiplication est associative et admet un élément neutre, noté 1_A ou 1, et appelé* **élément unité.**

(A_3) *La multiplication est distributive par rapport à l'addition.*

Si de plus la multiplication est commutative, c'est-à-dire si on a $xy = yx$ quels que soient $x, y \in A$, on dit que l'anneau est **commutatif.**

Si A est un anneau quelconque, on dit que deux éléments x et y de A **commutent** ou sont **permutables** si l'on a $xy = yx$.

On appelle **pseudo-anneau,** un ensemble A muni d'une addition et d'une multiplication satisfaisant aux axiomes des anneaux mais tel que la multiplication n'ait pas d'élément neutre.

L'élément neutre pour l'addition dans un anneau A est noté 0 et est appelé **l'élément nul** de A.

4.1.1.2. Remarque

Certains auteurs appellent anneaux les objets que nous avons appelés pseudo-anneaux ; ils appellent anneaux unitaires, ou unifères, les triplets que nous appelons anneaux. Notre point de vue est justifié par le fait que tout pseudo-anneau peut être plongé dans un anneau avec élément unité.

4.1.1.3. Exemples

a) Munis de l'addition et de la multiplication ordinaires, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs.

b) Soit A un ensemble réduit à un seul élément, que l'on peut toujours noter 0 : $A = \{0\}$. Muni de l'addition $0 + 0 = 0$ et de la multiplication $0 \times 0 = 0$, A est un anneau qu'on appelle **l'anneau nul**. Dans cet anneau, on a : $1 = 0$.

Un anneau est dit **non nul** s'il n'est pas réduit à $\{0\}$.

Si A est un anneau non nul on note $A^* = A - \{0\}$.

4.1.1.4. Exemple

Soient A un anneau et E un ensemble non vide ; soit $\mathcal{F}(E, A)$ l'ensemble des applications de E dans A.
Pour $f, g \in \mathcal{F}(E, A)$, définissons la somme $f + g$ et le produit fg par les équations

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fg)(x) &= f(x)g(x)\end{aligned}$$

quel que soit $x \in E$.

Alors l'ensemble $\mathcal{F}(E, A)$, muni des deux lois de composition

$$(f, g) \longmapsto f + g \quad \text{et} \quad (f, g) \longmapsto fg$$

est un anneau (commutatif si et seulement si A est commutatif). L'élément unité de $\mathcal{F}(E, A)$ est l'application constante égale à 1.

4.1.1.5. Exemple

Soit G un groupe abélien non réduit à $\{0\}$ (noté additivement). L'ensemble $\mathrm{End}(G)$ des endomorphismes de G, muni des deux lois de composition

$$(f, g) \longmapsto f + g \quad \text{et} \quad (f, g) \longmapsto fog$$

définies par

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fog)(x) &= f\left(g(x)\right)\end{aligned}$$

pour tout $x \in G$, est un anneau en général non commutatif. L'élément unité de $\mathrm{End}(G)$ est l'application identique de G.

4.1.1.6. Exemple

Soient A et B deux anneaux. L'ensemble produit $A \times B$, muni des lois définies par :

$$\begin{aligned}(a, b) + (a', b') &= (a + a', b + b')\\ (a, b)(a', b') &= (aa', bb')\end{aligned}$$

quels que soient $a, a' \in A$ et $b, b' \in B$, est un anneau appelé **anneau produit** des anneaux A et B.

On vérifiera, à titre d'exercice, qu'on définit bien ainsi une structure d'anneau sur $A \times B$, l'élément unité étant (1,1).

De plus, l'anneau produit $A \times B$ est commutatif si et seulement si A et B le sont.

4.1.1.7. Exemple

Soit n un entier naturel > 0. Nous savons déjà, d'après l'Exemple 3.4.3.2, que $\mathbf{Z}/n\mathbf{Z}$ est un groupe abélien pour l'addition $(\overline{x}, \overline{y}) \longmapsto \overline{x} + \overline{y} = \overline{x+y}$. Montrons que $\mathbf{Z}/n\mathbf{Z}$ est un anneau commutatif. Pour cela, remarquons d'abord que la congruence modulo n est compatible avec la multiplication de $\mathbf{Z}$.

En effet, si x, y, x' et y' sont des nombres entiers relatifs tels que

$$x \equiv x' \pmod{n} \quad \text{et} \quad y \equiv y' \pmod{n},$$

il existe des éléments k et k' de $\mathbf{Z}$ tels que

$$x - x' = kn \quad \text{et} \quad y - y' = k'n.$$

On en tire $\qquad x = x' + kn, \qquad y = y' + k'n.$

D'où $\qquad xy = x'y' + n(ky' + k'x' + kk'n).$

On en déduit que $\qquad xy \equiv x'y' \pmod{n}.$

On peut donc définir une loi de composition interne dans $\mathbf{Z}/n\mathbf{Z}$, appelée multiplication, en posant :

$$\overline{x} \times \overline{y} = \overline{x \times y}.$$

Alors le groupe $\mathbf{Z}/n\mathbf{Z}$, muni de l'addition $(\overline{x}, \overline{y}) \longmapsto \overline{x} + \overline{y}$ et de la multiplication $(\overline{x}, \overline{y}) \longmapsto \overline{x} \times \overline{y}$ ainsi définies, est un anneau commutatif, l'élément unité étant $\overline{1}$ (à vérifier).

L'anneau ainsi défini s'appelle **l'anneau des entiers modulo** n.

Nous avons déjà dressé la table d'addition de $\mathbf{Z}/4\mathbf{Z}$. Dressons sa table de multiplication (la classe de n étant notée $\dot{n}$).

	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$	$\dot{0}$	$\dot{1}$	$\dot{2}$	$\dot{3}$
$\dot{2}$	$\dot{0}$	$\dot{2}$	$\dot{0}$	$\dot{2}$
$\dot{3}$	$\dot{0}$	$\dot{3}$	$\dot{2}$	$\dot{1}$

4.1.2. RÈGLES DE CALCULS DANS UN ANNEAU

Soit A un anneau. Toutes les règles de calcul valables dans un groupe abélien s'appliquent évidemment au **groupe additif** de A qui est l'ensemble A considéré comme groupe abélien. Par exemple, l'**opposé** d'un élément $x \in A$ se note $-x$ et on note $x + (-y) = x - y$.

1° Pour tout élément x d'un anneau A, on a :

$$x \cdot 0 = 0 \cdot x = 0. \tag{4.1.2.1}$$

En effet, on a :

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

d'où puisque tout élément de A est régulier pour l'addition, $x \cdot 0 = 0$.

On montre de même que $0 \cdot x = 0$.

2° Pour tout $x \in A$ et tout $y \in A$, on a :

$$x(-y) = (-x)y = -(xy). \tag{4.1.2.2}$$

En effet, pour tout $y \in A$, on a $y + (-y) = 0$; donc

$$x\,(y + (-y)) = xy + x(-y) = x \cdot 0 = 0.$$

Par suite $x(-y)$ est l'opposé de xy.

On démontrerait de même que $(-x)y$ est l'opposé de xy.

On en déduit ;

$$(-x)\,(-y) = -\,((-x)y) = -\,(-(xy)) = xy. \tag{4.1.2.3}$$

Notons que si A n'est pas l'anneau nul, alors $1 \neq 0$. En effet, la relation (4.1.2.1) montre que s'il existe $x \in A$ tel que $x \neq 0$, alors $x \cdot 0 = 0 \neq x$, donc 0 ne peut être l'élément neutre de la multiplication. L'anneau nul est donc le seul anneau dans lequel on a : $1 = 0$.

3° Pour tout élément $x \in A$, on définit par récurrence sur l'entier $n \in \mathbb{N}$ les éléments x^n et $n \cdot x$, en posant :

$$x^0 = 1, \qquad x^n = x^{n-1} \cdot x$$

$$0 \cdot x = 0, \qquad n \cdot x = (n-1)x + x.$$

On a alors les propriétés suivantes que l'on vérifie aisément par récurrence :

$$x^m \cdot x^n = x^{m+n} \tag{4.1.2.4}$$

$$(m + n)x = m \cdot x + n \cdot x \tag{4.1.2.5}$$

quels que soient $m, n \in \mathbb{N}$ et $x \in A$.

4° Pour tout $x \in A$ et pour tout $n \in \mathbb{N}$, on a :

$$n \cdot x = (n \cdot 1)x = x \cdot (n \cdot 1). \tag{4.1.2.6}$$

Pour $n = 0$, les égalités sont vraies d'après (4.1.2.1) et la définition de $0 \cdot x$. Supposons (4.1.2.6) vraie pour l'entier n. On a

$$\begin{aligned}(n+1)\cdot x &= nx + x = (n\cdot 1)x + 1\cdot x = (n\cdot 1 + 1)x \\ &= (n\cdot 1 + 1\cdot 1)x = \big((n+1)\cdot 1\big)\, x.\end{aligned}$$

On montrerait de même que

$$(n+1)x = x\,\big((n+1)\cdot 1\big)\,.$$

Ces règles de calcul nous permettent de développer les produits de sommes d'éléments d'un anneau A en tenant compte de l'ordre des termes. Si A est commutatif, on peut procéder à des simplifications.

5° Formule du binôme

4.1.2.1. Théorème

Soit A un anneau et soient a et b deux éléments permutables de A. Pour tout entier $n \geq 1$, on a la formule dite du **binôme**:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k. \tag{4.1.2.7}$$

Démonstration. Raisonnons par récurrence sur n. Pour $n = 1$, le résultat est trivial car la formule se réduit alors à $(a+b)^1 = 1\cdot a + 1\cdot b$.

Supposons (4.1.2.7) vraie pour l'entier $n \geq 1$, et montrons qu'elle est vraie pour $n+1$. On a donc d'après l'hypothèse de récurrence

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

En multipliant cette relation par $a + b$, il vient:

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

Or, on montre facilement que, puisque a et b sont permutables, il en est de même de a^p et b^q quels que soient $p, q \in \mathbb{N}$.

Donc:

$$(a+b)^{n+1} = \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k=0}^{n} C_n^k a^{n-k} b^{k+1}.$$

Le coefficient de $a^{n+1-k}b^k$ dans le second membre de cette relation est

$$C_n^k + C_n^{k-1} = C_{n+1}^k \quad \text{pour } 1 \leq k \leq n.$$

Comme d'autre part

$$C_n^0 = C_{n+1}^0 = 1 \quad \text{et} \quad C_n^n = C_{n+1}^{n+1} = 1,$$

on obtient, après regroupements :

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k a^{n+1-k} b^k.$$

Donc (4.1.2.7) est vraie pour $n+1$, donc pour tout entier $n \geq 1$.

4.1.3. PROPRIÉTÉS ÉLÉMENTAIRES DES ANNEAUX

• **Diviseurs de zéro**

Soit A un anneau et soit $a \in A$. Alors nous savons que $a \cdot 0 = 0 \cdot a = 0$.

On voit ainsi que dans un anneau, le produit de deux facteurs est nul lorsque l'un des facteurs est nul. La réciproque est inexacte comme le montre l'exemple suivant.

4.1.3.1. Exemple

Prenons $A = \mathbb{R} \times \mathbb{R}$. Pour $(a,b) \in A$ et $(c,d) \in A$, posons :

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b)\,(c,d) = (ac, bd).$$

Alors A est un anneau commutatif, l'élément unité étant (1,1) et l'élément nul étant $0 = (0,0)$. On a $(1,0)\,(0,1) = (0,0) = 0$ et pourtant $(1,0) \neq 0$ et $(0,1) \neq 0$. Cette remarque permet de poser la définition suivante.

4.1.3.2. Définition

Soit A un anneau non réduit à $\{0\}$. On dit qu'un élément $a \in A$ est **un diviseur *de zéro* à gauche** (*resp.* **à droite**) *si $a \neq 0$ et s'il existe un élément non nul b de A tel que $ab = 0$ (resp. $ba = 0$).*

Si A est commutatif, les notions de diviseur de zéro à gauche et à droite coïncident.

Dire que a est un diviseur de zéro à gauche, revient à dire que $a \neq 0$ et que a n'est pas régulier à gauche pour la multiplication.

En effet, si a est non nul et est un diviseur de zéro à gauche, il existe b non nul dans A tel que $ab = 0$; alors la relation $ab = 0 = a.0$ montre que a n'est pas régulier à gauche pour la multiplication de A.

Réciproquement, si $ax = ay$ avec $x \neq y$, alors on a

$$a(x-y) = 0 \quad \text{avec} \quad x - y \neq 0 ;$$

a est un diviseur de zéro à gauche.

De même, a est un diviseur de zéro à droite si et seulement si $a \neq 0$ et n'est pas régulier à droite pour la multiplication de A.

4.1.3.3. Définition

On dit qu'un anneau A est **intègre** *ou est un* **anneau d'intégrité** *s'il est non nul, commutatif et s'il ne possède pas de diviseurs de zéro.*

Autrement dit l'anneau A est intègre si la relation $ab = 0$ implique $a = 0$ ou $b = 0$.

• Éléments nilpotents

4.1.3.4. Définition

Soit A un anneau. On dit qu'un élément $x \in A$ est **nilpotent** *s'il existe un entier $n \geq 1$ tel que $x^n = 0$.*

On notera que si A possède un élément nilpotent a non nul, alors A possède des diviseurs de zéro car alors $a \cdot a^{n-1} = 0 = a^{n-1} \cdot a$.

• Éléments inversibles

4.1.3.5. Définition

Soit A un anneau et soit $a \in A$. On dit que a est un élément **inversible** *de A si a possède un symétrique pour la multiplication.*

Nous noterons $A^\times$ l'ensemble des éléments inversibles de A.

4.1.3.6. Théorème

Soit A un anneau non nul. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la multiplication de A.

Démonstrations. D'après le Théorème 2.2.4.2 **d)**, si $x \in A^\times$ et $y \in A^\times$, alors $xy \in A^\times$; on peut donc définir sur $A^\times$ la multiplication $(x, y) \longmapsto xy$. La multiplication est associative dans $A^\times$ puisqu'elle l'est déjà dans A.

On a évidemment $1 \in A^\times$ et 1 est l'élément neutre pour la multiplication dans $A^\times$. Enfin si $a \in A^\times$, on a

$$aa^{-1} = a^{-1}a = 1,$$

ce qui montre que $a^{-1} \in A^\times$. Donc $A^\times$ est un groupe pour la multiplication.

L'ensemble $A^\times$, muni de la multiplication $(x, y) \longmapsto xy$ s'appelle le **groupe multiplicatif de l'anneau** A ou encore le **groupe des éléments inversibles de l'anneau** A.

Par exemple, dans l'anneau $\mathbf{Z}$ des entiers relatifs, on a $\mathbf{Z}^\times = \{-1, 1\}$.

4.2. Sous-anneaux. Idéaux. Anneaux quotients

4.2.1. SOUS-ANNEAUX

4.2.1.1. Définition

Soient A un anneau et B une partie non vide de A. On dit que B est un **sous-anneau** *de A si les conditions suivantes sont vérifiées :*

a) *B est un sous-groupe du groupe additif A.*

b) *Les relations $x \in B$ et $y \in B$ impliquent $xy \in B$.*

c) *L'élément unité 1 de A appartient à B.*

On vérifie facilement que l'ensemble B, muni des deux lois de composition

$$(x, y) \longmapsto x + y \quad \text{et} \quad (x, y) \longmapsto xy$$

induites par celles de A, est un anneau.

Le théorème suivant donne une caractérisation des sous-anneaux.

4.2.1.2. Théorème

Soient A un anneau et B une partie de A. Les conditions suivantes sont équivalentes :

a) *B est un sous-anneau de A.*

b) *$1 \in B$ et quels que soient $x, y \in B$, on a $x - y \in B$ et $xy \in B$.*

Démonstrations. Si B est un sous-anneau de A, il est clair que la condition **b)** est vérifiée.

Réciproquement, si la condition **b)** est vérifiée, $B \neq \emptyset$ car $1 \in B$ et B est un sous-groupe du groupe additif A (puisque les relations $x \in B$ et $y \in B$ entraînent $x - y \in B$). D'autre part, comme les relations $x \in B$ et $y \in B$ impliquent $xy \in B$, on voit que B est bien un sous-anneau de A.

On démontre aisément que toute intersection de sous-anneaux de A est un sous-anneau de A. On peut donc parler du plus petit sous-anneau contenant une partie non vide H de A ; c'est l'intersection de tous les sous-anneaux de A contenant H. On l'appelle le **sous-anneau engendré par** H.

4.2.1.3. Exemples

a) $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

b) Soit A un anneau ; A est un sous-anneau de A mais $\{0\}$ n'est pas un sous-anneau de A si $A \neq \{0\}$.

Nous allons introduire maintenant la notion d'idéal dont le rôle en théorie des anneaux est l'analogue de celui des sous-groupes distingués en théorie des groupes.

4.2.2. IDÉAUX

4.2.2.1. Définition

Soit A un anneau et I une partie de A. On dit que I est un **idéal à gauche** *(resp.* **à droite***) de A si :*

a) *I est un sous-groupe du groupe additif A.*

b) *Quel que soit $a \in A$ et quel que soit $x \in I$, on a $ax \in I$* (resp. $xa \in I$). *On dit que I est un* **idéal bilatère** *ou simplement un* **idéal** *de A si I est à la fois un idéal à gauche et un idéal à droite de A.*

Notons que dans un anneau commutatif, tous les idéaux sont bilatères.

4.2.2.2. Exemple

Dans tout anneau A, les sous-groupes triviaux A et $\{0\}$ sont des idéaux. Tout idéal de A autre que A et l'idéal nul $\{0\}$ s'appelle un **idéal propre** de A.

4.2.2.3. Exemple

Soit A un anneau et soit $a \in A$. Alors $Aa = \{xa : x \in A\}$ est un idéal à gauche de A. En effet, d'une part $Aa \neq \emptyset$ car $a = 1 \cdot a \in Aa$, et d'autre part si x et y appartiennent à Aa, il existe x' et y' dans A tels que $x = x'a$ et $y = y'a$, d'où :

$$x - y = (x' - y')a \in Aa ;$$

donc Aa est un sous-groupe du groupe additif A. Enfin pour tout $z \in A$, on a :

$$zx = z(x'a) = (zx')a \in Aa$$

et la condition **b)** de la définition d'un idéal est vérifiée.

De même aA est un idéal à droite de A.

Désormais, lorsqu'on parlera d'idéal sans préciser, il s'agira toujours d'idéal bilatère.

4.2.2.4. Définition

Soit I un idéal de l'anneau A. On dit que I est un **idéal maximal** *si $I \neq A$ et si, pour tout idéal J différent de I, $I \subset J$ implique $J = A$.*

4.2.2.5. Remarques

a) Si I est un idéal de l'anneau A et si $1 \in I$, alors $I = A$. En effet, quel que soit $a \in A$, on a $1 \cdot a = a \in I$, donc $A \subset I$. Comme on a toujours $I \subset A$, alors $I = A$.

b) Si I est un idéal propre de l'anneau A, aucun élément de I n'est inversible. En effet, s'il existe $a \in I$ tel que a^{-1} existe, alors $a^{-1}a = 1 \in I$, et $I = A$ d'après **a)** ce qui est contraire à l'hypothèse, donc a n'est pas inversible.

4.2.2.6. Théorème

Soient A un anneau et $(I_\lambda)_{\lambda \in L}$ une famille d'idéaux à gauche (resp. à droite) de A. Alors $I = \bigcap_{\lambda \in L} I_\lambda$ est un idéal à gauche (resp. à droite) de A.

Démonstration. Supposons que $(I_\lambda)_{\lambda \in L}$ soit une famille d'idéaux à gauche de A. On sait déjà (Théorème 3.2.2.1) que I est un sous-groupe du groupe additif A. Soit $x \in I$; on a $x \in I_\lambda$ pour tout $\lambda \in L$. Comme I_λ est un idéal à gauche, on a $bx \in I_\lambda$ pour tout $b \in A$ et pour tout $\lambda \in L$, d'où $bx \in I$; donc I est un idéal à gauche de A.

On démontrerait de même que toute intersection d'idéaux à droite (resp. d'idéaux bilatères) de A est un idéal à droite (resp. bilatère) de A.

Soient A un anneau et X une partie de A. Il existe des idéaux à gauche de A contenant X (par exemple A lui-même). L'intersection de tous ces idéaux à gauche est un idéal à gauche de A contenant X et c'est le plus petit, au sens de l'inclusion. On l'appelle l'**idéal à gauche engendré par** X.

On définirait de même l'idéal à droite engendré par X et l'idéal bilatère engendré par X.

Par exemple, si a est un élément fixé de A, l'idéal à gauche engendré par a est l'ensemble

$$Aa = \{xa : x \in A\}.$$

Nous savons déjà que Aa est un idéal à gauche de A; cet idéal contient a car $a = 1 \cdot a \in Aa$. De plus, si I est un idéal à gauche de A contenant a, I contient xa pour tout $x \in A$; donc on a $Aa \subset I$ et par suite Aa est l'idéal à gauche engendré par a.

On montrerait de même que l'idéal à droite engendré par a est l'ensemble aA.

Plus généralement on démontrera le théorème suivant à titre d'exercice.

4.2.2.7. Théorème

Soient A un anneau et X une partie non vide de A. L'ensemble $\mathcal{J}$ des éléments x de A ayant la propriété suivante : il existe un entier $n > 0$, une suite $x_1, \ldots, x_n$ de n éléments de X et une suite $a_1, \ldots, a_n$ de n éléments de A tels que $x = a_1x_1 + \ldots + a_nx_n$ est l'idéal à gauche de A engendré par X.

4.2.2.8. Définition

Soit A un anneau. On dit qu'un idéal I de A est un **idéal principal** *s'il existe $a \in A$ tel que $I = Aa = aA$.*

On dit qu'un anneau A est **principal** *s'il est commutatif, intègre, et si tout idéal de A est principal.*

4.2.2.9. Exemple

Les idéaux de $\mathbb{Z}$ sont les ensembles de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$. On sait déjà que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$ (Exemple 3.2.1.6) et il est clair que si $a \in \mathbb{Z}$ et $x \in n\mathbb{Z}$, alors $ax \in n\mathbb{Z}$. Donc $\mathbb{Z}$ est un anneau principal.

4.2.3. ANNEAUX-QUOTIENTS

4.2.3.1. Théorème

Soient A un anneau et I un idéal bilatère de A. Alors la relation définie par $x\mathcal{R}y \iff x - y \in I$ est une relation d'équivalence sur A, compatible avec les deux lois de A. L'ensemble quotient, noté A/I, muni des deux lois quotients est un anneau appelé **anneau-quotient** *de A par I.*

Si, de plus, A est commutatif, l'anneau A/I est commutatif.

Démonstration. Comme I est un sous-groupe du groupe additif A, $\mathcal{R}$ est une relation d'équivalence (Théorème 3.4.2.3). On peut donc définir le groupe additif quotient A/I.

Montrons que la relation $\mathcal{R}$ est compatible avec la multiplication de A.

On doit démontrer que les relations $x - x' \in I$ et $y - y' \in I$ impliquent $xy - x'y' \in I$. Or si $x - x' = u \in I$ et $y - y' = v \in I$, on a :

$$x = x' + u \quad \text{et} \quad y = y' + v,$$

d'où

$$xy = x'y' + x'v + uy' + uv.$$

Comme I est un idéal, $x'v \in I$, $uy' \in I$ et $uv \in I$; on en déduit :

$$xy - x'y' = x'v + uy' + uv \in I.$$

On peut donc définir la loi quotient de la multiplication en posant

$$(x + I)\,(y + I) = xy + I$$

quels que soient $\dot{x} = x + I \in A/I$ et $\dot{y} = y + I \in A/I$.

Si A est commutatif, il est clair que cette multiplication de A/I est commutative.

On vérifie facilement que la multiplication de A/I est associative et distributive par rapport à l'addition de A/I. Donc A/I, muni des deux lois quotient, est un anneau.

Par exemple $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, est un anneau commutatif (voir l'Exemple 4.1.1.7) car $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

4.3. Morphismes d'anneaux

4.3.1. DÉFINITION ET PROPRIÉTÉS DES MORPHISMES D'ANNEAUX

4.3.1.1. Définition

Soient A et B deux anneaux. On dit qu'une application f de A dans B est un **morphisme** *ou un* **homomorphisme d'anneaux** *si :*

a) $f(1) = 1$.

b) $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)\, f(y)$ *quels que soient* $x, y \in A$.

On définit comme pour les groupes, les notions d'endomorphisme, d'isomorphisme et d'automorphisme d'anneaux.

Le **noyau** d'un morphisme d'anneaux est le noyau du morphisme des groupes sous-jacents $(A, +)$ et $(B, +)$.

Le noyau d'un homomorphisme d'anneaux f est noté $\mathrm{Ker}(f)$.

4.3.1.2. Exemple

Si I est un idéal bilatère d'un anneau A, l'application canonique $\pi : A \longrightarrow A/I$ est, par définition de l'anneau A/I, un morphisme d'anneaux. On l'appelle **l'homomorphisme canonique.**

4.3.1.3. Théorème

Soient A, B et C trois anneaux, f un morphisme de A dans B et g un morphisme de B dans C. Alors :

a) *gof est un morphisme de A dans C.*

b) *Si f est un isomorphisme de A sur B, l'application réciproque f^{-1} est un isomorphisme de B sur A.*

La démonstration est évidente et est laissée au lecteur.

4.3.1.4. Théorème

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

a) *$f(0) = 0$ et $f(-x) = -f(x)$ pour tout $x \in A$.*

b) *Si x est un élément inversible de A, on a $f(x^{-1}) = \big(f(x)\big)^{-1}$.*

c) *Si A' est un sous-anneau de A, $f(A')$ est un sous-anneau de B.*

d) *Si B' est un sous-anneau de B, $f^{-1}(B')$ est un sous-anneau de A.*

e) *Si I est un idéal de B, $f^{-1}(I)$ est un idéal de A, et f est injectif si et seulement si* $\mathrm{Ker}(f) = \{0\}$.

Démonstration. a) Puisque le morphisme d'anneaux $f : A \longrightarrow B$ possède les propriétés d'un morphisme de groupes abéliens, les propriétés du **a)** sont vérifiées.

b) se démontre comme le **b)** du Théorème 3.3.2.2.

c) On sait que $f(A')$ est un sous-groupe du groupe additif B. On a d'abord $1 \in f(A')$ car A' est un sous-anneau et f est un morphisme d'anneaux. Soient d'autre part $f(x)$ et $f(y)$ deux éléments de $f(A')$. On a $f(x)\ f(y) = f(xy) \in f(A')$; donc $f(A')$ est bien un sous-anneau de B.

d) Nous savons déjà que $f^{-1}(B')$ est un sous-groupe du groupe additif A (Théorème 3.3.2.2). On a $1 \in f^{-1}(B')$ car $f(1) = 1 \in B'$. Si $x \in f^{-1}(B')$ et $y \in f^{-1}(B')$, on a $f(x) \in B'$ et $f(y) \in B'$. D'où $f(xy) = f(x)\ f(y) \in B'$ car B' est un sous-anneau de B. Donc $xy \in f^{-1}(B')$ et $f^{-1}(B')$ est bien un sous-anneau de A.

e) I étant un sous-groupe du groupe additif B, $f^{-1}(I)$ est un sous-groupe du groupe additif A d'après le Théorème 3.3.2.2. Soient $a \in A$ et $x \in f^{-1}(I)$. Les relations $f(a) \in B$ et $f(x) \in I$ impliquent

$$f(ax) = f(a)\ f(x) \in I \quad \text{et} \quad f(xa) = f(x)\ f(a) \in I$$

puisque I est un idéal de B. Donc $ax \in f^{-1}(I)$ et $xa \in f^{-1}(I)$, ce qui prouve que $f^{-1}(I)$ est un idéal de A.

En particulier, $\mathrm{Ker}(f) = f^{-1}(\{0\})$ est un idéal de A et d'après le Théorème 3.3.2.4, f est injectif si et seulement si $\mathrm{Ker}(f) = \{0\}$.

4.3.2. DÉCOMPOSITION CANONIQUE D'UN MORPHISME D'ANNEAUX

Soient A et B deux anneaux et $f : A \longrightarrow B$ un morphisme d'anneaux. Considérons la relation d'équivalence $x\mathcal{R}y$ si et seulement si $f(x) = f(y) \iff f(x - y) = 0 \iff x - y \in \mathrm{Ker}(f)$. Comme $\mathrm{Ker}(f)$ est un idéal de A, on peut former l'anneau-quotient $A/\mathrm{Ker}(f)$. L'application canonique π de A sur $A/\mathrm{Ker}(f)$ est un homomorphisme d'anneaux (Exemple 4.3.1.2) ; l'injection canonique $j : f(A) \longrightarrow B$ est un homomorphisme d'anneaux. On peut montrer enfin comme pour les groupes, que la bijection $\overline{f}$ de $A/\mathrm{Ker}(f)$ sur $f(A)$ définie par $\overline{f}(\dot{x}) = f(x)$ où $x \in \dot{x}$ est un isomorphisme d'anneaux.

On peut donc énoncer :

4.3.2.1. Théorème

Soient $f : A \longrightarrow B$ un morphisme d'anneaux, π le morphisme canonique de A sur $A/\mathrm{Ker}(f)$ et j l'injection canonique de $f(A)$ dans B. Alors il existe un isomorphisme unique $\overline{f}$ de l'anneau-quotient $A/\mathrm{Ker}(f)$ sur le sous-anneau $f(A)$ de B tel que $f = j \circ \overline{f} \circ \pi$.

4.3.3. CARACTÉRISTIQUE D'UN ANNEAU

Soit A un anneau non nul. On vérifie immédiatement que l'application $f : \mathbf{Z} \longrightarrow A$ définie par

$$f(n) = n \cdot 1$$

pour tout $n \in \mathbf{Z}$ est un morphisme d'anneaux tel que $f(1) = 1$. Si g est un morphisme de $\mathbf{Z}$ dans A alors, $g(1) = 1$; on en déduit $g(n) = n \cdot 1$ pour tout $n \in \mathbf{Z}$, donc $g = f$. Il existe donc un morphisme unique f de $\mathbf{Z}$ dans A tel que $f(1) = 1$. Le noyau de f, qui est un idéal de $\mathbf{Z}$, est de la forme $p\mathbf{Z}$, pour un entier $p \in \mathbb{N}$

Ces considérations nous amènent à poser la définition suivante :

4.3.3.1. Définition

On appelle **caractéristique** *de l'anneau non nul A, l'entier $p \geq 0$ tel que $p\mathbf{Z}$ soit le noyau du morphisme $f : \mathbf{Z} \longrightarrow A$ défini par $f(n) = n \cdot 1$.*

D'après le Théorème 4.3.2.1, l'image $f(\mathbf{Z})$ de f est un sous-anneau de l'anneau A, isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Donc si le morphisme f est injectif, le seul entier p tel que $p \cdot 1 = 0$ est $p = 0$. On dit que l'anneau A est de **caractéristique nulle**. Dans ce cas, $f(\mathbf{Z})$ est isomorphe à $\mathbf{Z}$, donc A est un ensemble infini.

Si le morphisme f n'est pas injectif, il existe un plus petit entier $p > 0$ tel que $p \cdot 1 = 0$. On dit alors que l'anneau A est **de caractéristique** $p > 0$. Alors tout entier n tel que $n \cdot 1 = 0$ est un multiple de p et pour tout $a \in A$, on a $pa = (p \cdot 1)a = 0 \cdot a = 0$.

4.3.3.2. Exemples

a) Les anneaux $\mathbf{Z}$, $\mathbb{Q}$ $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.

b) Soit n un entier ≥ 2. La caractéristique de l'anneau $\mathbf{Z}/n\mathbf{Z}$ est n. En effet, on voit facilement par récurrence sur $m \in \mathbb{N}$, que $m\overline{x} = \overline{m}\,\overline{x}$ pour tout $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$. Donc pour tout $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$, on a $n\overline{x} = \overline{n}\,\overline{x} = \overline{0}\,\overline{x} = \overline{0 \cdot x} = \overline{0}$.

4.3.3.3. Théorème

Soit A un anneau d'intégrité et soit p sa caractéristique. Alors $p = 0$ ou p est un nombre premier.

Démonstration. Supposons $p > 0$. Si p n'est pas premier, on a $p = mn$ avec $0 < m < p$ et $0 < n < p$. Donc

$$0 = p \cdot 1 = (mn)1 = (m \cdot 1)\,(n \cdot 1).$$

Comme A est intègre, on a nécessairement $m \cdot 1 = 0$ ou $n \cdot 1 = 0$ ce qui contredit le fait que p est le plus petit entier positif tel que $p \cdot 1 = 0$. Donc p est un nombre premier.

4.4. Divisibilité dans un anneau

Dans ce paragraphe, nous considérons uniquement des anneaux commutatifs et intègres. Dans un tel anneau A l'idéal engendré par l'élément a de A est $aA = Aa$ et est noté (a).

Notre objectif principal est l'étude sommaire de la divisibilité dans un cadre plus général que celui déjà bien connu de l'anneau $\mathbf{Z}$.

4.4.1. GÉNÉRALITÉS

4.4.1.1. Définition

Soit A un anneau commutatif et intègre et soient a et b deux éléments de A. On dit que a **divise** *b ou que b est* **divisible** *par a, et on écrit $a|b$, s'il existe $q \in A$ tel que $b = aq$.*

On dit aussi que a est un **diviseur** *de b ou que b est un* **multiple** *de a.*

Par exemple, tout $a \in A$ est multiple de tout élément inversible u de A car $a = u(u^{-1}a)$ et tout $a \in A$ divise 0 car $0 = a \cdot 0$.

On dit que deux éléments a et b de l'anneau A sont **associés** s'il existe un élément inversible $u \in A$ tel que $b = au$. Alors $a = bv$ avec $v = u^{-1}$.

4.4.1.2. Définition

Soit A un anneau principal. On dit qu'un élément $p \neq 0$ de A est **premier** *ou* **irréductible** *ou* **extrémal** *s'il n'est pas inversible et si ses seuls diviseurs sont les éléments inversibles de A et les éléments qui lui sont associés.*

Dans $\mathbf{Z}$, un élément extrémal est appelé un **nombre premier.**

Le théorème suivant montre l'importance des idéaux principaux dans l'étude de la divisibilité.

4.4.1.3. Théorème

Soit A un anneau commutatif et intègre et soient a et b deux éléments de A. Alors :

a) *a divise b si et seulement si $(b) \subset (a)$.*

b) *$(a) = (b)$ si et seulement s'il existe un élément inversible u de A tel que $b = au$.*

Démonstration. a) Si $a|b$, il existe $q \in A$ tel que $b = aq$; alors pour tout $x \in A$, on a $bx = a(qx)$, donc $(b) \subset (a)$.

Réciproquement, si $(b) \subset (a)$, on a $b = b \cdot 1 \in aA$, donc $b \in aA$ et il existe $c \in A$ tel que $b = ac$, ce qui montre que $a|b$.

b) Si $(a) = (b)$, il existe $q, u \in A$ tels que $a = bq$ et $b = au$; d'où $b = bqu$. Si $b = 0$, $a = b = 0$ et $b = a \cdot 1$. Si $b \neq 0$, comme A est intègre, $qu = 1$ et u est inversible.

Réciproquement, s'il existe un élément inversible u de A tel que $b = au$, alors $a|b$, donc $(b) \subset (a)$. La relation $b = au$ implique $a = bu^{-1}$, donc $b|a$ et par suite $(a) \subset (b)$. Finalement, on a bien $(a) = (b)$.

Dans tout ce qui suit, lorsque nous dirons «soit A un anneau principal», il s'agira toujours d'anneau d'intégrité commutatif dans lequel tous les idéaux sont principaux. Nous nous proposons d'établir certaines propriétés arithmétiques des anneaux principaux ; le cas de l'anneau principal $\mathbf{Z}$ est déjà bien connu.

4.4.2. PLUS GRAND COMMUN DIVISEUR

Soit A un anneau principal et soient $a_1, ..., a_n$ des éléments non nuls de A. Nous nous proposons d'étudier les éléments p de A qui divisent chacun des a_i, c'est-à-dire les éléments p tels qu'il existe des éléments q_i de A vérifiant

$$a_i = pq_i \qquad (1 \leq i \leq n).$$

Il est clair que tout diviseur commun à $a_1, ..., a_n$ divise l'élément $a_1u_1 + ... + a_nu_n$ quels que soient les n éléments $u_1, ..., u_n$ de A. Cela nous conduit à étudier l'ensemble $\mathcal{J}$ des éléments de A de la forme

$$a_1u_1 + ... + a_nu_n \tag{4.4.2.1}$$

où $u_1, ..., u_n$ sont des éléments arbitraires de A.

4.4.2.1. Théorème

soit A un anneau principal et soient $a_1, ..., a_n$ des éléments non nuls de A. Alors

a) *Il existe un élément $d \in A$, unique à la multiplication près par un élément inversible de A, tel que l'ensemble des multiples de d dans A soit l'ensemble des éléments de la forme $z = a_1u_1 + ... + a_nu_n$.*

b) *Il existe des éléments $u_1, ..., u_n$ de A tels que*

$$d = a_1u_1 + ... + a_nu_n. \tag{4.4.2.2}$$

c) *Pour qu'un élément de A divise simultanément $a_1, ..., a_n$, il faut et suffit qu'il divise d.*

Démonstrations. a) Considérons l'ensemble $\mathcal{J}$ des élements de A de la forme

$$z = a_1u_1 + ... + a_nu_n$$

où $u_1, ..., u_n \in A$.

Il est clair que $\mathcal{J}$ est un idéal de A. C'est même l'idéal, noté $(a_1, ..., a_n)$, engendré par $a_1, ..., a_n$. Comme l'anneau A est principal, $\mathcal{J}$ est engendré par un élément d de A ; autrement dit, on a $\mathcal{J} = (d)$. L'unicité de d résulte du Théorème 4.4.1.3 **b)**.

b) Puisque $d \in (d)$, il existe $u_1, ..., u_n \in A$ tels que

$$d = a_1 u_1 + ... + a_n u_n.$$

c) Soit p un diviseur commun à $a_1, ..., a_n$. Écrivons

$$a_i = pq_i \qquad (1 \leq i \leq n).$$

En portant dans 4.4.2.2, il vient

$$d = p(q_1 u_1 + ... + q_n u_n)$$

ce qui montre que p divise d.

Réciproquement, soit c un diviseur de d. La relation $\mathcal{J} = (d)$ montre que l'idéal (d) contient les a_i qui sont donc des multiples de d; par suite c est un diviseur commun à $a_1, ..., a_n$.

4.4.2.2. Définition

On appelle **plus grand commun diviseur** (P.G.C.D.) *de* $a_1, ..., a_n$, *et on note* P.G.C.D. $(a_1, a_2, ..., a_n)$, *tout élément* d *de* A *tel que*

$$dA = a_1 A + ... + a_n A.$$

La relation 4.4.2.2 s'appelle l'**identité de Bezout.**

4.4.2.3. Définition

On dit que les éléments $a_1, ..., a_n$ *de* A *sont* **premiers entre eux dans leur ensemble** *s'ils admettent* 1 *pour* P.G.C.D.

On dit que les a_i *sont* **premiers entre eux deux à deux** *si* $\mathrm{PGCD}(a_i, a_j) = 1$ *pour tous les* i, j *tels que* $i \neq j$.

On remarque que si $n \geq 3$ et si $a_1, ..., a_n$ sont premiers entre eux deux à deux, ils sont premiers entre eux dans leur ensemble ; cependant si $a_1, ..., a_n$ sont premiers entre eux dans leur ensemble, ils ne sont pas nécessairement premiers entre eux deux à deux. Par exemple, dans $\mathbb{Z}$, les nombres 12, 15 et 16 sont premiers entre eux mais il ne sont pas premiers entre eux deux à deux puisque $\mathrm{PGCD}(12, 15) = 3$.

4.4.2.4. Théorème (Bezout)

Soient A un anneau principal et $a_1, ..., a_n$ des éléments de A. Les propriétés suivantes sont équivalentes :

a) *$a_1, ..., a_n$ sont premiers entre eux dans leur ensemble.*

b) *Il existe des éléments $u_1, ..., u_n$ de A tels que*

$$a_1 u_1 + ... + a_n u_n = 1.$$

Démonstration. a) $\Longrightarrow$ b) : Si $a_1, ..., a_n$ sont premiers entre eux dans leur ensemble, 1 est un PGCD de $a_1, ..., a_n$, donc un élément de l'idéal engendré par $a_1, ..., a_n$. Donc il existe $u_1, ..., u_n \in A$ tels qu'on ait

$$a_1 u_1 + ... + a_n u_n = 1.$$

b) $\Longrightarrow$ a) : S'il existe des éléments $u_1, ..., u_n$ de A tels que $a_1 u_1 + ... + a_n u_n = 1$, alors $1 \in (a_1, ..., a_n)$, donc $(a_1, ..., a_n) = A$ et par suite 1 est un PGCD de $a_1, ..., a_n$.

4.4.2.5. Corollaire

Soient a, b et c des éléments de l'anneau principal A. Si a est premier séparément avec b et c, alors il est premier avec le produit bc.

Démonstration. D'après l'identité de Bezout, il existe des éléments u_1, v_1, x, y de A tels que

$$au_1 + bv_1 = 1 \quad \text{et} \quad ax + cy = 1.$$

D'où, en multipliant membre à membre :

$$au + bcv = 1$$

avec $u = au_1 x + cu_1 y + bv_1 x$ et $v = v_1 y$, ce qui montre que a et bc sont premiers entre eux.

4.4.2.6. Théorème (Gauss)

Soient a et b des éléments non nuls de A et soit d un diviseur du produit ab. Si d est premier avec a, alors d divise b.

Démonstration. Si d et a sont premiers entre eux, il existe $u, v \in A$ tels que

$$du + av = 1.$$

En multipliant les deux membres de cette identité par b, il vient

$$bdu + abv = b;$$

puisque d divise à la fois bdu et ab (par hypothèse), il divise b.

4.4.2.7. Corollaire

Soient $b_1, ..., b_n$ des éléments de A premiers entre eux deux à deux. Si un élément a de A est divisible séparément par $b_1, ..., b_n$, alors a est divisible par le produit $b_1\ b_2 \ ...\ b_n$.

Démonstration. Il suffit de démontrer le résultat dans le cas où $n = 2$; le théorème s'obtient en faisant une récurrence facile sur n.

Par hypothèse, il existe $c_1 \in A$ tel que $a = b_1 c_1$; b_2, divisant $b_1 c_1$ et étant premier avec b_1, divise c_1. Il existe donc $c_2 \in A$ tel que $c_1 = b_2 c_2$; d'où $a = b_1 b_2 c_2$.

4.4.3. PLUS PETIT COMMUN MULTIPLE

Soient $a_1, ..., a_n$ des éléments non nuls de l'anneau principal A. Tout multiple de a_i est un élément de l'idéal (a_i) ; donc les multiples communs aux a_i sont les éléments de l'idéal $(a_1) \cap ... \cap (a_n)$. Cet idéal étant principal, il existe un élément m de A, unique à la multiplication près par un élément inversible quelconque de A, tel que

$$(a_1) \cap ... \cap (a_n) = (m) \tag{4.4.3.1}$$

et tout multiple commun aux a_i est un multiple de m.

On est ainsi amené à poser la définition suivante.

4.4.3.1. Définition

On appelle **plus petit commun multiple** (P.P.C.M.) *de $a_1, ..., a_n$, tout élément m de A tel que*

$$(a_1) \cap ... \cap (a_n) = (m).$$

4.4.3.2. Théorème

Soient A un anneau principal, a et b des éléments non nuls de A, d un P.G.C.D., *m un* P.P.C.M. *de a et b. Alors $ab = md$ à la multiplication près par un élément inversible.*

Démonstration. Posons $a = a'd$ et $b = b'd$; alors a' et b' sont premiers entre eux. En effet, il existe $u, v \in A$ tels que $au = bv = d$, d'où en simplifiant par d, la relation $a'u + b'v = 1$, qui montre que P.G.C.D.$(a', b') = 1$.

On peut écrire $a'b'd = ab' = a'b$, donc $a'b'd \in (m)$.

Réciproquement, en écrivant $m = xa$ et $m = yb$, on a: $xa = yb$ ou $xa'd = yb'd$. On en déduit $xa' = yb'$ puisque d est un élément non nul de l'anneau intègre A. Comme PG.C.D.$(a', b') = 1$, on peut écrire (Théorème de

Gauss), $x = zb'$, d'où $m = zb'a = za'b'd$. Donc $m \in (a'b'd)$ et par suite, on a $(m) = (a'b'd)$. D'après le Théorème 4.4.1.3**b)**, il existe un élément inversible u de A tel que $m = a'b'du$, d'où $md = a'b'dud = abu$.

4.5. Corps

4.5.1. DÉFINITIONS. PROPRIÉTÉS FONDAMENTALES

4.5.1.1. Définition

On appelle **corps** *tout anneau K non nul dans lequel tout élément non nul est inversible.*

On dit qu'un corps est **commutatif** si sa multiplication est commutative.

Ainsi pour un corps K on a, $K^\times = K^*$.

Si 1 est l'élément unité du groupe multiplicatif $K^\times$, alors 1 est l'élément unité de K. Ainsi un corps possède toujours au moins les deux éléments 0 et 1.

Les notions définies pour les anneaux (intégrité, morphisme, idéal, caractéristique) s'appliquent également aux corps qui sont des anneaux particuliers, mais certains résultats prendront ici des formes particulières.

4.5.1.2. Exemple

Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs de caractéristique 0.

4.5.1.3. Exemple

L'ensemble $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ muni de l'addition et de la multiplication ordinaires est un corps commutatif.

Dans un corps commutatif, on écrit souvent $xy^{-1} = y^{-1}x = x/y$. On vérifie facilement que toutes les règles de calculs habituelles dans $\mathbb{R}$ et $\mathbb{C}$ sont valables dans un corps commutatif.

Le résultat suivant fournit un exemple important de corps.

4.5.1.4. Théorème

a) *Soit $a \in \mathbb{Z}$. Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, l'élément $\overline{a}$ est inversible si et seulement si a et n son premiers entre eux.*

b) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*

Démonstration. a) On a les équivalences :
a inversible $\iff$ il existe $u \in \mathbb{Z}$ tel que $\overline{a}\,\overline{u} = \overline{1}$
$\iff au \equiv 1 \bmod(n)$
$\iff$ il existe $v \in \mathbb{Z}$ tel que $au - 1 = vn$ soit $au - vn = 1$, ce qui, d'après l'identité de Bezout, signifie que a et n sont premiers entre eux.

b) Rappelons que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Supposons que n soit premier et soit $p \in \mathbb{N}$ tel que $0 < p < n$; alors n et p sont premiers entre eux, donc d'après **a)**, $\overline{p}$ est inversible et $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Inversement, si $\mathbb{Z}/n\mathbb{Z}$ est un corps, tout élément $\overline{m}$ $(0 < m < n)$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible ; donc d'après **a)**, m et n sont premiers entre eux. n n'admet donc pas d'autres diviseurs positifs que 1 et lui-même. Donc n est un nombre premier.

4.5.1.5. Théorème

a) *Tout corps K est intègre.*

b) *Dans un corps K, tout élément non nul est régulier pour la multiplication de K.*

Démonstration. a) Soient $a, b \in K$ tels que $ab = 0$ et $a \neq 0$. Alors a^{-1} existe et $a^{-1} \in K$. La relation $ab = 0$ implique

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b.$$

b) On sait que $K^* = K - \{0\}$ est un groupe multiplicatif ; donc tout élément de K^* est régulier pour la multiplication de K d'après le Théorème 2.2.4.2.

4.5.1.6. Remarque

Le théorème 4.3.3.3 montre que la caractéristique d'un corps est, soit 0, soit un nombre premier.

4.5.2. SOUS-CORPS. IDÉAUX D'UN CORPS. MORPHISMES DE CORPS

4.5.2.1. Définition

Soit K un corps. On dit qu'une partie K' de K est un **sous-corps** *de K si :*

a) *K' est un sous-anneau de K.*

b) *Les relations $x \neq 0$ et $x \in K'$ impliquent $x^{-1} \in K'$.*

On vérifie alors que l'ensemble K', muni des lois de composition induites par celles de K est un corps. On dit aussi que K est un **sur-corps** ou une **extension** du sous-corps K'.

Par exemple $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$.

On montre facilement que toute intersection de sous-corps d'un corps K est un sous-corps de K ; on peut donc définir le sous-corps **engendré** par une partie A de K comme étant l'intersection de tous les sous-corps contenant A.

4.5.2.2. Théorème

Soit M un idéal d'un anneau commutatif A. Alors M est maximal si et seulement si l'anneau quotient A/M est un corps.

Démonstration. Supposons M maximal et soit a un élément de A n'appartenant pas à M. L'ensemble $aA + M$ est un idéal de A contenant M et différent de M ; donc $aA + M = A$. Alors, il existe un élément z de A et un élément m de M tels que $az + m = 1$. En prenant les classes modulo M, on obtient $\overline{az} = \overline{a}\,\overline{z} = \overline{1}$, ce qui montre que la classe de a est inversible dans A/M ; autrement dit l'anneau quotient A/M est un corps.

Réciproquement, supposons que A/M soit un corps. Soit I un idéal contenant M. Prenons un élément quelconque a de I, n'appartenant pas à M. La classe de a n'est pas la classe nulle et est donc inversible dans A/M. Il existe un élément u de A tel que $\overline{1} = \overline{a}\,\overline{u} = \overline{au}$, ou $\overline{1 - au} = \overline{0}$; donc $1 - au \in M$ et par suite $1 = (1 - au) + au \in I$. On en déduit que $I = A$ d'après la Remarque 4.2.2.5**a**). Donc l'idal I est maximal.

4.5.2.3. Théorème

Soit K un anneau commutatif non nul. Pour que K soit un corps il faut et il suffit que les seuls idéaux de K soient $\{0\}$ et K.

Démonstration. Supposons que K soit un corps et soit I un idéal de K distinct de $\{0\}$. Soit x un élément non nul de I. Comme K est un corps, x^{-1} existe et $x^{-1} \in K$; donc $x^{-1}x = 1 \in I$ puisque I est un idéal. Ainsi, pour tout $a \in K$, $1 \cdot a = a \in I$, ce qui prouve que $K \subset I$; donc $I = K$.

Réciproquement, supposons que les seuls idéaux de K soient $\{0\}$ et K. Soit a un élément non nul de K et considérons l'idéal principal (a) engendré par a :

$$(a) = \{ax : x \in K\}.$$

$(a) \neq \{0\}$ puisque $a = a.1 \in (a)$ et $a \neq 0$. On a donc nécessairement $(a) = K$. Comme $1 \in (a)$, il existe un élément $x \in K$ tel que $ax = xa = 1$; autrement dit x est l'inverse de a. Ainsi tout élément non nul de K est inversible dans K ; donc K est un corps.

Le théorème précédent est très utile dans l'étude des morphismes de corps.

4.5.2.4. Théorème

Soient K et K' deux corps commutatifs et $f : K \longrightarrow K'$ un morphisme de corps. Alors f est une application injective.

Démonstration. f étant un morphisme d'anneaux, $\mathrm{Ker}(f)$ est un idéal de K ; donc $\mathrm{Ker}(f) = \{0\}$ ou $\mathrm{Ker}(f) = K$. Si $\mathrm{Ker}(f) = K$, f est nulle, ce qui est impossible puisque $f(1) = 1 \neq 0 \in K'$; donc $\mathrm{Ker}(f) = \{0\}$ et par suite, f est injective.

4.5.3. CORPS DES FRACTIONS D'UN ANNEAU COMMUTATIF INTÈGRE

Étant donné un anneau commutatif et intègre A, nous nous proposons de trouver un corps commutatif K contenant A comme sous-anneau.

4.5.3.1. Définition

On dit qu'un corps K est un **corps des fractions** *de l'anneau intègre A si les deux conditions suivantes sont vérifiées :*

a) *A est un sous-anneau du corps K.*

b) *Pour tout $x \in K$, il existe dans A des éléments a et b tels que $x = ab^{-1}$.*

4.5.3.2. Théorème

Tout anneau commutatif intègre A admet un corps des fractions. Si K et L sont des corps des fractions de l'anneau A, alors K et L sont isomorphes.

Démonstration. Soit E l'ensemble des couples (p, q) où $p \in A$, $q \in A$ et $q \neq 0$. Sur E, la relation $\mathcal{R}$ définie par $(p, q)\mathcal{R}(p', q') \iff pq' = qp'$ est une relation d'équivalence.

Il est clair que la relation $\mathcal{R}$ est réflexive et symétrique. Montrons qu'elle est transitive.

Si $(p, q)\mathcal{R}(p', q')$ et $(p', q')\mathcal{R}(p'', q'')$, on a $pq' = qp'$ et $p'q'' = q'p''$, donc $pq'q'' = qp'q'' = qq'p''$. Comme A est intègre et $q' \neq 0$, on en déduit $pq'' = qp''$, donc $(p, q)\mathcal{R}(p'', q'')$. Ainsi $\mathcal{R}$ est bien une relation d'équivalence.

Soit K l'ensemble quotient $E/\mathcal{R}$; notons φ l'application canonique de E sur $E/\mathcal{R}$.

On définit deux lois internes sur E en posant :

Addition : $\quad (p, q) + (r, s) = (ps + qr, qs)$

Multiplication : $\quad (p, q) \cdot (r, s) = (pr, qs)$.

On vérifie sans peine que l'addition et la multiplication ainsi définies sont associatives, commutatives, admettent pour élément neutre (0,1) et (1,1) respectivement, et que la multiplication est distributive par rapport à l'addition.

On vérifie également qu'elles sont compatibles avec la relation d'équivalence $\mathcal{R}$; par exemple, pour l'addition si

$$(p, q)\mathcal{R}(p', q') \quad \text{et} \quad (r, s)\mathcal{R}(r', s')$$

la relation

$$\big((p, q) + (r, s)\big)\, \mathcal{R}\, \big((p', q') + (r', s')\big)$$

qui s'écrit

$$(ps + qr)q's' - (p's' + q'r')qs = 0$$

ou

$$ss'(pq' - p'q) + qq'(rs' - r's) = 0$$

est vérifiée.

Dans l'ensemble quotient notons encore $+$ et $\bullet$ les lois quotients. Ces lois sont associatives, commutatives et la multiplication est distributive par rapport à l'addition.

Pour l'addition, $\varphi(0,1)$ est l'élément neutre et $\varphi(-p,q)$ est l'opposé de $\varphi(p,q)$; donc $(K,+)$ est un groupe abélien.

Pour la multiplication, $\varphi(1,1)$ est l'élément neutre. Donc $(K,+,\bullet)$ est un anneau commutatif.

En outre, si $\varphi(p,q)$ est différent de $\varphi(0,1)$, c'est-à-dire si $p \neq 0$, $\varphi(p,q)$ admet pour inverse $\varphi(q,p)$. En conclusion $(K,+,\bullet)$ est un **corps commutatif.**

Considérons l'application $\psi : A \longrightarrow K$, définie par $\psi(x) = \varphi(x,1)$.

On a

$$\psi(x+y) = \varphi(x+y,1) = \varphi(x,1) + \varphi(y,1) = \psi(x) + \psi(y)$$

$$\psi(xy) = \varphi(xy,1) = \varphi(x,1) \cdot \varphi(y,1) = \psi(x)\,\psi(y)$$

$$\psi(1) = \varphi(1,1) = 1_K.$$

ψ est donc un morphisme d'anneaux. Ce morphisme est injectif car si $\varphi(x,1) = 0$, alors $x = 0$. Donc l'anneau A s'identifie au sous-anneau $\psi(A)$ de K, puisque ψ est un isomorphisme de A sur le sous-anneau $\psi(A)$ de K.

Supposons maintenant qu'il existe un corps L et un morphisme injectif $\theta : A \longrightarrow L$. La relation $(p,q)\mathcal{R}(p',q')$ qui s'écrit $pq' = p'q$ entraîne $\theta(p)\,\theta(q') = \theta(p')\,\theta(q)$. Comme $q \neq 0$ et $q' \neq 0$, on a $\theta(q) \neq 0$ et $\theta(q') \neq 0$ puisque θ est injectif ; ainsi $\theta(p)\,\theta(q)^{-1}$ ne change pas lorsqu'on remplace (p,q) par un autre représentant de $\varphi(p,q)$. Alors l'application $\varphi(p,q) \longmapsto \theta(p)\,\theta(q)^{-1}$ de K dans L est un morphisme injectif de corps.

Le corps K qui vient d'être construit répond donc à la question et c'est, à un isomorphisme près, le seul corps répondant à la question.

4.5.3.3. Remarque

Si l'on identifie A au sous-anneau $\psi(A)$ de K, ce qui revient à remplacer l'élément $\psi(p)$ de $\psi(A)$ par p, alors l'élément générique $\psi(p,q)$ de K prend la forme pq^{-1} que l'on écrit aussi p/q.

4.5.3.4. Remarque

Si l'on applique la construction du corps des fractions en partant de l'anneau $\mathbf{Z}$, on obtient le **corps $\mathbb{Q}$ des nombres rationnels.** Tout nombre rationnel s'écrit donc p/q, avec $p \in \mathbf{Z}$ et $q \in \mathbf{Z} - \{0\}$.

Nous étudierons au Chapitre 5 un autre exemple important des corps de fractions : le corps $K(X)$ des fractions rationnelles à une indéterminée à coefficients dans un anneau commutatif intègre K.

Chapitre 5 : POLYNÔMES ET FRACTIONS RATIONNELLES

Dans ce chapitre, nous nous proposons de définir, à partir d'un anneau commutatif K donné, un nouvel anneau commutatif noté $K[X]$ et contenant K comme sous-anneau. Cet anneau $K[X]$ possède de nombreuses «propriétés arithmétiques» de l'anneau $\mathbf{Z}$; nous étudierons quelques-unes de ces propriétés.

Les polynômes, c'est-à-dire les éléments de l'anneau $K[X]$ seront introduits comme expressions formelles.

Si K est un anneau commutatif intègre, nous verrons que l'anneau $K[X]$ est intègre; cet anneau n'est pas un corps mais il possède un corps des fractions. Si en particulier K est un corps commutatif, le corps des fractions de l'anneau $K[X]$ est appelé l'anneau des fractions rationnelles à une indéterminée à coefficients dans K. Ce corps sera étudié dans la deuxième partie.

Polynômes

5.1. Définitions générales

5.1.0.1. Définition

Soit K un anneau commutatif. On appelle **polynôme à une indéterminée à coefficients dans** K, *toute suite* $(a_0, a_1, \ldots,)$ *d'éléments de K nuls à partir d'un certain rang.*

Un tel polynôme est noté

$$P = (a_0, a_1, \ldots, a_n, \ldots) \quad \text{ou} \quad P = (a_n)_{n \in \mathbb{N}}.$$

Les a_n sont appelés les **coefficients** du polynôme P; on dit que a_n est le **coefficient d'indice** n; a_0 s'appelle le **terme constant.**

Si tous les coefficients a_n du polynôme P sont nuls, on dit que P est le **polynôme nul** et on le note 0. On appelle **monôme** un polynôme dont tous les coefficients sont nuls sauf, au plus, l'un d'entre eux.

L'ensemble des polynômes à une indéterminée à coefficients dans l'anneau commutatif K se note $K[X]$.

Étant donné un polynôme $P = (a_0, a_1, ..., a_n...)$ à coefficients dans K, on appelle **degré** de P, et on note $\deg(P)$, le plus grand entier n tel que $a_n \neq 0$. Cette définition s'applique à tout polynôme de $K[X]$ sauf au polynôme nul 0. En effet, tous les coefficients de 0 étant nuls, l'ensemble des indices des coefficients non nuls de 0 est vide, donc cet ensemble n'admet pas de plus grand élément.

De même, le plus petit entier k tel que $a_k \neq 0$ s'appelle la **valuation** du polynôme P et se note $\mathrm{val}(P)$. Tout polynôme P sauf 0 admet une valuation.

On convient de noter $\deg(0) = -\infty$ et $\mathrm{val}(0) = +\infty$ où les symboles $-\infty$ et $+\infty$ sont assujettis à vérifier les relations suivantes :

Pour tout $n \in \mathbf{Z}$, $\quad -\infty < n < +\infty$

Pour tout $n \in \mathbf{Z}$, $n + (+\infty) = +\infty ; n + (-\infty) = -\infty.$

$$(+\infty) + (+\infty) = +\infty ; \ (-\infty) + (-\infty) = -\infty.$$

Si P est un monôme non nul, c'est-à-dire si un seul coefficient a_n est non nul, alors $\deg(P) = \mathrm{val}(P) = n$.

5.1.0.2. Exemple

Prenons $K = \mathbf{Z}$ et $P = (0, 1, 0, 4, 0, 0, ...)$. On a $\deg(P) = 3$ et $\mathrm{val}(P) = 1$.

5.1.0.3. Définition

On dit que deux polynômes $P = (a_n)_{n \in \mathbb{N}}$ *et* $Q = (b_n)_{n \in \mathbb{N}}$ *de* $K[X]$ *sont* **égaux** *si pour tout entier* n, *on a* $a_n = b_n$.

En particulier P est le polynôme nul si et seulement si, pour tout entier n, $a_n = 0$.

5.2. Structure d'anneau de $K[X]$

Dans ce paragraphe K désigne un anneau commutatif sauf mention expresse du contraire.

5.2.1. ADDITION DE DEUX POLYNÔMES

5.2.1.1. Définition

Soient $P = (a_n)_{n \geq 0}$ *et* $Q = (b_n)_{n \geq 0}$ *deux polynômes de* $K[X]$. *On appelle* **somme** *de* P et Q, et on note $P + Q$, *le polynôme dont le coefficient d'indice* n *est égal à* $a_n + b_n$:

(5.2.1.1) $$P + Q = (a_0 + b_0, ..., a_n + b_n, ...).$$

5.2.1.2. Théorème

Le couple $(K[X], +)$ *est un groupe abélien.*

Démonstration. Comme $(K, +)$ est un groupe abélien, pour tout $n \in \mathbb{N}$, $a_n + b_n \in K$; donc $(a_0 + b_0, ..., a_n + b_n, ...)$ est une suite d'éléments de K. Si l'un des polynômes est nul, $P + Q$ est égal à l'autre polynôme, donc la suite $(a_n + b_n)_{n \geq 0}$ possède un nombre fini d'éléments non nuls et $P + Q \in K[X]$. Si aucun des polynômes n'est nul, soient n et m les degrés de P et Q respectivement ; si $k > \max(n, m)$, on aura $a_k = b_k = 0$, donc $a_k + b_k = 0$, ce qui montre que $P + Q \in K[X]$.

Les propriétés de l'addition dans $K[X]$ se déduisent facilement de celles de l'addition dans K. Ainsi, pour tout $n \in \mathbb{N}$, $(a_n + b_n) + c_n = a_n + (b_n + c_n)$, donc $(P + Q) + R = P + (Q + R)$ et pour tout $n \in \mathbb{N}$, $a_n + b_n = b_n + a_n$, donc $P + Q = Q + P$. Le polynôme 0 est l'élément neutre pour l'addition dans $K[X]$ et tout polynôme $P = (a_n)_{n \geq 0}$ a pour opposé le polynôme, noté $-P$, tel que $-P = (-a_n)_{n \geq 0}$.

5.2.1.3. Théorème

Posons $K[X]^* = K[X] - \{0\}$. *Alors si* $P, Q \in K[X]^*$ *et si* $Q \neq -P$, *on a*

$$\deg(P + Q) \leq \max\big(\deg(P), \deg(Q)\big) \tag{5.2.1.2}$$

$$\operatorname{val}(P + Q) \geq \min\big(\operatorname{val}(P), \operatorname{val}(Q)\big). \tag{5.2.1.3}$$

Démonstration. Il existe deux possibilités : $\deg(P) = \deg(Q)$ et $\deg(P) \neq \deg(Q)$.

1^er^ cas : $\deg(P) = \deg(Q) = n$.

• Si $a_n + b_n = 0$, alors $\deg(P + Q) < \deg(P)$, donc (5.2.1.2) est vraie, l'inégalité stricte ayant lieu.

• Si $a_n + b_n \neq 0$, alors $\deg(P + Q) = \deg(P) = \deg(Q)$, donc (5.2.1.2) est encore vraie, l'égalité ayant lieu dans ce cas.

2^e^ cas : $\deg(P) \neq \deg(Q)$. Supposons par exemple que $\deg(P) < \deg(Q)$. Alors, par définition du degré et de la somme, on a $\deg(P + Q) = \deg(Q) = \max\big(\deg(P), \deg(Q)\big)$. Donc (5.2.1.2) est vérifiée.

On démontrerait de même la relation (5.2.1.3), en raisonnant sur a_k et b_r, où $\operatorname{val}(P) = k$ et $\operatorname{val}(Q) = r$ et en considérant les deux cas $k = r$ et $k \neq r$.

5.2.2. MULTIPLICATION DE DEUX POLYNÔMES

5.2.2.1. Définition

Soient $P = (a_n)_{n \geq 0}$ *et* $Q = (b_n)_{n \geq 0}$ *deux polynômes de* $K[X]$. *On appelle* **produit** *de* P *et* Q, *et on note* PQ, *le polynôme dont le coefficient d'indice* n *est défini par :*

(5.2.2.1) $$c_n = \sum_{i+j=n} a_i b_j = \sum_{k=0}^{n} a_k b_{n-k}.$$

Montrons que l'on définit bien ainsi un polynôme à coefficients dans K. Si $a_i = 0$ pour $i > n_0$ et $b_j = 0$ pour $j > m_0$, on a $c_n = 0$ pour $n > n_0 + m_0$. En effet, si $n > n_0 + m_0$, dans chaque terme $a_i b_j$ de c_n, on a soit $i > n_0$ et alors $a_i = 0$, soit $j > m_0$ et alors $b_j = 0$; donc chaque terme de c_n est nul, et par suite $PQ \in K[X]$.

5.2.2.2. Théorème

Le triplet $(K[X], +, .)$ est un anneau commutatif.

Démonstration. Nous savons déjà que $(K[X], +)$ est un groupe abélien et que la multiplication est une loi interne sur $K[X]$. Il suffit donc de vérifier que la multiplication des polynômes est commutative, associative, distributive par rapport à l'addition et qu'elle admet un élément neutre.

Soit $1 = (1, 0, 0, \ldots)$ le polynôme constant dont tous les coefficients sont nuls sauf a_0 qui vaut 1. On vérifie facilement que pour tout $P \in K[X]$, $1 \cdot P = P \cdot 1 = P$, donc le polynôme 1 est l'élément unité de l'anneau $K[X]$.

Montrons que la multiplication est associative.

Soient $P = (a_n)_{n\geq 0}$, $Q = (b_n)_{n\geq 0}$ et $R = (c_n)_{n\geq 0}$ trois polynômes de $K[X]$.

On a

$$PQ = (d_n)_{n\geq 0} \quad \text{avec} \quad d_n = \sum_{i+j=n} a_i b_j$$

$$QR = (e_n)_{n\geq 0} \quad \text{avec} \quad e_n = \sum_{r+s=n} b_r c_s$$

Écrivons le terme u_n de rang n du produit $(PQ)R$:

$$\begin{aligned} u_n &= d_0 c_n + \ldots + d_k c_{n-k} + \ldots + d_n c_0 \\ &= a_0 b_0 c_n + (a_0 b_1 + a_1 b_0) c_{n-1} + \ldots + (a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0) c_0. \end{aligned}$$

De même le terme général v_n du produit $P(QR)$ est:

$$\begin{aligned} v_n &= a_0 e_n + \ldots + a_k e_{n-k} + \ldots + a_n c_0 \\ &= a_0 (b_0 c_n + b_1 c_{n-1} + \ldots + b_n c_0) + \ldots + a_n b_0 c_0. \end{aligned}$$

Si on utilise la distributivité de la multiplication par rapport à l'addition dans K et l'associativité de ces lois dans K, on trouve $u_n = v_n$ pour tout $n \in \mathbb{N}$. Donc les deux polynômes $(PQ)R$ et $P(QR)$ sont égaux.

On démontrerait par une méthode analogue que

$$P(Q + R) = PQ + PR \quad \text{et} \quad (Q + R)P = QP + RP.$$

5.2.2.3. Théorème

a) *L'anneau $K[X]$ est intègre si et seulement si l'anneau K est intègre.*

b) *Si $P, Q \in K[X]$, on a*

$$\deg(PQ) \leq \deg(P) + \deg(Q) \tag{5.2.2.2}$$

$$\mathrm{val}(PQ) \geq \mathrm{val}(P) + \mathrm{val}(Q) \tag{5.2.2.3}$$

Dans les relations (5.2.2.1) et (5.2.2.2) il y a égalité si l'anneau K est intègre.

Démonstration. a) Si l'anneau K possède des diviseurs de zéro, il existe des éléments $a \neq 0$ et $b \neq 0$ de K tels que $ab = 0$. Alors dans $K[X]$, on a

$$(a, 0, \ldots)\,(b, 0, \ldots) = (ab, 0, \ldots) = 0,$$

donc $K[X]$ possède des diviseurs de zéro.

Si au contraire K est intègre, montrons que $K[X]$ est intègre. Soient $P = (a_n)_{n\geq 0}$ et $Q = (b_n)_{n\geq 0}$ deux polynômes non nuls ; posons $k = \mathrm{val}(P)$ et $r = \mathrm{val}(Q)$.

$$P = (0, \ldots, 0, a_k, a_{k+1}, \ldots) \quad \text{avec } a_k \neq 0.$$

$$Q = (0, \ldots, 0, b_r, b_{r+1}, \ldots) \quad \text{avec } b_r \neq 0.$$

Alors par définition de la multiplication,

$$PQ = (0, \ldots, 0, a_k b_r, \ldots).$$

Comme K est intègre, les relations $a_k \neq 0$ et $b_r \neq 0$ impliquent $a_k b_r \neq 0$; donc $PQ \neq 0$.

b) Les inégalités sont évidentes si l'un des deux polynômes est nul. Écartons ce cas. Supposons que $\deg(P) = n$ et $\deg(Q) = m$. La formule (5.2.2.1) montre que $c_p = 0$ si $p > n + m$ et $c_{n+m} = a_n b_m$. Si l'anneau K possède des diviseurs de zéro, rien ne dit que $c_{n+m} \neq 0$. On a donc en général

$$\deg(PQ) \leq n + m = \deg(P) + \deg(Q).$$

Si l'anneau K est intègre, les relations $a_n \neq 0$ et $b_n \neq 0$ entraînent $c_{n+m} = a_n b_m \neq 0$. Donc

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

On démontrerait de même l'inégalité (5.2.2.3) en posant $\mathrm{val}(P) = k$ et $\mathrm{val}(Q) = r$ et en remarquant que le premier coefficient non nul de PQ est $a_k b_r$ si l'anneau K est intègre.

5.2.2.4. Théorème

Soit K un corps commutatif. Le groupe des éléments inversibles de l'anneau $K[X]$ est l'ensemble des polynômes de degré 0.

Démonstration. Si le polynôme $P \in K[X]$ est inversible et si Q est son inverse, on a $PQ = 1$; d'où $\deg(PQ) = \deg(P) + \deg(Q) = \deg(1) = 0$. Donc $\deg(P) = \deg(Q) = 0$, ce qui, par définition du degré, montre que P et Q sont de la forme

$$P = (a_0, 0, \ldots) \quad \text{et} \quad Q = (b_0, 0, \ldots).$$

Réciproquement dans $K[X]$, tout élément $\lambda \in K^*$ est inversible, son inverse étant le polynôme constant λ^{-1} (inverse de λ dans K).

5.3. Notation définitive

Dans ce paragraphe on désigne par K un anneau commutatif.

5.3.1. IMMERSION DE K DANS $K[X]$

Considérons l'application $f : a \longmapsto f(a) = (a, 0, \ldots)$ de K dans $K[X]$; elle est évidemment injective. C'est aussi un morphisme d'anneaux car les formules (5.2.1.1) et (5.2.2.1) montrent que

$$f(a + b) = f(a) + f(b), \qquad f(ab) = f(a)\, f(b)$$

et de plus,

$$f(0) = 0, \qquad f(1) = 1.$$

Par suite, f est un isomorphisme de K sur $f(K)$. On identifiera désormais, grâce à cet isomorphisme, tout élément de K avec son image dans $K[X]$ en posant, pour tout $a \in K$:

$$a = (a, 0, \ldots). \tag{5.3.1.1}$$

Si $\lambda \in K$ et si $P = (a_0, a_1, \ldots)$ est un polynôme, on a

$$\lambda P = (\lambda, 0, \ldots)\,(a_0, a_1, \ldots) = (\lambda a_0, \lambda a_1, \ldots). \tag{5.3.1.2}$$

On vérifie aisément que si $\lambda, \mu \in K$ et $P, Q \in K[X]$, alors

$$(\lambda + \mu)P = \lambda P + \mu P, \qquad \lambda(P + Q) = \lambda P + \lambda Q. \tag{5.3.1.3}$$

$$(\lambda\mu)P = \lambda(\mu P), \qquad 1 \cdot P = P. \tag{5.3.1.4}$$

On exprime ces propriétés en disant que $K[X]$, muni des opérations $(P, Q) \longmapsto P + Q$ et $(\lambda, P) \longmapsto \lambda P$ possède une structure de K-**module** (nous y reviendrons).

Remarquons en outre que, quels que soient $P, Q \in K[X]$ et quel que soit $\lambda \in K$, on a

$$\lambda(PQ) = (\lambda P)Q = P(\lambda Q). \tag{5.3.1.5}$$

5.3.2. NOTION D'INDÉTERMINÉE

5.3.2.1. Définition

On appelle **indéterminée** *le polynôme X dont tous les coefficients sont nuls, sauf le coefficient d'indice $1 \in \mathbb{N}$ qui est égal à $1 \in K$:*

$$X = (0, 1, 0, ...). \tag{5.3.2.1}$$

La formule (5.2.2.1) donne facilement

$$X^2 = (0, 0, 1, 0, ...)$$
$$X^3 = (0, 0, 0, 1, 0, ...)$$
$$- - - - - - - - - -$$
$$X^n = (0, 0, ..., 1, 0, ...)$$

où le coefficient 1 de X^n se trouve au $(n+1)^{\text{ème}}$ rang.

En utilisant la formule (5.3.1.2), on voit que pour tout $a_n \in K$,

$$a_n X^n = (0, ..., 0, a_n, 0, ...)$$

d'où, si $a_0, a_1, ...,$ sont des éléments de K et si $a_k = 0$ pour $k > n$,

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

Nous écrivons donc désormais le polynôme $P = (a_0, a_1, ...)$ de degré n sous la forme

$$a_0 + a_1 X + ... + a_n X^n = \sum_{k=0}^{n} a_k X^k. \tag{5.3.2.2}$$

Quand on écrit P sous la forme $a_0 + a_1 X + ... + a_n X^n$, on dit que P est **ordonné suivant les puissances croissantes de X** ; si on écrit: $P = a_n X^n + ... + a_0$, on dit que P est **ordonné suivant les puissances décroissantes de X**.

Le coefficient a_n est appelé **coefficient dominant** de P ; lorsque $a_n = 1$, on dit que le polynôme P est **unitaire** ou mieux **normalisé**.

Nous verrons plus tard que si K est un corps commutatif, alors $K[X]$ est un K-espace vectoriel ; de même si on désigne par $K_n[X]$ l'ensemble des polynômes à coefficients dans K de degré $\leq n$, $K_n[X]$ est un K-espace vectoriel dont une base est $(1, X, ..., X^n)$ (*cf.* Chapitre 6).

5.4. Propriétés arithmétiques de $K[X]$

Dans tout ce paragraphe, on désigne par K un corps commutatif. Nous allons étendre à $K[X]$ un certain nombre de propriétés de l'anneau $\mathbf{Z}$

5.4.1. DIVISION EUCLIDIENNE DANS $K[X]$

5.4.1.1. Définition

Soient A et B deux polynômes de $K[X]$. On dit que B **divise** *A, et l'on note $B|A$ s'il existe un polynôme Q de $K[X]$ tel que $A = BQ$.*

On dit aussi que A est un **multiple** *de B, ou que B est un* **diviseur** *de A. Q* s'appelle le **quotient** dans la division de A par B.

5.4.1.2. Remarques

a) Si A et B sont des polynômes non nuls et si B divise A, on a nécessairement $\deg(B) \leq \deg(A)$; si de plus $\deg(B) = \deg(A)$, alors la relation $A = BQ$ donne $\deg(B) = \deg(A) - \deg(B) = 0$, ce qui montre que Q est une constante non nulle de K. On dit que A et B sont **proportionnels ou associés.** Réciproquement, toute constante non nulle divise A.

b) La relation de divisibilité dans $K[X]$ est réflexive et transitive mais elle n'est ni symétrique, ni antisymétrique.

5.4.1.3. Théorème

Soient A et B deux polynômes de $K[X]$ tels que $B \neq 0$. Alors il existe un couple unique (Q, R) de polynômes de $K[X]$ tels que

$$A = BQ + R \quad \textit{avec} \quad \deg(R) < \deg(B). \tag{5.4.1.1}$$

Q s'appelle le **quotient** *et R le* **reste** *de la* **division euclidienne** *de A par B. A s'appelle le* **dividende**, *B le* **diviseur.**

Démonstration. a) Existence d'une solution

Posons

$$A = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \quad \text{avec} \quad a_n \neq 0$$
$$B = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_0 \quad \text{avec} \quad b_m \neq 0.$$

Si $n < m$, alors on peut écrire $A = 0 . B + A$ avec $\deg(A) < \deg(B)$, donc $Q = 0$ et $R = A$ conviennent.

Supposons donc $n \geq m$. Posons

$$q_1 = \frac{a_n}{b_m} X^{n-m} \quad \text{et} \quad R_1 = A - Bq_1.$$

Comme Bq_1 admet $a_n X^n$ pour terme de plus haut degré, on a $\deg(R_1) < \deg(A)$.

Si $\deg(R_1) < \deg(B)$, on peut prendre $Q = q_1$ et $R = R_1$.

Si $\deg(R_1) \geq \deg(B)$, on répète sur le couple (R_1, B) ce qui vient d'être fait sur le couple (A, B) ; en désignant par q_2 le quotient du terme de plus haut degré de R_1 par $b_m X^m$, on effectue la différence

$$R_1 - Bq_2 = R_2 \quad \text{avec} \quad \deg(R_2) < \deg(R_1).$$

Si $\deg(R_2) < \deg(B)$, on peut écrire $A = Bq_1 + R_1 = Bq_1 + Bq_2 + R_2 = B(q_1+q_2)+R_2$ avec $\deg(R_2) < \deg(B)$; donc on peut prendre comme solution $Q = q_1 + q_2$ et $R = R_2$.

Si $\deg(R_2) \geq \deg(B)$, on continue le processus avec R_2 et B. En répétant ce processus on forme une suite de polynômes R_k tels que

$$\deg(A) > \deg(R_1) > \ldots > \deg(R_k) > \ldots$$

La suite des degrés des R_k étant décroissante et majorée, est nécessairement finie ; au bout d'un nombre fini d'itérations, on arrivera à une égalité de la forme.

$$R_{k-1} - Bq_k = R_k \quad \text{avec } \deg(R_k) < \deg(B).$$

Si on ajoute membre à membre les k égalités

$$A - Bq_1 = R_1, \quad R_1 - Bq_2 = R_2, \ldots, R_{k-1} - Bq_k = R_k,$$

on obtient :

$$A - B(q_1 + \ldots + q_k) = R_k.$$

On peut donc prendre $Q = q_1 + \ldots + q_k$ et $R = R_k$.

b) Unicité

Supposons qu'il existe un autre couple (Q_1, R_1) tel que $A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$. On en déduit $B(Q - Q_1) = R_1 - R$. Par conséquent,

$$\deg(R_1 - R) = \deg(B) + \deg(Q - Q_1). \tag{5.4.1.2}$$

Or puisque $\deg(R) < \deg(B)$ et $\deg(R_1) < \deg(B)$, on a

$$\deg(R_1 - R) \leq \max\big(\deg(R_1), \deg(R)\big) < \deg(B). \tag{5.4.1.3}$$

Les deux relations (5.4.1.2) et (5.4.1.3) sont incompatibles si $\deg(Q - Q_1) \geq 0$ c'est-à-dire si $Q - Q_1 \neq 0$. Par suite $Q = Q_1$ et $R = R_1$ ce qui établit l'unicité et achève la démonstration du théorème.

5.4.1.4. Corollaire

Si $B \neq 0$, pour que le polynôme A soit divisible par le polynôme B, il faut et suffit que le reste de la division euclidienne de A par B soit nul.

5.4.1.5. Exemple

Diviser $A = X^4 + X^2 - 4X + 2$ par $B = X^2 + 2X + 1$.

Voici comment il faut disposer les calculs.

A	:	$X^4 \quad +X^2-4X+2$	X^2+2X+1	:	B
$-Bq_1$	:	$-X^4-2X^3-X^2$	X^2-2X+4	:	Q
R_1	:	$-2X^3 \qquad -4X+2$	$q_1 \quad q_2 \quad q_3$		
$-Bq_2$	:	$2X^3+4X^2+2X$			
R_2	:	$4X^2-2X+2$			
$-Bq_3$	:	$-4X^2-8X-4$			
R	:	$-10X-2$			

5.4.2. IDÉAUX DE $K[X]$

5.4.2.1. Théorème

L'anneau $K[X]$ est principal.

Démonstration. Nous savons déjà que $K[X]$ est un anneau commutatif et intègre ; il suffit donc de montrer que tout idéal I peut être engendré par un élément.

Si $I = \{0\}$, alors I est engendré par 0 et le théorème est évident. Supposons $I \neq \{0\}$. L'ensemble des degrés des éléments non nuls de I est une partie non vide de $\mathbb{N}$. Cet ensemble admet donc un plus petit élément que nous noterons n_0. Soit P un polynôme non nul de I tel que $\deg(P) = n_0$. Tout multiple de P appartient à I. Réciproquement, pour tout élément non nul A de I, on a $\deg(A) \geq \deg(P)$. La division euclidienne de A par P donne alors

$$A = PQ + R \quad \text{avec} \quad \deg(R) < \deg(P).$$

Des relations $A \in I$ et $P \in I$ on déduit $PQ \in I$ puis $R = A - PQ \in I$. Si $R \neq 0$, l'inégalité $\deg(R) < \deg(P)$ contredit le choix de P. Donc $R = 0$ et A est un multiple de P. L'idéal I est donc bien l'ensemble des multiples de P.

On notera (P) l'idéal engendré par le polynôme P.

5.4.2.2. Remarques

a) Le générateur P n'est pas unique car quel que soit $\lambda \in K^*$, $\lambda P \in I$ et a même degré que P.

b) Si A et B sont deux polynômes de $K[X]$ tels que $B \neq 0$, alors $B|A$ si et seulement si $(A) \subset (B)$.

Le Théorème 5.4.2.1 nous permet d'établir des propriétés qui, vraies dans tous les anneaux principaux, généralisent celles de $\mathbf{Z}$

5.4.3. PLUS GRAND COMMUN DIVISEUR

5.4.3.1. Théorème

Soient $A_1, ..., A_n$ des polynômes non nuls de $K[X]$. Alors :

a) *Tout diviseur commun à $A_1, ..., A_n$ divise le polynôme $A_1P_1 + ... + A_nP_n$ quels que soient les polynômes $P_1, ..., P_n$.*

b) *Il existe un polynôme D dans $K[X]$ tel que :*

1) *D divise chaque polynôme A_i.*

2) *Il existe des polynômes $U_1, ..., U_n$ de $K[X]$ tels que*

$$D = A_1U_1 + ... + A_nU_n, \tag{5.4.3.1}$$

et l'ensemble des diviseurs communs aux polynômes A_i est égal à l'ensemble des diviseurs de D.

Démonstration. a) Soit Q un diviseur commun à $A_1, ..., A_n$; il existe donc des polynômes $C_1, ..., C_n$ tels que $A_i = C_iQ$, $1 \leq i \leq n$. Alors

$$A_1P_1 + ... + A_nP_n = C_1QP_1 + ... + C_nQP_n = Q(C_1P_1 + ... + C_nP_n),$$

ce qui prouve **a)**.

b) Considérons l'ensemble I des polynômes de la forme $A_1P_1 + ... + A_nP_n$, où les P_i sont des polynômes quelconques de $K[X]$. I est évidemment un idéal de $K[X]$ contenant $A_1, ..., A_n$. I étant un idéal principal d'après le Théorème 5.4.2.1, il existe un polynôme D de I de degré minimum tel que I soit l'ensemble des multiples de D. Comme $A_i \in I$ pour tout i, on a $A_i = DQ_i$ et D divise chaque polynôme A_i. D'autre part, puisque $D \in I$, il existe des polynômes $U_1, ..., U_n$ tels que

$$D = A_1U_1 + ... + A_nU_n.$$

D'après **a)** tout polynôme qui divise chaque polynôme A_i divise D. Inversement tout diviseur de D divise tous les éléments de I (qui sont des multiples de D) et en particulier les polynômes $A_1, ..., A_n$.

Remarquons que le polynôme D n'est défini qu'à une constante multiplicative non nulle près. En effet, si D' est un autre polynôme vérifiant la condition **b)**, alors D divise D' et D' divise D, donc $D = \lambda D'$ avec $\lambda \in K^*$.

5.4.3.2. Définition

Avec les notations du Théorème 5.4.3.1, le polynôme D est appelé un **plus grand commun diviseur** (*en abrégé* P.G.C.D.) *des polynômes* $A_1, A_2, ..., A_n$ et se note P.G.C.D. $(A_1, ..., A_n)$.

*La relation (5.4.3.1) s'appelle l'***identité de Bezout.**

D est un diviseur commun à $A_1, ..., A_n$ de degré maximum, d'où son nom. Si on choisit D normalisé, on dit que D est **le** P.G.C.D. de $A_1, ..., A_n$.

5.4.3.3. Définition

On dit que les polynômes $A_1, ..., A_n$ **sont premiers entre eux dans leur ensemble** *si* P.G.C.D. $(A_1, ..., A_n) = 1$.

Il revient au même de dire que l'idéal engendré par les A_i dans $K[X]$ est $K[X]$ tout entier.

D'après la remarque précédant la Définition 5.4.3.2, la relation P.G.C.D. $(A_1, ..., A_n) = 1$ équivaut à P.G.C.D. $(A_1, ..., A_n) = \lambda$, où λ est un élément quelconque de K^*.

On dit que les polynômes $A_1, ..., A_n$ sont **premiers entre eux deux à deux** si P.G.C.D. $(A_i, A_j) = 1$ pour tous les indices i et j tels que $i \neq j$.

Il est évident que si $n \geq 3$ et si les polynômes $A_1, ..., A_n$ sont premiers entre eux deux à deux ils sont premiers entre eux dans leur ensemble. Mais si $A_1, ..., A_n$ sont premiers entre eux dans leur ensemble, ils ne sont pas nécessairement premiers entre eux deux à deux. En effet, dans $\mathbb{Q}[X]$, les trois polynômes $A = X(X+1)$, $B = X(X+2)$, $C = (X+1)(X+2)$ sont premiers entre eux dans leur ensemble mais ils ne sont pas premiers entre eux deux à deux puisque

$$\text{P.G.C.D. } (A, B) = X, \quad \text{P.G.C.D. } (B, C) = X+2, \quad \text{P.G.C.D. } (A, C) = X+1.$$

Recherche pratique du P.G.C.D. : Algorithme d'Euclide

Soient A et B deux polynômes de $K[X]$ et supposons que $\deg(B) \leq \deg(A)$. La division euclidienne de A par B donne $A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$.

Tout polynôme qui divise A et B divise B et $R_1 = A - BQ_1$. Réciproquement, tout polynôme qui divise B et R_1 divise $A = BQ_1 + R_1$ et B. Le calcul d'un P.G.C.D. de A et B est donc équivalent au calcul d'un P.G.C.D. de B et R_1.

1er cas : Si $R_1 = 0$, alors B est un P.G.C.D. de A et B.

2e cas : Si $R_1 \neq 0$, soit R_2 le reste de la division euclidienne de B par R_1. Si $R_2 = 0$, B est multiple de R_1 et R_1 est donc un P.G.C.D. de A et B. Si $R_2 \neq 0$ un P.G.C.D. de R_1 et R_2 est un P.G.C.D. de B et R_1 donc un P.G.C.D. de A et B, et ainsi de suite.

En effectuant la suite des divisions euclidiennes

$$\begin{aligned} A &= BQ_1 + R_1 && , \quad \deg(R_1) < \deg(B) \\ B &= R_1Q_2 + R_2 && , \quad \deg(R_2) < \deg(R_1) \\ R_1 &= R_2Q_3 + R_3 && , \quad \deg(R_3) < \deg(R_2) \\ &\text{- -} \\ R_{j-1} &= R_jQ_{j+1} + R_{j+1} && , \quad \deg(R_{j+1}) < \deg(R_j) \end{aligned}$$

on obtient nécessairement un reste $R_{h+1} = 0$, puisque les degrés des restes sont strictement décroissants. Le dernier reste précédant le reste nul est donc un P.G.C.D. de A et B.

Dans le cas de n polynômes $A_1, ..., A_n$, les communs diviseurs de A_1 et A_2 étant les diviseurs de leur plus grand commun diviseur D_2 nous avons

$$\text{P.G.C.D. } (A_1, ..., A_n) = \text{P.G.C.D. } (D_2, A_3, ..., A_n).$$

Les diviseurs communs de D_2 et A_3 étant les diviseurs de leur plus grand commun diviseur D_3, on a

$$\text{P.G.C.D. } (A_1, ..., A_n) = \text{P.G.C.D. } (D_3, A_4, ..., A_n).$$

De proche en proche, on voit que l'on peut ramener le calcul du P.G.C.D. de n polynômes au calcul du P.G.C.D. de deux polynômes.

Les propriétés démontrées au Chapitre 4 pour le P.G.C.D. dans un anneau principal restent valables dans l'anneau $K[X]$ et se démontrent de la même manière. Énonçons quelques propriétés du P.G.C.D. à titre d'exemples.

5.4.3.4. Théorème

Soient $A_1, ..., A_n$ des éléments de $K[X]$. Si on multiplie (resp. divise, si cela est possible) $A_1, ..., A_n$ par un même polynôme $P \neq 0$, le P.G.C.D. *de $A_1, ..., A_n$ est multiplié (resp. divisé) par P.*

Démonstration. Démontrons la propriété relative à la multiplication par P; l'autre propriété se démontre de la même manière.

Posons $D =$ P.G.C.D. $(A_1, ..., A_n)$. Il existe des polynômes $U_1, ..., U_n$ tels que

$$D = A_1U_1 + ... + A_nU_n.$$

Donc si un polynôme Q divise chacun des polynômes $A_1P, ..., A_nP$, il divise $A_1PU_1 + ... + A_nPU_n = (A_1U_1 + ... + A_nU_n)P = DP$. Réciproquement, DP divise chacun des polynômes $A_1P, ..., A_nP$; donc tout diviseur de DP est un diviseur de $A_1P, ..., A_nP$. On en déduit

$$\text{P.G.C.D. } (A_1P, ..., A_nP) = DP.$$

5.4.3.5. Théorème (Bezout)

Pour que les polynômes $A_1, A_2, ..., A_n$ de $K[X]$ soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe des polynômes $U_1, ..., U_n$ de $K[X]$ tels que

$$A_1U_1 + ... + A_nU_n = 1.$$

La démonstration est la même que celle du Théorème 4.4.2.4.

5.4.3.6. Corollaire

Soient A, B et C des polynômes de $K[X]$. Si A est premier séparément avec B et C, alors A est premier avec le produit BC.

Du Théorème de Bezout, on déduit également le théorème suivant connu sous le nom de Théorème de Gauss.

5.4.3.7. Théorème (Gauss)

Soient A, B et C des polynômes de $K[X]$. Si A divise le produit BC et si A est premier avec B, alors A divise C.

Même démonstration que celle du Théorème 4.4.2.6.

5.4.3.8. Corollaire

Soient $B_1, ..., B_n$ des polynômes de $K[X]$ premiers entre eux deux à deux. Si un polynôme A de $K[X]$ est divisible par chaque polynôme B_i, alors A est divisible par le produit $B_1 ... B_n$.

5.4.4. PLUS PETIT COMMUN MULTIPLE

Soient $A_1, A_2, ..., A_n$ des éléments non nuls de $K[X]$. Les multiples communs à $A_1, ..., A_n$ dans $K[X]$ sont les éléments de l'idéal $(A_1) \cap (A_2) \cap ... \cap (A_n)$. Cet idéal étant principal, il existe un élément M de $K[X]$, unique à la multiplication près par une constante non nulle, tel que

$$(A_1) \cap ... \cap (A_n) = (M)$$

et tout multiple commun à $A_1, A_2, ..., A_n$ est un multiple de M ; réciproquement tout multiple de M est un multiple commun à $A_1, ..., A_n$.

5.4.4.1. Définition

On appelle **plus petit commun multiple** (P.P.C.M.) *des polynômes $A_1, ..., A_n$, et on note* P.P.C.M. $(A_1, ..., A_n)$, *tout polynôme M de $K[X]$ tel que*

$$(A_1) \cap (A_2) \cap ... \cap (A_n) = (M).$$

Notons que M est un multiple commun à $A_1, ..., A_n$ de degré minimum, d'où son nom.

On a le résultat suivant qui ramène le calcul du P.P.C.M. de deux polynômes non nuls à celui de leur P.G.C.D. La démonstration est exactement la même que celle du Théorème 4.4.3.2.

5.4.4.2. Théorème

Soient A et B deux polynômes non nuls de $K[X]$, D un P.G.C.D., *M un* P.P.C.M. *de A et B. Alors $AB = MD$ (à une constante multiplicative non nulle près).*

5.4.5. POLYNÔMES IRRÉDUCTIBLES

5.4.5.1. Définition

On dit qu'un polynôme P de $K[X]$ est **premier ou irréductible** *sur le corps K s'il n'est pas constant et si ses seuls diviseurs dans $K[X]$ sont les polynômes associés à P et les éléments non nuls de K.*

Il faut bien noter que cette définition dépend essentiellement du corps K : il se peut très bien qu'un polynôme donné soit irréductible sur un corps et réductible sur un autre. Par exemple, $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais est réductible sur $\mathbb{C}$.

5.4.5.2. Remarque

Dire qu'un polynôme de $K[X]$ est irréductible revient à dire qu'il est impossible de l'écrire comme produit de deux polynômes de $K[X]$ de degrés positifs.

5.4.5.3. Exemple

Tout polynôme P de $K[X]$, du premier degré, est irréductible. Si en effet $P = AB$, avec $A \in K[X]$ et $B \in K[X]$, on a $1 = \deg(P) = \deg(A) + \deg(B)$ donc, nécessairement, l'un des polynômes A ou B est de degré 0 et l'autre de degré un.

5.4.5.4. Exemple

Le polynôme $X^2 - 2$ est irréductible sur $\mathbb{Q}[X]$. Si en effet $X^2 - 2$ n'était pas irréductible, on pourrait écrire

$$X^2 - 2 = (aX + b)(cX + d) = acX^2 + (ad + bc)X + bd$$

avec $a, b, c, d \in \mathbb{Q}$ et $a \neq 0$, $c \neq 0$. D'où

$$ac = 1, \quad ad + bc = 0, \quad bd = -2.$$

Il résulte de là que

$$c = \frac{1}{a}, \quad d = -\frac{2}{b}.$$

et en substituant dans $ad + bc = 0$, il vient $b^2 - 2a^2 = 0$, d'où $\left(\frac{b}{a}\right)^2 = 2$, ce qui est impossible puisque $\sqrt{2}$ n'est pas un nombre rationnel.

$X^2 - 2$ est réductible sur $\mathbb{R}$ car $X^2 - 2 = \left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)$.

5.4.5.5. Théorème

Soient P un polynôme irréductible de $K[X]$ et Q un polynôme de $K[X]$. Alors P et Q sont premiers entre eux si et seulement si P ne divise pas Q.

Démonstration. Si P et Q sont premiers entre eux, les seuls diviseurs communs à P et Q sont les constantes, donc P ne divise pas Q.

Réciproquement, si P ne divise pas Q, un P.G.C.D. de P et Q étant un diviseur de P ne peut être qu'une constante non nulle ou un polynôme associé à P. Le second cas étant exclu par hypothèse, la conclusion en résulte. □

5.4.5.6. Corollaire

Si un polynôme irréductible divise un produit de polynômes, il divise au moins l'un des facteurs.

Démonstration. Soit P un polynôme irréductible et supposons que P divise le produit AB sans diviser A. D'après le théorème précédent, P est premier avec A, donc (Théorème 5.4.3.7), P divise B.

Par récurrence, on démontrerait l'assertion lorsqu'on a un nombre fini quelconque de facteurs.

5.4.5.7. Théorème

Tout polynôme P non nul de $K[X]$ peut s'écrire d'une manière unique sous la forme

$$P = \lambda P_1 \ldots P_n \tag{5.4.5.1}$$

où λ est constante non nulle et où $P_1, \ldots, P_n$ sont des polynômes irréductibles normalisés.

Démonstration. Démontrons l'existence d'une factorisation de P par récurrence sur le degré de P.

Si $\deg(P) = 1$, le résultat est trivial car d'après l'Exemple 5.4.5.3, si $P = aX + b = a(X + a^{-1}b)$, $X + a^{-1}b$ est un polynôme irréductible normalisé.

Supposons le théorème établi pour les polynômes de degré inférieur à n. Soit P un polynôme de degré n. Alors, ou bien P est irréductible et le théorème est évident, ou bien P est décomposable en un produit de deux polynômes de degré inférieur à n : $P = Q_1 Q_2$ avec $\deg(Q_1) < n$, $\deg(Q_2 < n$.

En appliquant l'hypothèse de récurrence à Q_1 et à Q_2 on obtient une décomposition de P sous la forme (5.4.5.1) L'existence est établie.

Démontrons l'unicité de la décomposition. Supposons que

$$P = \lambda P_1 \dots P_n = \mu Q_1 \dots Q_m. \tag{5.4.5.2}$$

où λ et μ sont des constantes, et où les facteurs P_i et Q_j sont des polynômes irréductibles et normalisés. On a nécessairement $\lambda = \mu$ car chacune de ces constantes est le coefficient dominant de P. D'autre part, le polynôme irréductible P_1 divise le premier membre de l'égalité (5.4.5.2). Il divise donc le second membre et, d'après le Corollaire 5.4.5.8, il en divise l'un des facteurs. Appelons Q_1 ce facteur en changeant au besoin la numérotation des facteurs du second membre. Comme P_1 et Q_1 sont irréductibles et normalisés, on a $P_1 = Q_1$. Puisque $K[X]$ est intègre, on peut simplifier par P_1. En recommençant ce raisonnement avec P_2 puis avec P_3 et ainsi de suite, on pourra identifier les n facteurs du premier produit avec autant de facteurs du second. On en déduit $n \leq m$. On verrait de même que $m \leq n$, d'où $n = m$. Les deux décompositions sont donc ientiques à l'ordre près.

5.4.5.8. Remarque

Dans la décomposition de P, il est possible que certains polynômes premiers soient égaux. En regroupant les polynômes normalisés, on peut écrire

$$P = k\, P_1^{\alpha_1}\, P_2^{\alpha_2} \dots P_r^{\alpha_r} \tag{5.4.5.3}$$

$P_1, \dots, P_r$ désignant des polynômes irréductibles normalisés distincts et k une constante.

On dit que (5.4.5.3) est la **décomposition de P en facteurs irréductibles.**

5.5. Division suivant les puissances croissantes

K désigne toujours un corps commutatif. Nous présentons dans ce paragraphe la division suivant les puissances croissantes. Il s'agit, étant donnés deux polynômes A et B, de trouver un polynôme Q tel que val $(A - BQ)$ soit supérieure à un entier naturel fixé à l'avance.

5.5.0.1. Théorème

Soient n un entier naturel, A un polynôme quelconque et B un polynôme tel que $\text{val}(B) = 0$. *Il existe un couple unique (Q, R) de polynômes de $K[X]$ tels que*

$$A = BQ + X^{n+1}R \quad \textit{avec} \quad \deg(Q) \leq n. \tag{5.5.0.1}$$

Démonstration. a) Existence d'une solution

Ordonnons les polynômes A et B suivant les puissances croissantes de X :

$$A2 = a_r X^r + a_{r+1}X^{r+1} + \ldots + a_m X^m \text{ avec } a_r \neq 0 \text{ et } a_m \neq 0$$
$$B = b_0 + b_1 X + \ldots + b_p X^p \text{ avec } b_0 \neq 0 \text{ et } b_p \neq 0.$$

Si $A = 0$ ou si $r = \text{val}(A) > n$, on peut écrire $A = X^{n+1}R$, d'où la solution évidente $Q = 0$ et R.

Supposons $A \neq 0$ et $r = \text{val}(A) \leq n$. Posons $q_1 = \dfrac{a_r}{b_0} X^r$ et

$$R_1 = A - Bq_1. \tag{5.5.0.2}$$

Comme A et Bq_1 ont le même terme de plus bas degré, on a soit $R_1 = 0$ soit $\text{val}(R_1) > \text{val}(A)$.

Si $R_1 = 0$ ou si $\text{val}(R_1) > n$, nous pouvons écrire $R_1 = X^{n+1}R$ et nous pouvons prendre comme solution $Q = q_1$ et R.

Si $\text{val}(R_1) \leq n$, répétons sur le couple (R_1, B) ce qui vient d'être fait sur le couple (A, B) : on calcule le quotient q_2 du premier terme de R_1 par b_0 et on forme la différence

$$R_2 = R_1 - Bq_2. \tag{5.5.0.3}$$

Remarquons que $\deg(q_1) < \deg(q_2) = \text{val}(R_1) \leq n$.

Les premiers termes de R_1 et Bq_2 étant égaux, nous avons soit $R_2 = 0$, soit $\text{val}(R_2) > \text{val}(R_1)$. Si $R_2 = 0$ ou si $\text{val}(R_2) > n$ on peut écrire $R_2 = X^{n+1}R$.

Si nous ajoutons membre à membre les égalité (5.5.0.2) et (5.5.0.3) nous obtenons $A - B(q_1 + q_2) = R_2$, d'où la solution $Q = q_1 + q_2$ et R.

Si $\text{val}(R_2) \leq n$, on recommence l'opération en remplaçant R_1 par R_2, et ainsi de suite. Comme $\text{val}(A) < \text{val}(R_1 < \text{val}(R_2 < \ldots$, nous obtiendrons au bout d'un nombre fini d'itérations, un polynôme R_k tel que $R_k = 0$ ou $\text{val}(R_k) > n$, donc tel que $R_k = X^{n+1}R$.

En ajoutant membre à membre les égalités

$$A - Bq_1 = R_1, \quad R_1 - Bq_2 = R_2, \ldots, R_{k-1} - Bq_k = R_k,$$

nous obtenons $A - B(q_1 + \ldots + q_k) = R_k$.

Comme $\deg(q_1) < \deg(q_2) < \ldots < \deg(q_k) = \text{val}(R_{k-1}) \leq n$, il suffit de prendre $Q = q_1 + q_2 + \ldots + q_k$ et R tel que $R_k = X^{n+1}R$, R_k étant le premier reste dont la valuation est strictement supérieure à n.

b) Unicité

Supposons que l'on ait deux décompositions

$$A = BQ + X^{n+1}R = BQ_1 + X^{n+1}R_1 \quad \text{avec} \quad \deg(Q) \leq n \quad \text{et} \quad \deg(Q_1) \leq n.$$

Par différence, nous obtenons $B(Q - Q_1) = X^{n+1}(R_1 - R)$.

Si on avait $Q - Q_1 \neq 0$, le terme de plus bas degré de $B(Q - Q_1)$ serait le degré n au plus puisque $b_0 \neq 0$ et $\deg(Q - Q_1) \leq n$. Comme le terme de plus bas degré de $X^{n+1}(R_1 - R)$ est de degré $(n + 1)$ au moins, on aboutit à une contradiction. Donc $Q = Q_1$ et alors $R = R_1$.

5.5.0.2. Définition

Pour un entier n donné, l'écriture 5.5.0.1 s'appelle la **division suivant les puissances croissantes de A par B l'ordre n.** *Dans cette division Q est le* **quotient à l'ordre n** *et $X^{n+1}R$ le* **reste à l'ordre n.**

5.5.0.3. Exemple

Diviser $A = 1 + X$ par $B = 1 - X + X^2$ suivant les puissances croissantes de X à l'ordre 2.

La disposition pratique est la même que celle de la division euclidienne mais on écrit les monômes de A et B par ordre de degré croissant, ce qui explique le nom donné à cette division.

		$1 + X$	$1 - X + X^2$	
$-Bq_1$	:	$-1 + X - X^2$		
			$1 + 2X + X^2$	
R_1	:	$2X - X^2$	q_1 q_2 q_3	
$-Bq_2$	:	$-2X + 2X^2 - 2X^3$		
R_2	:	$X^2 - 2X^3$		
$-Bq_3$	:	$-X^2 + X^3 - X^4$		
R_3	:	$-X^3 - X^4$		

Donc $1 + X = (1 - X + X^2)(1 + 2X + X^2) - X^3(1 + X)$.

5.6. Fonction polynômes. Racines d'un polynôme

5.6.1. FONCTIONS POLYNÔMES

5.6.1.1. Définition

Soient K un anneau commutatif et $P = a_0 + a_1 X + ... + a_n X^n$ un polynôme de $K[X]$. On appelle **fonction polynôme** (*ou* **fonction polynomiale**) *associée au polynôme P, l'application $\tilde{P}$ de K dans K, associant à tout x de K l'élément*

$$\tilde{P}(x) = a_0 + a_1 x + ... + a_n x^n.$$

5.6.1.2. Remarque

Il est essentiel de ne pas confondre le polynôme $P = (a_0, a_1, ..., a_n, 0, ...)$ qui est une suite d'éléments de K dont un nombre fini sont non nuls et qui s'écrit, si $X = (0, 1, 0, ...)$, $P = a_0 + a_1 X + ... + a_n X^n$, et la fonction polynôme $\tilde{P}$. La fonction polynôme associée au polynôme P se note souvent à l'aide du même symbole P mais cette notation est dangereuse à cause des confusions possibles.

5.6.1.3. Théorème

K^K désignant l'ensemble des applications de K dans K, l'application φ de $K[X]$ dans K^K qui associe à un polynôme P la fonction polynôme $\tilde{P}$ est un morphisme d'anneaux.

Démonstration. On sait (voir l'Exemple 4.1.1.4) que K^K est un anneau. Il faut démontrer que, quels que soient les polynômes P et Q de $K[X]$, on a $\varphi(P+Q) = \varphi(P) + \varphi(Q)$, $\varphi(PQ) = \varphi(P)\,\varphi(Q)$ et $\varphi(1) = 1$.

Soient $P = (a_0, a_1, ..., a_n)$, $\quad Q = (b_0, b_1, ..., b_n, ...)$.

On a

$$P + Q = (a_0 + b_0, a_1 + b_1, ...).$$

$\varphi(P+Q)$ est l'application de K^K définie, pour tout $x \in K$, par

$$\big(\varphi(P+Q)\big)(x) = a_0 + b_0 + (a_1 + b_1)x + ... + (a_I + b_i)x^i + ...$$

ce qui, dans l'anneau K, est égal à

$$\begin{aligned}(a_0 + a_1 x + ... + a_i x^i + ...) + (b_0 + b_1 x + ... + b_i x^i + ...)\\ = \big(\varphi(P)\big)(x) + \big(\varphi(Q)\big)(x).\end{aligned}$$

On vérifierait de même que quel que soit $x \in K$,

$$\big(\varphi(PQ)\big)(x) = \big(\varphi(P)\big)(x) \cdot \big(\varphi(Q)(x)\big)\,.$$

Les images de tout $x \in K$ par $\varphi(P+Q)$ et par $\varphi(P)+\varphi(Q)$ étant égales, ces deux applications de K^K sont égales. On a de même $\varphi(PQ) = \varphi(P)\,\varphi(Q)$.

Enfin, si $1 = (1,0,0,\ldots)$ est l'élément unité de $K[X]$ on a, pour tout $x \in K$, $(\varphi(1))\,(x) = 1$, d'où $\varphi(1) = 1$.

5.6.1.4. Remarque

Il faut noter que le morphisme φ défini dans le Théorème 5.6.1.3 n'est pas nécessairement injectif. Ainsi, si $K = \mathbf{Z}/3\mathbf{Z}$, le polynôme $P = X^3 - X$ a pour fonction polynôme associée la fonction nulle (c'est le théorème de Fermat) mais P n'est pas le polynôme nul. Le morphisme φ n'est pas surjectif en général car si $K = \mathbb{R}$, il existe des applications de $\mathbb{R}$ dans $\mathbb{R}$ (par exemple les fonctions exponentielles) qui ne sont pas polynomiales.

5.6.2. RACINES D'UN POLYNÔME

Désormais et jusqu'à la fin de ce paragraphe, on suppose que K est un corps commutatif.

5.6.2.1. Définition

Soient P un polynôme de $K[X]$ et a un élément de K. On dit que a est une **racine** *ou un* **zéro** *de P si $\tilde{P}(a) = 0$.*

5.6.2.2. Théorème

Soient $P \in K[X]$ et $a \in K$. Pour que a soit racine de P, il faut et il suffit que P soit divisible par $X - a$.

Démonstration. Si P est divisible par $X - a$, alors il existe $Q \in K[X]$ tel que $P = (X - a)\,Q$; donc d'après le Théorème 5.6.1.3, pour tout $x \in K$, on a $\tilde{P}(x) = (x - a)\,\tilde{Q}(x)$. Si en particulier $x = a$, on a $\tilde{P}(a) = 0$. $\tilde{Q}(a) = 0$, donc a est racine de P.

Réciproquement, supposons que $\tilde{P}(a) = 0$. Effectuons la division euclidienne de P par $X - a$. On obtient $P = (X - a)Q + R$ avec $\deg(R) < \deg(X - a) = 1$, donc R est un polynôme constant. En prenant les valeurs des fonctions polynômes associées au point $x = a$, il vient $0 = \tilde{P}(a) = 0.\,\tilde{Q}(a) + R$. Donc P est divisible par $X - a$.

5.6.2.3. Définition

Soient P un polynôme de $K[X]$, a un élément de K et $\propto$ un entier ≥ 1. On dit que a est **racine d'ordre** $\propto$ *(ou de* **multiplicité** $\propto$*) de P si P est divisible par $(X - a)^{\propto}$ sans l'être par $(X - a)^{\propto+1}$.*

On dit que l'entier α *est la* **multiplicité** *ou* **l'ordre de multiplicité** *de la racine* a.

Une racine d'ordre 1 *est dite* **racine simple**, *une racine d'ordre* 2 *est dite* **racine double**, *etc.*

5.6.2.4. Théorème

Soit P *un élément de* $K[X]$. *Soient* $a_1, a_2, \ldots, a_r$ *les* r *racines distinctes de* P *dans* K, *et* $\alpha_1, \alpha_2, \ldots, \alpha_r$ *leurs ordres de multiplicité respectifs. Il existe un polynôme* $Q \in K[X]$ *qui n'admet pas de racine dans* K *tel que*

$$P = (X - a_1)^{\alpha_1} (X - a_2)^{\alpha_2} \ldots (X - a_r)^{\alpha_r} Q.$$

Démonstration. Pour $1 \leq i \leq r$ et $1 \leq j \leq r$, avec $i \neq j$, les deux polynômes $(X - a_i)$ et $(X - a_j)$ sont premiers entre eux puisque $a_i \neq a_j$. Donc $(X - a_i)^{\alpha_i}$ et $(X - a_j)^{\alpha_j}$ sont premiers entre eux ; ainsi les polynômes $(X - a_i)^{\alpha_i}$ pour $1 \leq i \leq r$ sont premiers entre eux deux à deux et divisent P. Il en résulte que P est divisible par le produit $(X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r}$; il existe donc un polynôme Q tel que $P = (X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r} Q$. D'autre part, si Q admettait la racine a_i, Q serait divisible par $(X - a_i)$ et P serait divisible par $(X - a_i)^{\alpha_i + 1}$, ce qui est absurde.

5.6.2.5. Remarque

Le théorème ne dit pas que le polynôme Q n'admet pas d'autres racines ; il peut en admettre dans un sur-corps de K. Par exemple, si $P = X^4 - 2X^3 - X^2 + 4X - 2$ est considéré comme polynôme de $\mathbb{Q}[X]$, on a $P = (X - 1)^2 (X^2 - 2)$, donc $Q = X^2 - 2$ et ce n'admet pas de racines dans $\mathbb{Q}$, mais admet $\sqrt{2}$ et $-\sqrt{2}$ comme racines dans $\mathbb{R}$.

5.6.2.6. Corollaire

Tout polynôme $P \in K[X]$ *non nul de degré* n *admet au plus* n *racines dans* K *en convenant de compter* α *fois une racine multiple d'ordre* α. *Si* P *admet* n *racines distinctes, elles sont toutes simples.*

Démonstration. Soient $a_1, \ldots, a_r$ les racines distinctes de P, $\alpha_1, \ldots, \alpha_r$ leurs ordres de multiplicité. On a

$$P = (X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r} Q ;$$

comme $P \neq 0$, on a $Q \neq 0$, donc

$$\deg(P) = \alpha_1 + \ldots + \alpha_r + \deg(Q) \quad \text{avec} \quad \deg(Q) \geq 0.$$

On en déduit $\alpha_1 + \ldots + \alpha_r \leq \deg(P) = n$.

Si P admet n racines distinctes, on a d'après ce qui précède, $\alpha_1 + ... + \alpha_n \leq n$; or comme $\alpha_i \geq 1$ pour tout $i \in \{1, ..., n\}$, on a $\alpha_1 + ... + \alpha_n \geq n$. Donc $\alpha_1 + ... + \alpha_n \geq n$ et par suite $\alpha_i = 1$ pour tout $i \in \{1, ..., n\}$.

5.6.2.7. Corollaire

Soit K un corps infini. Alors l'application $P \longmapsto \tilde{P}$ de $K[X]$ dans K^K est injective.

Démonstration. Soient P et Q deux polynômes de $K[X]$ tels que $\tilde{P} = \tilde{Q}$. Si $P - Q \neq 0$, soit n le degré de $P - Q$. Considérons $n + 1$ éléments distincts de K, ce qui est possible puisque K est infini. La fonction $\tilde{P} - \tilde{Q}$ s'annule pour ces valeurs; donc le polynôme $P - Q$ admet $(n + 1)$ racines, ce qui est impossible d'après le Corollaire 5.6.2.6. Donc $P = Q$. □

Lorsque K est infini (par exemple, si $K = \mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$) on peut identifier sans inconvénient un polynôme P à la fonction polynôme $\tilde{P}$ qui lui est associée; c'est ce que nous ferons désormais lorsque K est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. La valeur $\tilde{P}(a)$ de P en un point a de K sera donc notée $P(a)$.

5.6.2.8. Définition

On dit qu'un polynôme P de $K[X]$ est **scindé sur** *K si $P = 0$, ou, dans le cas contraire, si P est décomposable en un produit de facteurs du premier degré (distincts ou non) de $K[X]$.*

5.7. Étude de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$

5.7.1. CORPS ALGÉBRIQUEMENT CLOS

5.7.1.1. Définition

On dit qu'un corps commutatif K est **algébriquement clos** *si tout polynôme non constant de $K[X]$ possède au moins une racine dans K.*

Un tel corps est nécessairement infini car si K est fini et possède n éléments $a_1, ..., a_n$, le polynôme $(X - a_1)(X - a_2) ... (X - a_n) + 1$ n'a pas de racine dans K.

5.7.1.2. Théorème

Soit K un corps commutatif. Les propriétés suivantes sont équivalentes :

a) *K est algébriquement clos.*

b) *Tout polynôme P non nul de $K[X]$ de degré $n > 0$ admet n racines dans K.*

c) *Les seuls polynômes irréductibles de $K[X]$ sont les polynômes de degré* 1.

Démonstration. a) $\Longrightarrow$ b) Supposons K algébriquement clos. Soit P un polynôme de $K[X]$ de degré $n \geq 1$. Alors P possède au moins une racine a_1 dans K ; il existe donc un polynôme $Q_1 \in K[X]$ tel que $P = (X - a_1)Q_1$ avec $\deg(Q_1) = \deg(P) - 1 = n - 1$. Par récurrence, on voit que

$$P = (X - a_1)(X - a_2) \ldots (X - a_n)\, Q_n$$

avec $\deg(Q_n) = 0$, *i.e.* $Q_n \in K$, ce qui montre que P admet n racines dans K et prouve **b)**.

Il est évident que **b) $\Longrightarrow$ a)**, donc **a) $\Longleftrightarrow$ b)**.

b) $\Longrightarrow$ c) Supposons la condition **b)** vérifiée. Soit P un polynôme irréductible de $K[X]$. Alors P est de degré $n \geq 1$ puisqu'il est non inversible dans $K[X]$; donc P admet n racines dans K. Par suite, il existe au moins un élément $a \in K$ tel que P soit multiple de $X - a$. Comme P est irréductible il est proportionnel à $X - a$, donc P est de degré 1.

c) $\Longrightarrow$ b) Supposons que tout polynôme irréductible de $K[X]$ est de degré 1. Soit P un polynôme non nul de $K[X]$. D'après le théorème 5.4.4.9, P admet une décomposition unique en facteurs irréductibles :

$$P = \lambda P_1^{\alpha_1} \ldots P_r^{\alpha_r}$$

$P_1, \ldots, P_r$ désignant des polynômes irréductibles normalisés distincts et λ une constante non nulle. Par hypothèse, les P_i sont des polynômes de degré 1 ; donc P s'écrit

$$P = \lambda(X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r}$$

les a_i étant deux à deux distincts. Donc P possède n racines dans K (en comptant chaque racine avec son ordre de multiplicité) et **b)** est démontré.

On en déduit immédiatement les corollaires suivants :

5.7.1.3. Corollaire

Soit K un corps algébriquement clos. Alors tout polynôme de $K[X]$ est scindé sur K.

5.7.1.4. Corollaire

Soient K un corps algébriquement clos, A et B deux polynômes de $K[X]$. alors B divise A si et seulement si toute racine de B, d'ordre α, est racine de A avec un ordre au moins égal à α.

Les corps $\mathbb{Q}$ et $\mathbb{R}$ ne sont pas algébriquement clos car $X^2 - 2$ n'a pas de racine dans $\mathbb{Q}$ et $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$.

Le théorème suivant, dont la démonstration dépasse de loin le niveau de ce cours, fournit un exemple important de corps algébriquement clos.

5.7.1.5. Théorème *(d'Alembert-Gauss)*

Le corps $\mathbb{C}$ *des nombres complexes est algébriquement clos.*

$\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps du corps algébriquement clos $\mathbb{C}$. On démontre, plus généralement (Théorème de Steinitz) que tout corps commutatif K peut être plongé dans un corps commutatif L, algébriquement clos, unique à un isomorphisme près. L est appelé **clôture algébrique** de K.

5.7.2. POLYNÔMES DE $\mathbb{C}[X]$

Le corps $\mathbb{C}$ étant algébriquement clos, tous les résultats du n° précédent s'appliquent. En particulier le Théorème 5.6.2.4 peut être amélioré si K est un corps algébriquement clos, donc si $K = \mathbb{C}$.

5.7.2.1. Théorème

Soit P *un élément de* $\mathbb{C}[X]$ *de degré* n. *Soient* $a_1, \ldots, a_r$ *les racines distinctes de* P, *et* $\alpha_1, \ldots, \alpha_r$ *leurs ordres de multiplicité. On a alors*

$$P(X) = \lambda(X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r} \tag{5.7.2.1}$$

où λ *est le coefficient dominant de* P. *En outre*

$$\alpha_1 + \alpha_2 + \ldots + \alpha_r = n. \tag{5.7.2.2}$$

Démonstration. D'après le Théorème 5.6.2.4, on a

$$P(X) = (X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r} Q(X)$$

où le polynôme Q n'admet plus $a_1, \ldots, a_r$ pour racines ; comme toute racine de Q est racine de P (Corollaire 5.7.1.4), Q est constant. Le monôme de plus haut degré dans $\lambda(X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r}$ est $\lambda X^{\alpha_1 + \ldots + \alpha_r}$; comme P est de degré n, on a bien $\alpha_1 + \ldots + \alpha_r = n$. □

Le corps $\mathbb{C}$ étant algébriquement clos, les seuls polynômes irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1. Donc la formule (5.7.2.1) est la décomposition de P en facteurs irréductibles normalisés.

5.7.2.2. Définition

Soit $P = a_0 + a_1 X + \ldots + a_n X^n$ *un élément de* $\mathbb{C}[X]$. *On appelle* **polynôme conjugué** *de* P, et on note $\overline{P}$, *le polynôme* $\overline{P} = \overline{a_0} + \overline{a_1} X + \ldots + \overline{a_n} X^n$.

On vérifie facilement que si P et Q sont des éléments de $\mathbb{C}[X]$ et si $\lambda \in \mathbb{C}$, on a

$$\overline{P + Q} = \overline{P} + \overline{Q}, \quad \overline{PQ} = \overline{P}\,\overline{Q}, \quad \overline{\lambda P} = \overline{\lambda}\,\overline{P}, \quad \overline{\overline{P}} = P.$$

Autrement dit, l'application $P \longmapsto \overline{P}$ de $\mathbb{C}[X]$ dans $\mathbb{C}[X]$ (évidemment bijective) est un automorphisme de l'anneau $\mathbb{C}[X]$.

On en déduit que le polynôme B divise le polynôme A dans $\mathbb{C}[X]$ si, et seulement si $\overline{B}$ divise $\overline{A}$. En effet, l'égalité $A = BQ$ est équivalente à $\overline{A} = \overline{B}\,\overline{Q}$.

5.7.2.3. Théorème

Soient P un élément de $\mathbb{C}[X]$ et a un élément de $\mathbb{C}$. Alors :

a) *a est racine d'ordre $\propto$ de P si et seulement si $\overline{a}$ (conjugé de a) est racine d'ordre $\propto$ de $\overline{P}$.*

b) *Si $P \in \mathbb{R}[X]$, a est racine d'ordre $\propto$ de P si, et seulement si $\overline{a}$ est racine d'ordre $\propto$ de P.*

Démonstration. D'après la remarque précédente, $(X - a)^{\propto}$ divise P si, et seulement si, $\overline{(X-a)^{\propto}} = (X - \overline{a})^{\propto}$ divise $\overline{P}$, ce qui prouve **a)**. **b)** résulte immédiatement de **a)** car si $P \in \mathbb{R}[X]$, on a $P = \overline{P}$.

5.7.3. POLYNÔMES DE $\mathbb{R}[X]$

Dans ce numéro, nous nous proposons de déterminer tous les polynômes irréductibles de $\mathbb{R}[X]$.

5.7.3.1. Théorème

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un et les polynômes de degré deux sans racine réelle.

Démonstration. Les polynômes de degré 1 sont irréductibles (Exemple 5.4.5.3). De même, un polynôme P du second degré qui n'a aucune racine réelle est irréductible dans $\mathbb{R}[X]$. En effet, si P n'était pas irréductible dans $\mathbb{R}[X]$, il aurait un diviseur de degré 1, donc une racine réelle.

Réciproquement, montrons qu'un polynôme $P \in \mathbb{R}[X]$ de degré $n > 2$ n'est pas irréductible. Si P admet une racine réelle, le résultat est évident. Supposons que P n'ait aucune racine réelle. Considéré comme élément de $\mathbb{C}[X]$, P admet une racine complexe a. D'après le Théorème 5.7.2.3 **b)**, $\overline{a}$ est aussi racine de P ; donc P est divisible par $X - a$ et par $X - \overline{a}$. Les deux polynômes $X - a$ et $X - \overline{a}$ étant premiers entre eux puisque $a \neq \overline{a}$, P est divisible par $A = (X-a)\,(X-\overline{a})$ d'après le Corollaire 5.4.3.8. Mais

$$A = X^2 - (a + \overline{a})\ X + a\overline{a}$$

est un polynôme à coefficients réels puisque

$$a + \overline{a} = 2\mathcal{R}e(a) \in \mathbb{R} \quad \text{et} \quad a\overline{a} = |a|^2 \in \mathbb{R}.$$

donc P n'est pas irréductible.

5.7.3.2. Corollaire

Tout polynôme P non nul de $\mathbb{R}[X]$ de degré $n \geq 1$ et de coefficient dominant b_n s'écrit, d'une façon unique, sous la forme :

$$P = b_n \prod_{i=1}^{r} (X - a_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{\beta_j} \tag{5.7.3.1}$$

où les a_i $(1 \leq i \leq r)$, les p_j et les q_j $(1 \leq j \leq m)$ sont des nombres réels, où les polynômes $X^2 + p_j X + q_j$ vérifient les relations $p_j^2 - 4q_j < 0$ et où les entiers $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_m$ vérifient la relation :

$$\alpha_1 + \ldots + \alpha_r + 2(\beta_1 + \ldots + \beta_m) = n. \tag{5.7.3.2}$$

Démonstration. Soient $a_1, \ldots, a_r$ les racines réelles distinctes de P, $\alpha_1, \ldots, \alpha_r$ leurs ordres de multiplicité et soient $z_1, \overline{z_1}, \ldots, z_m, \overline{z_m}$ les racines deux à deux imaginaires conjuguées de P avec les ordres de multiplicité $\beta_1, \ldots, \beta_m$.

D'après le Théorème 5.7.2.1, on a

$$P = b_n (X-a_1)^{\alpha_1} \ldots (X-a_r)^{\alpha_r} (X-z_1)^{\beta_1} (X-\overline{z_1})^{\beta_1} \ldots (X-z_m)^{\beta_m} (X-\overline{z_m})^{\beta_m}$$

et $\alpha_1 + \ldots + \alpha_r + 2(\beta_1 + \ldots + \beta_m) = n$.

D'autre part, pour $1 \leq j \leq m$, on a

$$(X - z_j)^{\beta_j} (X - \overline{z_j})^{\beta_j} = (X^2 + p_j X + q_j)^{\beta_j}$$

avec $z_j + \overline{z_j} = -p_j \in \mathbb{R}$, $z_j \overline{z_j} = q_j \in \mathbb{R}$ et $p_j^2 - 4q_j < 0$.

On en déduit la formule (5.7.3.1) appelée **décomposition de Gauss du polynôme** P.

L'unicité de cette décomposition résulte du fait que les facteurs $X - a_i (1 \leq i \leq r)$ et $X^2 + p_j X + q_j$ $(1 \leq j \leq m)$ sont irréductibles et normalisés.

5.7.4. RELATIONS ENTRE LES COEFFICIENTS ET LES RACINES D'UN POLYNÔME

On sait que si $P = aX^2 + bX + c$ est un polynôme de $\mathbb{C}[X]$ et si x_1 et x_2 sont les racines de P, alors

$$x_1 + x_2 = -\frac{b}{a} \quad \text{et} \quad x_1 x_2 = \frac{c}{a}.$$

Nous nous proposons de généraliser ces relations entre les coefficients et les racines d'un polynôme du second degré au cas d'un polynôme de degré n quelconque.

5.7.4.1. Théorème

Soit $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ *un élément de* $\mathbb{C}[X]$ *de degré* $n \geq 1$. *Soient* $x_1, \ldots, x_n$ *les* n *racines distinctes ou non de* P. *Soient* $\sigma_1, \ldots, \sigma_n$ *les* **fonctions symétriques élémentaires** *des racines :*

$$\sigma_1 = \sum_i x_i = x_1 + \ldots + x_n,$$

$$\sigma_2 = \sum_{i<j} x_i x_j = x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n,$$

$$\sigma_3 = \sum_{i<j<k} x_i x_j x_k = x_1 x_2 x_3 + x_1 x_2 x_4 + \ldots + x_{n-2} x_{n-1} x_n,$$

$$- -$$

$$\sigma_n = x_1 x_2 \ldots x_n.$$

On a

$$\sigma_1 = -\frac{a_{n-1}}{a_n}, \quad \sigma_2 = \frac{a_{n-2}}{a_n}, \quad \ldots, \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}, \quad \ldots, \quad \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Démonstration. D'après le Théorème 5.7.2.1, on peut écrire :

$$P = a_n (X - x_1) \ldots (X - x_n).$$

Développons et ordonnons le produit $(X - x_1) \ldots (X - x_n)$ suivant les puissances décroissantes de X. On obtient

$$P = a_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \ldots + (-1)^k \sigma_k X^{n-k} + \ldots + (-1)^n \sigma_n).$$

En égalant les coefficients de X^{n-k} $(0 \leq k \leq n)$ dans les deux expressions de P, il vient $a_{n-k} = (-1)^k \sigma_k a_n$, d'où les formules annoncées.

5.8. Dérivation des polynômes

Dans ce paragraphe, nous allons définir une notion algébrique de dérivée qui coïncide avec la notion de dérivée des fonctions polynômes dans $\mathbb{R}$. On suppose que l'anneau K est de caractéristique 0.

5.8.1. DÉRIVÉE D'UN POLYNÔME

5.8.1.1. Définition

Soit K *un anneau commutatif et* $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$ *un polynôme de* $K[X]$. *On appelle* **polynôme dérivé** *de* P *le polynôme* $P' \in K[X]$ *défini par :*

(5.8.1.1) $$P' = na_nX^{n-1} + (n-1)\,a_{n-1}X^{n-2} + \ldots + 2a_2X + a_1.$$

En particulier, si P est une constante, P' est le polynôme nul.

Si $\deg(P) = n$, c'est-à-dire si $a_n \neq 0$, $na_n \neq 0$ si la caractéristique de K est nulle ou ne divise par n. Par suite, si la caractéristique de K est nulle, on a $\deg(P') = \deg(P) - 1$.

5.8.1.2. Théorème

Soient P et Q deux éléments de $K[X]$, $\lambda \in K$ et n un entier > 0. On a

$$(P+Q)' = P' + Q', \quad (\lambda P)' = \lambda P'$$
$$(PQ)' = P'Q + PQ', \quad (P^n)' = nP^{n-1}P'.$$

Démonstration. Soient

$$P = a_mX^m + a_{m-1}X^{m-1} + \ldots + a_0, \quad a_m \neq 0$$
$$Q = b_pX^p + b_{p-1}X^{p-1} + \ldots + b_0, \quad b_p \neq 0,$$

deux polynômes de $K[X]$. Supposons $p \leq m$; pour $p < k \leq m$, b_k est nul. Donc

$$P + Q = \sum_{k=0}^{m} (a_k + b_k)\, X^k.$$

Prenons les dérivées des polynômes P, Q et $P + Q$:

$$P' = \sum_{k=1}^{m} Ka_kX^{k-1}, \quad Q' = \sum_{k=1}^{p} kb_kX^{k-1}, \quad (P+Q)' = \sum_{k=1}^{m} k(a_k+b_k)\,X^{k-1}.$$

Par suite, on a

$$(P+Q)' = P' + Q'.$$

On montrerait de même que pour tout $\lambda \in K$, on a:

$$(\lambda P)' = \lambda P'.$$

Pour démontrer la troisième formule, supposons d'abord que P et Q soient des monômes:

$$P = \lambda\, X^p, \quad Q = \mu X^q, \quad \lambda, \mu \in K.$$

En écartant le cas trivial $p = 0$ et $q = 0$, on a

$$(PQ)' = (\lambda\mu X^{p+q})' = (p+q)\lambda\mu X^{p+q-1},$$

$$P'Q + PQ' = p\lambda\mu X^{p+q-1} + q\lambda\mu X^{p+q-1} = (p+q)\,\lambda\mu X^{p+q-1} = (PQ)'.$$

La propriété est donc vraie dans ce cas.

Soient alors $P = \sum_{r=0}^{n} a_r X^r$ et $Q = \sum_{k=0}^{m} b_k X^k$ deux polynômes de $K[X]$.

On a :

$$PQ = \sum_r \sum_k a_r b_k X^r X^k.$$

D'où, d'après ce qui précède :

$$\begin{aligned}(PQ)' &= \sum_r \sum_k a_r b_k (X^r X^k)' = \sum_r \sum_k a_r b_k \left((X^r)' X^k + X^r (X^k)'\right) \\ &= \sum_r r a_r X^{r-1} \sum_k b_k X^k + \sum_r a_r X^r \sum_k k b_k X^{k-1} = P'Q + PQ'.\end{aligned}$$

D'après la troisième formule, le polynôme dérivé de P^2 est $2P'P$. Par récurrence sur n, on voit facilement que $(P^n)' = nP^{n-1}P'$.

5.8.1.3. Définition

Soient $P \in K[X]$ et n un entier. On définit **le polynôme dérivé d'ordre n** *de P par récurrence en posant $P^{(n)} = \left(P^{(n-1)}\right)'$.*

On pose par convention, $P^{(0)} = P$.

5.8.2. FORMULE DE TAYLOR

On suppose maintenant que K est un corps commutatif de caractéristique 0.

5.8.2.1. Théorème

Soient P un polynôme de $K[X]$ de degré $n \geq 1$, et a un élément de K. On a (formule de Taylor) :

$$\begin{aligned}P &= P(a) + (X-a)\,P'(a) + \ldots + \frac{(X-a)^k}{K!}\,P^k(a) \\ &\quad + \ldots + \frac{(X-a)^n}{n!}\,P^{(n)}(a)\end{aligned} \tag{5.8.2.1}$$

où $P^{(k)}(a)$ désigne la valeur au point a de la fonction associée au polynôme $P^{(k)}$.

Démonstration. Soit

$$P = a_0 + a_1 X + \ldots + a_n X^n, \quad a_n \neq 0.$$

Pour simplifier l'écriture, nous noterons encore P la fonction polynôme $\tilde{P}$ associée à P.

Nous allons démontrer la formule (5.8.2.1), d'abord lorsque $a = 0$. On a

$$P(0) = a_0$$

$$P' = a_1 + 2a_2X + \ldots + na_nX^{n-1} \Longrightarrow P'(0) = a_1$$

$$- -$$

$$P^{(k)} = k(k-1)\ldots 3.2.1a_k + \ldots + n(n-1)\ldots(n-K+1)\,a_nX^{n-k},$$

d'où $P^{(k)}(0) = K\,!\,a_k$,

$$P^{(n)} = n\,(n-1)\ldots 3.2.1\,a_n \Longrightarrow P^{(n)}(0) = n\,!\,a_n.$$

On en déduit

$$a_0 = P(0), \quad a_1 = P'(0), \quad a_2 = \frac{1}{2\,!}\,P''(0), \quad \ldots, \quad a_k = \frac{1}{k\,!}\,P^{(k)}(0), \quad \ldots$$

$$\ldots \quad a_n = \frac{1}{n\,!}\,P^{(n)}(0).$$

En remplaçant les a_i $(0 \leq i \leq n)$ par ces expressions, on obtient la formule

$$P = P(0) + XP'(0) + \frac{X^2}{2\,!}\,P''(0) + \ldots + \frac{X^k}{k\,!}\,P^{(k)}(0) + \ldots + \frac{X^n}{n\,!}\,P^{(n)}(0)$$

appelée **formule de Mac-Laurin.**

Avec les notations précédentes, posons

$$Q(Y) = P(Y + a).$$

On a d'après la formule de Mac-Laurin,

$$Q = Q(0) + YQ'(0) + \ldots + \frac{Y^k}{k\,!}\,Q^{(k)}(0) + \ldots + \frac{Y^n}{n\,!}\,Q^{(n)}(0).$$

Comme

$$Q(Y) = P(Y+a) = a_0 + a_1(Y+a) + \ldots + a_K(Y+a)^k + \ldots + a_n(Y+a)^n,$$

on a

$$Q(0) = P(a),\ Q'(0) = P'(a),\ \ldots,\ Q^{(k)}(0) = P^{(k)}(a),\ \ldots,\ Q^{(n)}(0) = P^{(n)}(a).$$

On en déduit la formule de Taylor

$$(5.8.2.2) \quad P(Y+a) = P(a) + YP'(a) + \ldots + \frac{Y^k}{k\,!}\,P^{(k)}(a) + \ldots + \frac{Y^n}{n\,!}\,P^{(n)}(a)$$

ou, en posant $Y + a = X$,

$$P = P(a) + (X-a)P'(a) + \ldots + \frac{(X-a)^k}{k\,!}\,P^{(k)}(a) + \ldots + \frac{(X-a)^n}{n\,!}\,P^{(n)}(a). \quad \square$$

La formule de Taylor va nous permettre d'obtenir une condition nécessaire et suffisante pour qu'un élément a de K soit une racine d'ordre k d'un polynôme. Démontrons d'abord un Lemme.

5.8.2.2. Lemme

Soient P un élément de $K[X]$, a un élément de K et k un entier ≥ 2. Alors, si a est racine d'ordre k de P, a est racine d'ordre $k-1$ de P'.

Démonstration. Si a est racine d'ordre k de P, il existe un polynôme Q de $K[X]$ tel que

$$P = (X-a)^k Q \quad \text{avec} \quad Q(a) \neq 0.$$

Donc

$$P' = k(X-a)^{k-1} Q + (X-a)^k Q' = (X-a)^{k-1} H$$

où $H = kQ + (X-a) Q'$. On a $H(a) = kQ(a) \neq 0$, car $Q(a) \neq 0$ et $k \cdot 1 \neq 0$ dans K puisque K est de caractéristique 0. Donc a est bien racine d'ordre $k-1$ de P'.

5.8.2.3. Théorème

Soient K un corps de caractéristique 0, P un polynôme de $K[X]$, $a \in K$ et k un entier ≥ 1. Pour que a soit racine d'ordre k de P, il faut et il suffit que :

$$(5.8.2.3) \qquad P(a) = 0, \quad P'(a) = 0, \quad \ldots, \quad P^{(k-1)}(a) = 0, \quad P^{(k)}(a) \neq 0.$$

Démonstration. Si a est racine d'ordre k de P, d'après le Lemme 5.8.2.2, a est racine d'ordre $k-1, k-2, \ldots, 1$ de $P', P'', \ldots, P^{(k-1)}$ respectivement et $P^{(k)}(a) \neq 0$. Les relations (5.8.2.3) sont donc vérifiées.

Réciproquement, si les relations (5.8.2.3) sont vérifiées, le degré n de P est $\geq k$.

La formule de Taylor donne :

$$P = (X-a)^k \left[\frac{P^{(k)}(a)}{k!} + \frac{X-a}{(k+1)!} P^{(k+1)}(a) + \ldots + \frac{(X-a)^{n-k}}{n!} P^{(n)}(a) \right]$$

$$= (X-a)^k Q$$

avec $Q(a) = \dfrac{1}{k!} P^{(k)}(a) \neq 0$. Donc a est racine d'ordre k de P.

5.9. Polynômes à plusieurs indéterminées

Nous allons définir les polynômes à plusieurs indéterminées en nous inspirant du cas d'une indéterminée. Nous ne ferons pas une étude détaillée des propriétés de l'anneau des polynômes à plusieurs indéterminées mais nous invitons le lecteur inéressé à le faire lui-même (c'est très instructif). Les notions fondamentales seront exposées dans le cas de deux indéterminées.

5.9.1. DÉFINITIONS GÉNÉRALES

5.9.1.1. Définition

Soit K un anneau commutatif. On appelle **polynôme à deux indéterminées à coefficients** *dans K, toute suite double $(a_{ij})_{i\geq 0, j\geq 0}$ d'éléments de K dont seuls un nombre fini de termes sont non nuls.*

On note

$$P = (a_{00}, a_{10}, a_{01}, \ldots) \quad \text{ou} \quad P = (a_{ij})_{i\geq 0, j\geq 0}.$$

Les a_{ij} sont appelés **coefficients** du polynôme P ; a_{00} s'appelle le **terme constant.**

L'ensemble des polynômes à deux indéterminées à coefficients dans l'anneau commutatif K se note $K[X, Y]$.

Soient $P = (a_{ij})$ et $Q = (b_{ij})$ deux polynômes de $K[X, Y]$. On définit la somme et le produit de P et Q par les formules :

$$(a_{ij} + b_{ij}) = (a_{ij}) + (b_{ij}) \tag{5.9.1.1}$$

$$(a_{ij})\,(b_{ij}) = (c_{ij})$$

où

$$c_{ij} = \sum_{\substack{i'+i''=i \\ j'+j''=j}} a_{i'j'} b_{i''j''}. \tag{5.9.1.2}$$

On vérifie facilement que l'on définit bien ainsi sur $K[X, Y]$ une structure d'anneau commutatif (intègre si K est intègre).

On dit que deux polynômes $P = (a_{ij})$ et $Q = (b_{ij})$ sont égaux si on a $a_{ij} = b_{ij}$ pour tout élément (i, j) de $\mathbb{N} \times \mathbb{N}$ On identifie K à un sous-anneau de $K[X, Y]$ en identifiant tout élément $a \in K$ au polynôme (a_{ij}) tel que $a_{00} = a$ et $a_{ij} = 0$ si $i \geq 1$ ou $j \geq 1$.

Soit X (resp. Y) le polynôme dont tous les coefficients sont nuls sauf a_{10} (resp. a_{01}) qui est égal à 1. En raisonnant comme dans le cas de $K[X]$, on vérifie facilement que tout polynôme $P = (a_{ij})_{i\geq 0, j\geq 0}$ s'écrit de façon unique sous la forme :

$$P = \sum_{\substack{i\geq 0 \\ j\geq 0}} a_{ij} X^i Y^i. \tag{5.9.1.3}$$

On dit que X et Y sont les indéterminées et que P est un polynôme en X et Y.

On définirait de même l'anneau $K[X_1, X_2, \ldots, X_n]$ des polynômes à n indéterminées $X_1, X_2, \ldots, X_n$ à coefficients dans K. Un élément de cet anneau s'écrit

$$\sum_{(i_1, \ldots, i_n) \in \mathbb{N}^n} a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

où un nombre fini de coefficients $a_{i_1 \ldots i_n}$ sont non nuls.

5.9.2. ISOMORPHISME CANONIQUE DE $K[X][Y]$ SUR $K[X,Y]$

Soit K un anneau commutatif. $A = K[X]$ est un anneau commutatif. Pour tout polynôme $P \in A[Y]$, on a

$$P = \sum_j P_j Y^j$$

avec $P_j \in K[X]$, l'ensemble des indices j tels que $P_j \neq 0$ étant fini. Posons, pour tout indice j :

$$P_j = \sum_i a_{ij} X^i, \quad \text{où } a_{ij} \in K.$$

Alors

$$Q = \sum_j \left(\sum_i a_{ij} X^i \right) Y^j = \sum_{i,j} a_{ij} X^i Y^j$$

est un élément de $K[X,Y]$. On peut donc associer à P l'élément $Q = \sum_{i,j} a_{ij} X^i Y^j$ de $K[X,Y]$.

5.9.2.1. Théorème

L'application $P \longmapsto Q$ est un isomorphisme de $A[Y]$ sur $K[X,Y]$.

Démonstration. Notons φ l'application qui fait correspondre à P l'élément Q. Elle est surjective car les coefficients a_{ij} de $\varphi(P) = Q = \sum_{i,j} a_{ij} X^i Y^j$ sont arbitraires.

Montrons qu'elle est injective.

Soit $A = \sum_j A_j Y^i$ avec $A_j = \sum_i \alpha_{ij} X^i$; on a

$\varphi(A) = B = \sum_{i,j} \alpha_{ij} X^i Y^j$. Si $\varphi(A) = \varphi(P)$, on a $a_{ij} = \alpha_{ij}$ quels que soient i et j, donc $A_j = P_j$ quel que soit j ; par suite $A = P$ et φ est injective.

On verrait de même qu'il existe un isomorphisme de $K[X_1, ..., X_{n-1}][X_n]$ sur $K[X_1, ..., X_{n-1}, X_n]$.

5.9.3. DEGRÉ D'UN POLYNÔME A DEUX INDÉTERMINÉES

5.9.3.1. Définition

Soit $P = \sum_{i,j} a_{ij} X^i Y^j$ *un polynôme de* $K[X, Y]$. *On appelle* **degré partiel** *de* P *par rapport à* X, *le degré de* P *considéré comme élément de* $K[Y]\,[X]$, *c'est-à-dire le plus grand des entiers* i *tels que* $a_{ij} \neq 0$.

Ce degré partiel se note $\deg_X(P)$. On a les inégalités suivantes :

$$\deg_X(P+Q) \leq \sup\left(\deg_X(P),\ \deg_X(Q)\right)$$
$$\deg_X(P \cdot Q) \leq \deg_X(P) + \deg_X(Q)$$

cette dernière inégalité étant une égalité si K est intègre.

On définit de même le degré partiel de P par rapport à Y.

On a $\deg_X(P) = -\infty$ si $P = 0$.

On appelle **degré total**, ou simplement **degré de** P, et on note $\deg(P)$, le plus grand des entiers $i + j$ pour tout les couples (i, j) tels que $a_{ij} \neq 0$.

Si $P, Q \in K[X, Y]$, on a aussi les inégalités :

$$\deg(P+Q) \leq \sup\left(\deg(P), \deg(Q)\right)$$
$$\deg(P \cdot Q) \leq \deg(P) + \deg(Q).$$

Si par exemple $P = X^4 + X^2Y^3$, $\deg_X(P) = 4$, $\deg_Y(P) = 3$, et $\deg(P) = 5$.

On dit que le polynôme $P = \sum_{i,j} a_{ij} X^i Y^i$ est **homogène de degré** d si $a_{ij} = 0$ pour $i + j \neq d$. Autrement dit, P est homogène de degré d si chacun des monômes qu'il contient est de degré total d.

En regroupant ensemble, dans l'expression de $P = \sum_{i,j} a_{ij} X^i Y^j$ les termes pour lesquels $i+j$ a une valeur donnée, on voit que tout polynôme $P \in K[X, Y]$ de degré total d s'écrit d'une manière unique sous la forme

$$P = P_0 + P_1 + \ldots + P_d \tag{5.9.3.1}$$

où chaque polynôme P_r est homogène de degré r et où $P_d \neq 0$. On dit que P_r est la **composante homogène de degré** r de P.

Toutes les notions qui viennent d'être définies se généralisent aisément au cas de n indéterminées.

5.9.4. FONCTIONS POLYNÔMES

Nous traitons comme précédemment le cas de deux indéterminées X et Y, la généralisation étant facile à faire.

5.9.4.1. Définition

Soit $P = \sum_{i,j} a_{ij} X^i Y^i$ *un polynôme de* $K[X, Y]$. *On appelle* **fonction polynôme de deux variables** *associée au polynôme* P, *l'application* $\tilde{P}$ *de* $K \times K$ *dans* K, *associant à tout élément* (x, y) *de* $K \times K$, *l'élément* $\sum_{i,j} a_{ij} x^i y^j$.

On démontre, comme dans le cas de $K[X]$, que quels que soient les polynômes P et Q de $K[X, Y]$ et l'élément $\lambda \in K$, on a

$$(P \tilde{+} Q) = \tilde{P} + \tilde{Q}, \quad (P \tilde{\cdot} Q) = \tilde{P} \cdot \tilde{Q}, \quad (\lambda \tilde{P}) = \lambda \tilde{P}.$$

On démontre également que si K est un anneau intègre infini, l'application qui à un polynôme P de $K[X, Y]$ fait correspondre la fonction polynôme $\tilde{P}$ est un isomorphisme de $K[X, Y]$ sur l'anneau des fonctions polynômes à deux variables sur K. Ceci permet d'identifier un polynôme $P \in K[X, Y]$ à la fonction polynôme $\tilde{P}$ qui lui est associée lorsque $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

Toutes ces considérations se généralisent sans peine au cas de n indéterminées $X_1, \ldots, X_n$.

5.9.5. DÉRIVATION PARTIELLE DES POLYNÔMES

5.9.5.1. Définition

Soient K *un anneau commutatif et* P *un polynôme de* $K[X, Y]$. *On appelle polynôme* **dérivé partiel** *de* P *par rapport à l'indéterminée* X (resp. Y), *et on note* P'_X (resp. P'_Y) *ou* $\frac{\partial P}{\partial X}$ $\left(\text{resp. } \frac{\partial P}{\partial Y}\right)$ *le polynôme dérivé de* P *considéré comme élément de* $K[Y]\,[X]$ (*resp.* $K[X]\,[Y]$).

Si $K = \mathbb{R}$, on retrouve les dérivées partielles définies en analyse. On a des règles de calcul analogues à celles qui ont été établies au paragraphe 5.8 dans le cas d'une indéterminée.

Si $P = \sum a_{ij} X^i Y^j$ est un polynôme de $K[X, Y]$, on a

$$P''_{XY} = P''_{YX}.$$

Il suffit de vérifier cette formule lorsque $P = X^i Y^j$. Dans ce cas, on a :

$$P''_{XY} = \left(iX^{i-1}Y^j\right)'_Y = iX^{i-1}jY^{j-1} = ijX^{i-1}Y^{j-1}$$
$$P''_{YX} = \left(X^i jY^{j-1}\right)'_X = iX^{i-1}jY^{j-1} = ijX^{i-1}Y^{j-1}.$$

Cette remarque permet de calculer les dérivées partielles successives de P sans se préoccuper de l'ordre des dérivations.

On note $P^{(\alpha+\beta)}_{X^\alpha Y^\beta}$ le polynôme obtenu en dérivant α fois par rapport à X et β fois par rapport à Y.

5.9.5.2. Théorème (*Formule d'Euler*)

Soient K un corps de caractéristique 0, et P un élément de $K[X, Y]$. Pour que P soit homogène de degré n, il faut et il suffit que $XP'_X + YP'_Y = nP$.

Démonstration. Supposons P homogène de degré n. P s'écrit donc

$$P = \sum_{i=0}^{n} a_i X^i Y^{n-i}.$$

Alors :

$$XP'_X + YP'_Y = \sum_{i=0}^{n} i a_i X^i Y^{n-i} + \sum_{i=0}^{n} (n-i)\, a_i X^i Y^{n-i} = nP.$$

Réciproquement, supposons qu'on ait

$$XP'_X + YP'_Y = nP.$$

Nous savons que tout polynôme P de $K[X, Y]$ s'écrit de façon unique sous la forme $P = \sum_i P_i$ où chaque P_i est homogène de degré i. Alors d'après la première partie, on a

$$nP = XP'_X + YP'_Y = \sum_i \left(X(P_i)'_X + Y(P_i)'_Y\right) = \sum_i iP_i.$$

D'où

$$\sum_i nP_i = \sum_i iP_i.$$

En vertu de l'unicité de la décomposition d'un polynôme en somme de polynômes homogènes, nous obtenons $(n-i)P_i = 0$ pour tout i ; donc $P_i = 0$ pour $i \neq n$, puisque K est de caractéristique 0. Donc $P = P_n$ est homogène de degré n.

5.9.5.3. Théorème (*Formule de Taylor*)

Soient K un corps de caractéristique 0, a et b des éléments de K, et P un élément de $K[X, Y]$. On a

$$P(X, Y) = \sum_{i \geq 0, j \geq 0} \frac{1}{i!\,j!} P^{(i+j)}_{X^i Y^j}(a, b)\,(X-a)^i\,(Y-b)^j. \tag{5.9.5.1}$$

Démonstration. Notons d'abord que 5.9.5.1 a un sens car la somme du second membre est finie puisque les dérivées $P^{(i+j)}$ sont nulles pour $i + j$ assez grand.

D'autre part, tout élément de $K[X, Y]$ est somme d'éléments de la forme $\lambda(X-a)^r\,(Y-b)^s$, où $\lambda \in K$, et où r et s sont dans $\mathbb{N}$. En effet, pour un monôme $X^\alpha Y^\beta$, on a

$$X^\alpha Y^\beta = \big((X-a)+a\big)^\alpha\ \big((Y-b)+b\big)^\beta .$$

La formule du binôme donne

$$X^\alpha Y^\beta = \sum_{k=0}^{\alpha} C_\alpha^k\, a^{\alpha-k}(X-a)^k \sum_{q=0}^{\beta} C_\beta^q\, b^{\beta-q}\,(Y-b)^q,$$

expression que l'on peut toujours écrire sous la forme indiquée.

Par linéarité, il suffit donc de démontrer (5.9.5.1) lorsque $P(X, Y) = (X-a)^m(Y-b)^n$.

On a

$$P_{X^iY^j}^{(i+j)}(a, b) = 0 \text{ pour } (i, j) \neq (m, n) \text{ et } P_{X^mY^n}^{m+n)}(a, b) = m!\,n!$$

Le second membre de (5.9.5.1) se réduit donc à $\dfrac{1}{m!\,n!}\,m!\,n!\,(X-a)^m\,(Y-b)^n$, d'où le théorème.

Fractions rationnelles

Soit K un corps commutatif. Nous savons que l'ensemble $K[X]$ des polynômes à une indéterminée à coefficients dans K est un anneau commutatif intègre dans lequel les seuls éléments inversibles sont les polynômes de degré 0. $K[X]$ n'est donc pas un corps, mais on peut construire le corps des fractions de $K[X]$ (cf. Chapitre 4, § 4.5, n° 4.5.3).
Ce corps s'appelle le corps des fractions rationnelles à une indéterminée à coefficients dans K. On le note $K(X)$.

5.10. Définition du corps des fractions rationnelles

Nous allons rappeler dans ce paragraphe les principales étapes de la construction du corps $K(X)$ des fractions rationnelles à une indéterminée à coefficients dans K.

5.10.1. FRACTIONS RATIONNELLES

On pose comme d'habitude $K[X]^* = K[X] - \{0\}$.

• $K(X)$ est l'ensemble quotient de $K[X] \times K[X]^*$ par la relation d'équivalence $\mathcal{R}$:

$$(A, B)\mathcal{R}(A_1, B_1) \Longleftrightarrow AB_1 = A_1B.$$

Une fraction rationnelle F de $K(X)$ est donc une classe d'équivalence représentée par un couple (A, B) d'élément de $K[X]$ dans lequel $B \neq 0$; un autre couple (A_1, B_1) représente la même fraction rationnelle F si, et seulement si $AB_1 = A_1B$.

Si (A, B) est un représentant quelconque de F, on convient d'écrire $F = \dfrac{A}{B}$ ou $F = AB^{-1}$; on dit que A est le **numérateur** et que B est le **dénominateur** de la fraction rationnelle F.

• Dans $K[X] \times K[X]^*$, on définit l'addition et la multiplication en posant :

$$(A, B) + (C, D) = (AD + BC, BD)$$
$$(A, B) \cdot (C, D) = (AC, BD).$$

Les deux lois de $K(X)$ sont les lois quotients et on les note aussi, $+$ et $\cdot$; alors le triplet $(K(X), +, \cdot)$ est un corps commutatif. L'élément neutre pour l'addition est la fraction rationnelle nulle 0 qui est la classe des couples $(0, B)$ tels que $B \neq 0$. L'élément neutre pour la multiplication, appelée **fraction rationnelle unité**, et notée 1, est la classe des couples (B, B) avec $B \neq 0$. Pour la multiplication, l'inverse de la fraction rationnelle non nulle F, classe de (A, B) avec $A \neq 0$ et $B \neq 0$ est la fraction rationnelle notée $\dfrac{1}{F}$.

L'application qui, à $A \in K[X]$, associe la fraction rationnelle dont un représentant est le couple $(A, 1)$, est un morphisme injectif de l'anneau $K[X]$ dans l'anneau $K(X)$. On peut donc identifier $K[X]$ au sous-anneau de $K(X)$ constitué par les fractions rationnelles dont les représentants sont de la forme $(A, 1)$.

5.10.1.1. Définition

Soit $F \in K(X) - \{0\}$. On appelle **représentant irréductible** *de F ou* **forme irréductible** *de F toute représentation de F sous la forme $\dfrac{A}{B}$, où A et B sont des éléments de $K[X]$ premiers entre eux.*

Montrons que toute fraction rationnelle admet une forme irréductible.

5.10.1.2. Théorème

Soit F un élément de $K(X) - \{0\}$. Alors :

a) *F possède des représentants irréductibles.*

b) *Si* (A, B) *est un représentant irréductible de* F, *les autres représentants irréductibles de* F *sont de la forme* $(\lambda A, \lambda B)$, *où* $\lambda \in K^*$, *et les représentants de* F *sont de la forme* (AC, BC), *où* $C \in K[X]^*$.

Démonstration. a) Soit (A, B) un représentant de F. Par hypothèse, on a $A \neq 0$ et $B \neq 0$. Soit D le PGCD de A et B. On a $A = A_1 D$ et $B = B_1 D$, avec PGCD $(A_1, B_1) = 1$, $B_1 \neq 0$ puisque B n'est pas nul. Par suite $\dfrac{A}{B} = \dfrac{A_1}{B_1} = F$ et $\dfrac{A_1}{B_1}$ est bien un représentant irréductible de F.

b) Soit (A, B) un représentant irréductible de F et soit (A_1, B_1) un autre représentant irréductible de F. On a $AB_1 = A_1 B$. Donc B divise AB_1 et est premier avec A; d'après le Théorème de Gauss, B divise B_1. De même B_1 divise B. Ainsi, il existe $C \in K[X]$ tel que $B_1 = BC$. Comme l'anneau $K[X]$ est intègre et puisque $B \neq 0$, l'égalité $AB_1 = A_1 B$ qui s'écrit $A_1 B = ABC$, montre que $A_1 = AC$. On a ensuite $B_1 = BC$. De plus, P.G.C.D. $(A_1, B_1) = C$, d'où P.G.C.D. $(A_1, B_1) = 1$ si et seulement si $C \in K^*$. Si (A, B) est un représentant irréductible de F, il est clair que, pour tout $C \in K[X]^*$, (AC, BC) est un représentant de F.

Notation. Par abus de langage, nous dirons et nous noterons :

- $\dfrac{A}{B}$ la fraction rationnelle dont un représentant est le couple (A, B).
- $\dfrac{A}{B} = \dfrac{A_1}{B_1}$ si (A, B) et (A_1, B_1) représentent la même fraction rationnelle.
- La fraction irréductible $\dfrac{A}{B}$ au lieu de la fraction de représentant irréductible (A, B).
- Si B divise A, $A = BQ$. La fraction $\dfrac{A}{B}$ sera donc identifiée au polynôme Q.

Les opérations dans $K(X)$ s'expriment par

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD} \quad \text{et} \quad \frac{A}{B} \cdot \frac{C}{D} = \frac{AC}{BD}.$$

5.10.1.3. Théorème

Soit $F \in K(X) - \{0\}$. *Si* $\dfrac{A}{B}$ *est un représentant quelconque de* F, *l'entier* $\deg(A) - \deg(B)$ *ne dépend que de* F. *On l'appelle le* **degré** *de la fraction rationnelle* F, *et on le note* $\deg(F)$.

Démonstration. Soient en effet $\dfrac{A}{B}$ et $\dfrac{A_1}{B_1}$ deux représentants de F. On a $AB_1 = A_1 B$, donc

$$\deg(A) + \deg(B_1) = \deg(A_1) + \deg(B).$$

Comme $\deg(B)$ et $\deg(B_1)$ sont des éléments de $\mathbb{N}$ puisque $B \neq 0$ et $B_1 \neq 0$, on en déduit

$$\deg(A) - \deg(B) = \deg(A_1) - \deg(B_1).$$

Comme pour les polynômes, on convient de poser $\deg(0) = -\infty$.

5.10.1.4. Théorème

Si $\frac{A}{B}$ *et* $\frac{C}{D}$ *sont des éléments non nuls de* $K(X)$, *on a :*

$$\deg\left(\frac{A}{B} + \frac{C}{D}\right) \leq \sup\left(\deg\left(\frac{A}{B}\right), \deg\left(\frac{C}{D}\right)\right)$$

$$\deg\left(\frac{A}{B} \cdot \frac{C}{D}\right) = \deg\left(\frac{A}{B}\right) + \deg\left(\frac{C}{D}\right).$$

La vérification est immédiate et est laissée au lecteur.

5.10.2. FONCTION RATIONNELLE

Soit K un corps commutatif. Nous allons associer à toute fraction rationnelle sur K une fonction de K dans K, comme cela a été fait pour les polynômes (voir § 5.6).

5.10.2.1. Définition

Soit $F = \frac{P}{Q}$ *une fraction rationnelle de* $K(X)$ *écrite sous forme irréductible. On appelle* **pôle** *de* F *toute racine de son dénominateur. On dit que* $a \in K$ *est un* **pôle d'ordre** $\propto$ *de* F *si* a *est un zéro d'ordre* $\propto$ *de* Q.

Toute racine de multiplicité k *du polynôme* P *est dite racine* **d'ordre** k de F.

5.10.2.2. Remarque

Si $\frac{P}{Q}$ et $\frac{P_1}{Q_1}$ sont deux formes irréductibles de F, P et P_1 sont associés et ont donc les mêmes zéros ; de même Q et Q_1 étant associés ont les mêmes racines. Les notions de pôle et de racine sont donc indépendantes du représentant irréductible choisi. Mais il est indispensable, dans la définition précédente, de prendre un représentant irréductible; ainsi $+1$ n'est pas un pôle de la fraction rationnelle $\frac{X^3 - 1}{X^2 - 1}$.

5.10.2.3. Définition

Soit F une fraction rationnelle écrite sous forme irréductible $\frac{P}{Q}$. On appelle **domaine de définition** *de F, et on note D_F, le complémentaire dans K de l'ensemble des pôles de F.*

On appelle **fonction rationnelle** *associée à F, l'application $\tilde{F}$ de D_F dans K définie par $\tilde{F}(x) = \frac{\tilde{P}(x)}{\tilde{Q}(x)}$ pour tout $x \in D_F$.*

Cette définition est justifiée par le fait que si $\frac{P}{Q}$ et $\frac{P_1}{Q_1}$ sont deux représentants irréductibles de F, $\frac{P(x)}{Q(x)} = \frac{P_1(x)}{Q_1(x)}$ et $\tilde{F}$ ne dépend donc pas du représentant irréductible choisi.

5.10.2.4. Définition

Soient F et G deux fractions rationnelles sur K, de domaines de définition D_F et D_G respectivement. On définit les applications $F \tilde{+} G$ et $F \tilde{\cdot} G$ de $D_F \cap D_G$ dans K en posant :

$$(F \tilde{+} G)(x) = \tilde{F}(x) + \tilde{G}(x)$$
$$(F \tilde{\cdot} G)(x) = \tilde{F}(x) \cdot \tilde{G}(x)$$

pour tout $x \in D_F \cap D_G$.

5.10.2.5. Théorème

Soient K un corps commutatif infini, et F et G deux fractions rationnelles sur K telles que $\tilde{F}(x) = \tilde{G}(x)$ pour tout $x \in D_F \cap D_G$. Alors $F = G$.

Démonstration. Soient $\frac{P}{Q}$ et $\frac{P_1}{Q_1}$ des représentants irréductibles de F et G respectivement. Pour tout $x \in D_F \cap D_G$, on a $\frac{\tilde{P}(x)}{\tilde{Q}(x)} = \frac{\tilde{P}_1(x)}{\tilde{Q}_1(x)}$. Donc

$$\tilde{P}(x)\,\tilde{Q}_1(x) - \tilde{Q}(x)\,\tilde{P}_1(x) = 0.$$

Autrement dit la fonction polynôme associée au polynôme $PQ_1 - QP_1$ de $K[X]$ s'annule en tout point de l'ensemble $D_F \cap D_G$ qui est infini puisque le nombre de pôles est fini. Ainsi le polynôme $PQ_1 - QP_1$ s'annule pour une infinité de valeurs, donc (Corollaire 5.6.2.6), $PQ_1 - QP_1 = 0$, *i.e.* $F = G$.

5.11. Décomposition d'une fraction rationnelle en éléments simples

5.11.1. THÉORÈMES GÉNÉRAUX

5.11.1.1. Lemme

Soit F un élément de $K(X)$. Il existe un unique polynôme E tel que l'on ait $F = E + R$ où R est une fraction rationnelle de degré strictement négatif. On dit que E est la **partie entière** *de F.*

Démonstration. Soit $\frac{A}{B}$ un représentant quelconque de F. Comme $B \neq 0$, on peut effectuer la division euclidienne de A par B. On obtient

$$A = EB + D \text{ avec } D = 0 \text{ ou } \deg(D) < \deg(B).$$

Si $D = 0$, $F = E + 0$ et l'existence est établie. Sinon, on a

$$\frac{A}{B} = \frac{EB + D}{B} = E + \frac{D}{B}.$$

Posons $R = \frac{D}{B}$; on a $\deg(R) < 0$.

L'écriture est unique car si E et E_1 sont des polynômes tels que $F = E + R = E_1 + R_1$ avec $\deg(R) < 0$ et $\deg(R_1) < 0$, on a

$$\deg\left((F - E) + (E_1 - F)\right) \leq \sup\left(\deg(F - E),\ \deg(E_1 - F)\right).$$

On en déduit $\deg(E_1 - E) < 0$, d'où $E_1 = E$.

5.11.1.2. Lemme

Soit $F = \frac{P}{Q_1 Q_2 \dots Q_n}$ une fraction rationnelle, où les polynômes $Q_1, \dots, Q_n$ sont premiers entre eux deux à deux et $\deg(P) < \deg(Q_1 Q_2 \dots Q_n)$. *Il existe une famille et une seule de polynôme P_i, $1 \leq i \leq n$, tels que*

$$\frac{P}{Q_1 Q_2 \dots Q_n} = \sum_{i=1}^{n} \frac{P_i}{Q_i}; \quad \deg\left(\frac{P_i}{Q_i}\right) < 0 \quad \textit{pour tout} \quad i \in \{1, \dots, n\}.$$

Démonstration. Raisonnons par récurrence sur n.

a) Existence d'une décomposition lorsque $Q = Q_1 Q_2$:
Q_1 et Q_2 étant deux polynômes premiers entre eux, il existe, d'après le Théorème de Bezout, deux polynômes R_1 et R_2 tels que $R_2 Q_1 + R_1 Q_2 = 1$, soit $P = (PR_2)Q_1 + (PR_1)Q_2$.

On en déduit

$$\frac{P}{Q_1Q_2} = \frac{PR_1}{Q_1} + \frac{PR_2}{Q_2}.$$

D'après le Lemme 5.11.1.1, il existe des polynômes E_1, P_1, E_2, P_2 tels que :

$$\frac{PR_1}{Q_1} = E_1 + \frac{P_1}{Q_1}, \quad \frac{PR_2}{Q_2} = E_2 + \frac{P_2}{Q_2}, \quad \deg\left(\frac{P_1}{Q_1}\right) < 0, \quad \deg\left(\frac{P_2}{Q_2}\right) < 0.$$

D'où

$$\frac{P}{Q_1Q_2} = E_1 + E_2 + \frac{P_1}{Q_1} + \frac{P_2}{Q_2}, \quad \deg\left(\frac{P_1}{Q_1}\right) < 0, \quad \deg\left(\frac{P_2}{Q_2}\right) < 0.$$

On en déduit $\deg\left(\frac{P_1}{Q_1} + \frac{P_2}{Q_2}\right) < 0$, donc $E_1 + E_2$ est la partie entière de $\frac{P}{Q_1Q_2}$. Comme cette partie entière est nulle d'après l'hypothèse sur les degrés de P et Q_1Q_2, on a finalement

$$\frac{P}{Q_1Q_2} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} \quad \text{avec} \quad \deg\left(\frac{P_1}{Q_1}\right) < 0 \quad \text{et} \quad \deg\left(\frac{P_2}{Q_2}\right) < 0.$$

b) Unicité de la décomposition dans le cas de $Q = Q_1Q_2$:

Supposons qu'on ait trouvé deux couples (P_1, P_2) et (P_1', P_2') de polynômes vérifiant les conditions du théorème.

On obtient par différence :

$$\frac{P_1 - P_1'}{Q_1} = \frac{P_2' - P_2}{Q_2} \quad \text{ou} \quad Q_2(P_1 - P_1') = Q_1(P_2' - P_2).$$

Le polynôme Q_2 est premier avec Q_1 et il divise $Q_1(P_2' - P_2)$; d'après le Théorème de Gauss, Q_2 divise $P_2' - P_2$. Or $\deg(P_2' - P_2) \leq \sup\left(\deg(P_2'), \deg(P_2)\right) < \deg(Q_2)$, donc $P_2' - P_2 = 0$. Q_2 n'étant pas nul et $K[X]$ étant intègre, on a $P_1 - P_1' = 0$, d'où l'unicité de la décomposition.

c) Existence et unicité dans le cas général :

Raisonnons par récurrence sur n, le résultat étant vrai pour $n = 2$. Supposons le résultat démontré pour $(n-1)$ facteurs et soit $Q = Q_1Q_2 \ldots Q_n$ un produit de n polynômes premiers entre eux deux à deux. Q_1 étant premier avec $Q_2, \ldots, Q_n$ est premier avec le produit $Q_2Q_3 \ldots Q_n$. En appliquant la première partie de la démonstration, on conclut qu'il existe un couple unique (P_1, R_1) de polynômes vérifiant $\deg(P_1) < \deg(Q_1)$, $\deg(R_1) < \deg(Q_2 \ldots Q_n)$ et tels que :

$$\frac{P}{Q} = \frac{P_1}{Q_1} + \frac{R_1}{Q_2Q_3 \ldots Q_n}.$$

Appliquons alors l'hypothèse de récurrence à la fraction rationnelle $\frac{R_1}{Q_2 \dots Q_n}$; on obtient d'une manière et d'une seule, $n-1$ polynômes $P_2, \dots, P_n$ tels que :

$$\frac{P}{Q} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} + \dots + \frac{P_n}{Q_n}$$

avec $\deg(P_i) < \deg(Q_i)$ pour tout $i \in \{1, \dots, n\}$ ce qui achève la preuve.

5.11.1.3. Lemme

Soit $F = \frac{P}{Q^n}$, $n \in \mathbb{N}^*$, *une fraction rationnelle telle que* $\deg(P) < \deg(Q^n)$. *Il existe une famille unique de polynômes* $P_1, P_2, \dots, P_n$ *telle que :*

$$F = \sum_{i=1}^{n} \frac{P_i}{Q^i} \text{ et } \deg(P_i) < \deg(Q) \text{ pour tout } i \in \{1, \dots, n\}.$$

Démonstration. Raisonnons par récurrence sur l'entier n.

Le lemme est évident si $n = 1$. Supposons-le démontré jusqu'à l'ordre $n-1$ et démontrons-le à l'ordre n.

Effectuons la division euclidienne de P par Q : il existe des polynômes B et P_n dans $K[X]$ tels que

$$P = QB + P_n \text{ avec } \deg(P_n) < \deg(Q).$$

Alors $\frac{P}{Q^n} = \frac{B}{Q^{n-1}} + \frac{P_n}{Q^n}$.

Cette décomposition est unique à cause de l'unicité de la division euclidienne dans $K[X]$. Comme $\frac{B}{Q^{n-1}} = \frac{P - P_n}{Q^n}$ on a, d'après le Théorème 5.10.1.4, $\deg(B) < \deg(Q^{n-1})$. On peut donc appliquer l'hypothèse de récurrence à $\frac{B}{Q^{n-1}}$, ce qui achève la démonstration du lemme.

5.11.1.4. Définition

Toute fraction rationnelle de la forme $\frac{A}{B^\alpha}$, *où* B *est un polynôme irréductible de* $K[X]$, α *un entier supérieur ou égal à* 1 *et où* $\deg(A) < \deg(B)$, *s'appelle un* **élément simple.**

Le résultat fondamental de ce paragraphe est le théorème suivant qui s'obtient en utilisant les lemmes précédents.

5.11.1.5. Théorème

Soit F une fraction rationnelle de $K(X)$ écrite sous sa forme irréductible $\frac{P}{Q}$, Q étant un polynôme de degré au moins égal à 1. Si $Q = \lambda A^{\alpha} B^{\beta} \ldots L^{\gamma}$ est la décomposition de Q en facteurs irréductibles, il existe une famille unique $E, A_1, \ldots, A_{\alpha}, B_1, \ldots, B_{\beta}, \ldots, L_1, \ldots, L_{\gamma}$ de polynômes de $K[X]$ tels que

$$\frac{P}{Q} = E + \frac{A_1}{A} + \frac{A_2}{A^2} + \ldots + \frac{A_{\alpha}}{A^{\alpha}} + \frac{B_1}{B} + \frac{B_2}{B^2} + \ldots + \frac{B_{\beta}}{B^{\beta}} + \frac{L_1}{L} + \frac{L_2}{L^2} + \ldots + \frac{L_{\gamma}}{L^{\gamma}}$$

et $\deg(A_i) < \deg(A), \deg(B_i) < \deg(B), \ldots, \deg(L_i) < \deg(L)$ *pour tout i.*

Calculer ces polynômes c'est **décomposer la fraction rationnelle F en éléments simples.**

Démonstration. Puisque les polynômes $A, B, \ldots, L$ sont premiers entre eux deux à deux il en est de même de $A^{\alpha}, B^{\beta}, \ldots, L^{\gamma}$. D'après les lemmes 5.11.1.1 et 5.11.1.2, il existe une famille unique de polynômes $E, C_1, \ldots, C_{\gamma}$ tels que

$$\frac{P}{Q} = E + \frac{C_1}{A^{\alpha}} + \ldots + \frac{C_{\gamma}}{L^{\gamma}}$$

avec $\deg\left(\frac{C_1}{A^{\alpha}}\right) < 0, \ldots, \deg\left(\frac{C_{\gamma}}{L^{\gamma}}\right) < 0$. Il suffit maintenant d'appliquer le Lemme 5.11.1.3 à chacun des termes $\frac{C_1}{A^{\alpha}}, \ldots, \frac{C_{\gamma}}{L^{\gamma}}$ pour obtenir la décomposition annoncée.

5.11.2. DÉCOMPOSITION EN ÉLÉMENTS SIMPLES D'UNE FRACTION RATIONNELLE SUR $\mathbb{C}$

Nous savons que les polynômes irréductibles de $\mathbb{C}[X]$ sont de la forme $X - a$, où $a \in \mathbb{C}$. Le Théorème 5.11.1.5 se simplifie de la manière suivante :

5.11.2.1. Théorème

Soit F une fraction rationnelle de $\mathbb{C}(X)$ écrite sous forme irréductible $\frac{P}{Q}$ telle que $\deg(Q) \geq 1$. Si $Q(X) = \lambda(X - a_1)^{\alpha_1} \ldots (X - a_n)^{\alpha_n}$ est la décomposition de Q en facteurs irréductibles, il existe un polynôme unique E et une unique famille de scalaires $(b_{ij})_{1 \leq i \leq n, 1 \leq j \leq \alpha_i}$ tels que :

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{\alpha_i} \frac{b_{ij}}{(X - a_i)^j} \right).$$

Démonstration. Les polynômes $A, B, ..., L$ du Théorème 5.11.1.5 sont ici $(X - a_1), (X - a_2), ..., (X - a_n)$; comme ces polynômes sont du premier degré, les polynômes $A_i, B_j \ ... \ L_k$ de la théorie générale, qui vérifient $\deg(A_i) < \deg(A)$, sont des constantes.

5.11.2.2. Définition

Les notations étant celles du Théorème 5.11.2.1, $\sum_{j=1}^{\alpha_i} \frac{b_{ij}}{(X - a_i)^j}$ *s'appelle la* **partie polaire** (*ou* **partie principale**) *de F relative au pôle a_i.*

Méthode pratique de calcul des b_{ij}

Étant donné une fraction rationnelle F de $\mathbb{C}(X)$, le Théorème 5.11.2.1 affirme l'existence et l'unicité de la décomposition en éléments simples de F. La partie entière (qui est non nulle si et seulement si $\deg(F) \geq 0$) s'obtient en effectuant la division euclidienne du numérateur de F par son dénominateur. Nous supposerons dans la suite que cette opération a été faite et nous ne considérons plus que des fractions rationnelles de degré strictement négatif.

a) Partie polaire relative à un pôle multiple :

Soit $F(X) = \dfrac{P(X)}{(X - a)^k \, Q(X)}$ une fraction rationnelle de $\mathbb{C}(X)$ de degré strictement négatif admettant a pour pôle d'ordre k (on a donc $P(a) \neq 0$ et $Q(a) \neq 0$).

D'après le Théorème 5.11.2.1, la décomposition de F s'écrit :

$$F(X) = \frac{b_1}{X - a} + \frac{b_2}{(X - a)^2} + ... + \frac{b_k}{(X - a)^k} + \frac{P_1(X)}{Q(X)}.$$

D'où

$$P(X) = \left(b_k + b_{k-1}(X - a) + ... + b_1(X - a)^{k-1}\right) Q(X) + (X - a)^k \, P_1(X).$$

Prenons alors le polynôme $X - a = Y$ comme nouvelle indéterminée ; on obtient

$$P(a + Y) = (b_k + b_{k-1}Y + ... + b_1 Y^{k-1}) \, Q(a + Y) + Y^k P_1(a + Y).$$

La partie polaire relative au pôle a apparaît ainsi comme le quotient de la division suivant les puissances croissantes de $P(a + Y)$ par $Q(a + Y)$ à l'ordre $k - 1$.

b) Partie polaire relative à un pôle simple :

Si $\dfrac{P}{Q}$ est une fraction rationnelle irréductible de $\mathbb{C}(X)$ admettant le nombre a pour pôle simple, la partie polaire de cette fraction rationnelle relative au pôle a est $\dfrac{P(a)}{Q'(a)} \cdot \dfrac{1}{X - a}$.

En posant $Q(X) = (X - a)\, Q_1(X)$, on a une décomposition de la forme

$$\frac{P(X)}{(X-a)Q_1(X)} = \frac{A}{X-a} + \frac{R(X)}{Q_1(X)} \quad \text{avec } Q_1(a) \neq 0.$$

Multiplions les deux membres par $X - a$ puis faisons $X = a$; on obtient $A = \dfrac{P(a)}{Q_1(a)}$.

De l'égalité $Q(X) = (X - a)\, Q_1(X)$, on obtient en prenant les polynômes dérivés, $Q'(X) = (X-a)\, Q_1'(X) + Q_1(X)$. D'où $Q'(a) = Q_1(a)$ et $A = \dfrac{P(a)}{Q'(a)}$.

5.11.2.3. Exemple

Décomposer la fraction rationnelle $F(X) = \dfrac{1}{X(X+1)\,(X-1)^3}$ en éléments simples sur $\mathbb{C}$.

Le degré du numérateur étant strictement inférieur à celui du dénominateur, la partie entière de la décomposition est nulle.

La décomposition est de la forme :

$$F(X) = \frac{A}{X} + \frac{B}{X+1} + \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{(X-1)^3}.$$

Multiplions les deux membres de cette égalité par X puis faisons $X = 0$; il vient $A = -1$.

En multipliant de même les deux membres de l'égalité par $X + 1$ puis faisant $X = -1$, nous obtenons $B = \dfrac{1}{8}$.

Pour obtenir la partie principale relative au pôle triple 1, nous posons $Y = X - 1$. D'où $F(1+Y) = \dfrac{1}{(2+3Y+Y^2)Y^3}$.

La division de 1 par $2+3Y+Y^2$ suivant les puissances croissantes à l'ordre 2 donne :

$$1 = (2+3Y+Y^2)\left(\frac{1}{2} - \frac{3}{4}Y + \frac{7}{8}Y^2\right) + Y^3\left(-\frac{15}{8} - \frac{7}{8}Y\right),$$

soit en revant à $F(1+Y)$:

$$\frac{1}{(2+3Y+Y^2)\,Y^3} = \frac{\frac{1}{2}}{Y^3} - \frac{\frac{3}{4}}{Y^2} + \frac{\frac{7}{8}}{Y} + \frac{-\frac{15}{8} - \frac{7}{8}Y}{2+3Y+Y^2}$$

et en revant enfin à X,

$$F(X) = \frac{1}{2(X-1)^3} - \frac{3}{4(X-1)^2} + \frac{7}{8(X-1)} + \frac{-\frac{7}{8}X - 1}{X(X+1)}.$$

La décomposition cherchée est donc

$$F(X) = -\frac{1}{X} + \frac{1}{8(X+1)} + \frac{7}{8(X-1)} - \frac{3}{4(X-1)^2} + \frac{1}{2(X-1)^3}.$$

5.11.3. DÉCOMPOSITION EN ÉLÉMENTS SIMPLES D'UNE FRACTION RATIONNELLE SUR $\mathbb{R}$

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes du premier degré et ceux du second degré à discriminant négatif. Le Théorème 5.11.1.5 prend alors la forme suivante :

5.11.3.1. Théorème

Soit F une fraction rationnelle de $\mathbb{R}(X)$ admettant un représentant irréductible $\frac{P}{Q}$ tel que $\deg(Q) \geq 1$.

Si $Q(X) = \lambda \prod_{i=1}^{n} (X - a_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{\beta_j}$ *est la décomposition de Q en polynômes irréductibles, il existe un polynôme unique E et des familles uniques de nombres réels* $(A_{ij})_{1 \leq i \leq n, 1 \leq j \leq \alpha_i}$ $(B_{kr})_{1 \leq k \leq m, 1 \leq r \leq \beta_k}$ et $(C_{kr})_{1 \leq k \leq m, 1 \leq r \leq \beta_k}$ tels que :

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{\alpha_i} \frac{A_{ij}}{(X - a_i)^j} \right) + \sum_{k=1}^{m} \left(\sum_{r=1}^{\beta_k} \frac{B_{kr} X + C_{kr}}{(X^2 + p_k X + q_k)^r} \right).$$

5.11.3.2. Définition

Dans la décomposition en éléments simples d'une fraction rationnelle de $\mathbb{R}(X)$, une fraction de la forme $\frac{A_{ij}}{(X - a)^j}$ *s'appelle un* **élément simple de première espèce**, *une fraction de la forme* $\frac{B_{kr} X + C_{kr}}{(X^2 + p_k X + q_k)^r}$ *s'appelle un* **élément simple de deuxième espèce.**

Méthode pratique de décomposition

a) Pour la recherche de la partie entière et les éléments simples de première espèce, tout ce qui a été dit au n° 5.11.2 reste valable.

b) Pour les éléments simples de deuxième espèce, les méthodes suivantes peuvent être utilisées :

• On écrit la décomposition de F à l'aide de coefficients indéterminés et on détermine ces coefficients par des considérations numériques particulières ;

l'examen de la parité de la fraction rationnelle considérée peut simplifier les calculs.

• On utilise la décomposition dans $\mathbb{C}(X)$ puis en regroupant les parties polaires relatives aux pôles conjugués, on obtient la décomposition dans $\mathbb{R}(X)$.

• Si F n'admet que deux pôles complexes conjugués, on procède par divisions successives.

Pour conclure ce chapitre, examinons quelques exemples qui mettent en œuvre les méthodes qui viennent d'être expliquées.

5.11.3.3. Exemple

Décomposer la fraction rationnelle $F(X) = \dfrac{1}{(X^2-1)(X^2+1)^2}$ en éléments simples sur $\mathbb{R}$.

On a $P = 1$, $Q = (X^2-1)(X^2+1)^2$; $\deg(P) < \deg(Q)$, donc la partie entière est nulle. F s'écrit

$$F(X) = \frac{A}{X-1} + \frac{B}{X+1} + \frac{aX+b}{X^2+1} + \frac{cX+d}{(X^2+1)^2}.$$

Nous remarquons que F est paire, c'est-à-dire $F(-X) = F(X)$.

Comme

$$F(-X) = -\frac{A}{X+1} - \frac{B}{X-1} + \frac{-aX+b}{X^2+1} + \frac{-cX+d}{(X^2+1)^2},$$

l'unicité de la décomposition nous permet d'affirmer que $B = -A$, $a = -a$, $c = -c$, donc $a = c = 0$.

Pour déterminer A, multiplions les deux membres par $X-1$ et après simplification, donnons à X la valeur 1 ; nous trouvons $A = \dfrac{1}{8}$. On utilise une méthode analogue pour déterminer d ; on trouve $d = -\dfrac{1}{2}$.

Il ne reste plus qu'un coefficient inconnu ; il suffit de donner à X une valeur particulière, par exemple 0, pour obtenir $b = -\dfrac{1}{4}$.

La décomposition cherchée est donc

$$\frac{1}{(X^2-1)(X^2+1)^2} = \frac{1}{8(X-1)} - \frac{1}{8(X+1)} - \frac{1}{4(X^2+1)} - \frac{1}{2(X^2+1)^2}.$$

5.11.3.4. Exemple

Décomposer la fraction rationnelle $F(X) = \dfrac{X}{(X+1)(X^2+1)}$ en éléments simples sur $\mathbb{R}$.

La partie entière étant nulle, la décomposition sur $\mathbb{C}$ est de la forme

$$F(X) = \frac{A}{X+1} + \frac{B}{X+i} + \frac{C}{X-i}.$$

Pour obtenir A, on multiplie les deux membres de cette égalités par $X+1$ puis on fait $X = -1$, d'où $A = \frac{-1}{2}$. On obtient de même $B = \frac{1+i}{4}$, $C = \frac{1-i}{4}$, ce qui donne

$$F(X) = \frac{-1}{2(X+1)} + \frac{1+i}{4(X+i)} + \frac{1-i}{4(X-i)}.$$

En regroupant les parties polaires relatives aux pôles conjugués et en réduisant au même dénominateur, nous obtenons la décomposition sur $\mathbb{R}$:

$$\begin{aligned} F(X) &= \frac{-1}{2(X+1)} + \frac{(1+i)(X-i) + (1-i)(X+i)}{4(X^2+1)} \\ &= \frac{-1}{2(X+1)} + \frac{X+1}{2(X^2+1)}. \end{aligned}$$

5.11.3.5. Exemple

Décomposer la fraction rationnelle $\frac{2X^4 + X^3 + 1}{(X^2+X+1)^3}$ en éléments simples sur $\mathbb{R}$.

La partie entière est nulle. Le dénominateur admet deux racines complexes conjuguées.

La division euclidienne du numérateur par $X^2 + X + 1$ donne :

$$2X^4 + X^3 + 1 = (X^2 + X + 1)(2X^2 - X - 1) + 2X + 2,$$

d'où

$$\frac{2X^4 + X^3 + 1}{(X^2+X+1)^3} = \frac{2X^2 - X - 1}{(X^2+X+1)^2} + \frac{2X+2}{(X^2+X+1)^3}.$$

La division euclidienne du quotient $2X^2 - X - 1$ par $X^2 + X + 1$ s'écrit :

$$2X^2 - X - 1 = 2(X^2 + X + 1) - 3X - 3.$$

On en déduit : $\frac{2X^2 - X - 1}{(X^2+X+1)^2} = \frac{2}{X^2+X+1} + \frac{-3X-3}{(X^2+X+1)^2}$.

La décomposition cherchée est donc :

$$\frac{2X^4 + X^3 + 1}{(X^2+X+1)^3} = \frac{2}{X^2+X+1} + \frac{-3X-3}{(X^2+X+1)^2} + \frac{2X+2}{(X^2+X+1)^3}.$$

Chapitre 6 : ESPACES VECTORIELS

La notion d'espace vectoriel est l'une des notions les plus importantes en mathématiques et dans les applications des mathématiques aux autres sciences. En physique et dans les sciences de l'ingénieur, les espaces vectoriels constituent un outil indispensable pour représenter certaines quantités : forces, vitesses, état d'un système en mécanique quantique, etc.

Dans ce chapitre, nous allons introduire la notion abstraite d'espace vectoriel puis nous étudierons les principales conséquences des axiomes définissant la structure d'espace vectoriel. Dans tout ce qui suit, K désignera toujours un corps commutatif.

6.1. Définition d'un espace vectoriel

6.1.1. DÉFINITIONS

6.1.1.1. Définition

Soient E un groupe commutatif noté additivement, et K un corps commutatif. On dit que E est un **espace vectoriel sur** *K ou un* **K-espace vectoriel**, *s'il existe une loi externe, de domaine K, associant à tout élément (λ, x) de $K \times E$ l'élément de E noté $\lambda \cdot x$ ou λx avec les propriétés suivantes :*

$$\begin{aligned} \lambda \cdot (x + y) &= \lambda \cdot x + \lambda \cdot y \\ (\lambda + \mu) \cdot x &= \lambda \cdot x + \mu \cdot x \\ \lambda \cdot (\mu \cdot x) &= (\lambda\mu) \cdot x \\ 1 \cdot x &= x \end{aligned}$$

quels que soient $x, y \in E$ et $\lambda, \mu \in K$, 1 désignant l'élément unité du corps K.

Les éléments de E s'appellent les **vecteurs** ; ceux de K s'appellent les **scalaires.** Nous désignerons en général les vecteurs par des lettres latines minuscules, et les scalaires par des lettres grecques minuscules. On parlera d'**espace vectoriel réel** si $K = \mathbb{R}$, d'**espace vectoriel complexe** si $K = \mathbb{C}$.

L'élément neutre du groupe $(E, +)$ est noté 0_E ou simplement 0 et est appelé le **vecteur nul** ou l'**origine** de E. Si $E = \{0\}$, on dit que E est un **espace vectoriel nul.**

6.1.1.2. Remarque

Si au lieu de prendre un corps K, on prend un anneau A (non commutatif), on dit que E, muni des deux lois de composition précédentes est un **module à gauche sur l'anneau** A ou encore un **A-module à gauche** (l'ordre d'écriture λx pour le produit externe de $(\lambda, x) \in K \times E$ doit être respecté).

On définit de même un **A-module à droite.** C'est un ensemble E sur lequel on a défini :

a) une loi de groupe abélien, notée $(x, y) \longmapsto x + y$;

b) une application $(x, \lambda) \longmapsto x \cdot \lambda$ de $E \times A$ dans E, vérifiant les propriétés suivantes :

$$\begin{aligned} (x+y)\cdot\lambda &= x\cdot\lambda + y\cdot\lambda \\ x\cdot(\lambda+\mu) &= x\cdot\lambda + x\cdot\mu \\ (x\cdot\lambda)\cdot\mu &= x\cdot(\lambda\mu) \\ x\cdot 1 &= x \end{aligned}$$

quels que soient $x, y \in E$ et $\lambda, \mu \in A$.

Si A est un anneau commutatif, ces deux notions de module à gauche et de module à droite coïncident. On dit que E est un **A-module.**

6.1.2. RÈGLES DE CALCUL DANS UN ESPACE VECTORIEL

L'opposé du vecteur x dans le groupe $(E, +)$ est noté $-x$; la somme du vecteur x et de l'opposé du vecteur y est notée $x - y$ et est appelée **différence** de x et y.

a) On a

$$\lambda(x - y) = \lambda x - \lambda y \tag{6.1.2.1}$$

quels que soient $x, y \in E$ et $\lambda \in K$.

En effet,

$$\lambda(x - y) + \lambda y = \lambda\left[(x - y) + y\right] = \lambda x.$$

D'où la formule (6.1.2.1) Si dans cette formule, on fait $x = y$, il vient

$$\lambda \cdot 0 = 0$$

pour tout $\lambda \in K$.

b) On a

$$(\lambda - \mu)x = \lambda x - \mu x \tag{6.1.2.2}$$

quels que soient $x \in E$ et $\lambda, \mu \in K$.

En effet,

$$(\lambda - \mu)x + \mu x = \left[(\lambda - \mu) + \mu\right] x = \lambda x.$$

On en déduit la formule (6.1.2.2). En faisant $\lambda = \mu$ dans cette formule, on obtient

$$0 \cdot x = 0$$

pour tout vecteur x.

c) Quel que soit $x \in E$ et quel que soit $\lambda \in K$, on a

(6.1.2.3) $$(-\lambda)x = \lambda(-x) = -(\lambda x).$$

On a en effet

$$\lambda x + \lambda(-x) = \lambda(x - x) = \lambda \cdot 0 = 0$$

et

$$\lambda x + (-\lambda)x = \big(\lambda + (-\lambda)\big)\, x = (\lambda - \lambda)x = 0 \cdot x = 0.$$

d) Pour tout $x \in E$ et pour tout $\lambda \in K$,

$$\lambda x = 0 \Longleftrightarrow \lambda = 0 \text{ ou } x = 0.$$

D'après b) et c), on a $\lambda \cdot 0 = 0 \cdot x = 0$.

Réciproquement, supposons que $\lambda \cdot x = 0$ et $\lambda \neq 0$. Alors λ^{-1} existe et on a

$$\lambda^{-1}(\lambda x) = \lambda^{-1} \cdot 0 = 0.$$

Or

$$\lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1 \cdot x = x,$$

donc $x = 0$.

6.1.3. EXEMPLE D'ESPACES VECTORIELS

6.1.3.1. Exemple

L'ensemble E des vecteurs libres du plan (ou de l'espace) de la géométrie élémentaire est un espace vectoriel réel pour les lois de composition $\left(\vec{V}_1, \vec{V}_2\right) \longmapsto \vec{V}_1 + \vec{V}_2$ de $E \times E$ dans E et $\left(\lambda, \vec{V}\right) \longmapsto \lambda \vec{V}$ de $\mathbb{R} \times E$ dans E. Cet exemple est à l'origine de l'étude abstraite des espaces vectoriels.

6.1.3.2. Exemple

Soient K un corps commutatif et K' un sous-corps de K. Muni de la loi de groupe abélien et de la loi externe $(\lambda, \mu) \longmapsto \lambda \cdot \mu$ de $K' \times K$ dans K, K est un K'-espace vectoriel. Si on prend en particulier $K' = K$, on voit que tout corps K est un espace vectoriel sur lui-même, la loi externe étant la multiplication interne. Ainsi $\mathbb{R}$ est un espace vectoriel réel. $\mathbb{C}$ est un espace vectoriel réel ou complexe.

6.1.3.3. Exemple

Soit E un espace vectoriel sur K et soit K' un sous-corps de K. En considérant la restriction de l'opération externe de $K \times E$ à $K' \times E$, on obtient une structure d'espace vectoriel sur le corps K'. Ainsi, tout $\mathbb{C}$-espace vectoriel est aussi un $\mathbb{R}$-espace vectoriel. Ce procédé est appelé **restriction du corps des scalaires**. Le procédé inverse, appelé **extension du corps des scalaires** ne sera pas exposé dans ce cours.

6.1.3.4. Exemple

Soient $E_1, E_2, ..., E_n$, n espaces vectoriels sur le même corps K. Nous allons munir l'ensemble produit $E_1 \times E_2 \times ... \times E_n$ d'une structure d'espace vectoriel sur K. Pour cela, si $(x_1, x_2, ..., x_n) \in E_1 \times E_2 \times ... \times E_n$, $(y_1, y_2, ..., y_n) \in E_1 \times E_2 \times ... \times E_n$ et $\lambda \in K$, posons :

$$(x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

$$\lambda(x_1, x_2, ..., x_n) = (\lambda x_1, \lambda x_2, ..., \lambda x_n).$$

On vérifie facilement qu'on obtient ainsi une structure de K-espace vectoriel.

On dit que $E_1 \times E_2 \times ... \times E_n$ est l'**espace vectoriel produit** des n espaces $E_1, E_2, ..., E_n$.

Si en particulier $E_1 = E_2 = ... = E_n = E$, on obtient le K-espace vectoriel E^n. Par exemple K^n, $n \geq 2$, est un espace vectoriel sur K puisque K est un espace vectoriel sur lui-même.

6.1.3.5. Exemple

Soient X un ensemble quelconque F un K-espace vectoriel et soit E l'ensemble de toutes les applications $f : X \longrightarrow F$.

Si $f, g \in E$ et $\lambda \in K$, définissons $f + g$ et λf en posant

$$(f + g)(x) = f(x) + g(x)$$

$$(\lambda f)(x) = \lambda f(x)$$

pour tout $x \in X$.

On vérifie facilement que E est un K-espace vectoriel lorsqu'on le munit des deux lois de composition $(f, g) \longmapsto f + g$ et $(\lambda, f) \longmapsto \lambda f$ ainsi définies.

6.1.3.6. Exemple

L'ensemble E des fonctions réelles continues d'une variable réelle, muni des lois de composition définies dans l'Exemple 6.1.3.5 est un espace vectoriel réel. On démontre en effet dans le cours d'analyse que si f et g sont partout continues et si $\lambda \in \mathbb{R}$, alors $f + g$ et λf sont continues partout, donc sont dans E.

De même l'ensemble des fonctions réelles d'une variable réelle, dérivables en un point $x_0 \in \mathbb{R}$ (ou dérivables en tout point) est un espace vectoriel réel.

6.1.3.7. Exemple

Soit K un corps commutatif. L'ensemble $K[X]$ des polynômes à une indéterminée X, à coefficients dans K, est un K-espace vectoriel lorsqu'on le munit de l'addition des polynômes : $(P, Q) \longmapsto P + Q$ et de la multiplication par un scalaire $(\lambda, P) \longmapsto \lambda \cdot P$, définies au Chapitre 5.

6.2. Sous-espaces vectoriels

6.2.1. DÉFINITIONS. EXEMPLES

6.2.1.1. Définition

Soit E un K-espace vectoriel. On dit qu'une partie F de E est un **sous-espace vectoriel** *ou simplement un* **sous-espace** *de E (en abrégé* : s. e. v.) *si F vérifie les conditions suivantes :*

a) *F n'est pas vide.*

b) *Les relations $x \in F$ et $y \in F$ entraînent $\lambda x + \mu y \in F$ quels que soient $\lambda, \mu \in K$.*

Faisons $\lambda = 1$ et $\mu = -1$ dans la condition **b)** ; alors les relations $x \in E$ et $y \in F$ impliquent $x - y \in F$; donc, puisque $F \neq \emptyset$, F est un sous-groupe du groupe additif E. Si dans la condition **b)** on fait maintenant $\mu = 0$, on voit que les relations $x \in F$ et $\lambda \in K$ entraînent $\lambda x \in F$. On peut donc définir une application $(\lambda, x) \longmapsto \lambda x$ de $K \times F$ dans F et F, muni des lois induites par les lois $(x, y) \longmapsto x + y$ et $(\lambda, x) \longmapsto \lambda x$ est un K-espace vectoriel, ce qui justifie la locution « sous-espace vectoriel ».

6.2.1.2. Exemple

Soit E un K-espace vectoriel. Les parties $\{0\}$ et E sont des sous-espaces vectoriels de E, dits **triviaux**. Tout sous-espace différent de ces deux sous-espaces est dit **propre**.

6.2.1.3. Exemple

Soit $n \in \mathbb{N}$ L'ensemble $K_n[X]$ des polynômes à une indéterminée X, à coefficients dans le corps commutatif K, de degré $\leq n$, est un sous-espace vectoriel de $K[X]$.

En effet, quels que soient les polynômes P et Q et les scalaires λ et μ, on a

$$\deg(\lambda P + \mu Q) \leq \sup\big(\deg(P),\ \deg(Q)\big)\ .$$

Donc si $\deg(P) \leq n$ et $\deg(Q) \leq n$, alors $\deg(\lambda P + \mu Q) \leq n$; par suite $K_n[X]$ est bien un sous-espace vectoriel de $K[X]$.

6.2.1.4. Exemple

L'ensemble $\mathcal{C}(I, \mathbb{C})$ des fonctions continues sur un intervalle I de la droite réelle et à valeurs complexes, est un sous-espace vectoriel de l'espace vectoriel $\mathcal{F}(I, \mathbb{C})$ de toutes les fonctions définies sur I et à valeurs complexes.

De même l'ensemble $\mathcal{D}(I, \mathbb{C})$ des fonctions dérivables sur I et à valeurs complexes est un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{C})$.

6.2.1.5. Exemple

Soit E un K-espace vectoriel et soit x un vecteur non nul de E. L'ensemble Kx des vecteurs de la forme λx, où $\lambda \in K$, est un sous-espace vectoriel de E. On l'appelle la **droite vectorielle engendrée par** x.

6.2.1.6. Exemple

Soit E un K-espace vectoriel et soient x et y deux vecteurs de E tels que $x \neq 0$ et $y \notin Kx$. L'ensemble des vecteurs de la forme $\lambda x + \mu y$, où $\lambda, \mu \in K$, est un sous-espace vectoriel de E. On l'appelle le plan **vectoriel engendré par** x **et** y.

6.2.2. INTERSECTION DE SOUS-ESPACES VECTORIELS. SOUS-ESPACE ENGENDRÉ PAR UNE PARTIE D'UN ESPACE VECTORIEL

6.2.2.1. Théorème

Soit $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels d'un K-espace vectoriel E. Alors $F = \bigcap_{i \in I} F_i$ est un sous-espace vectoriel de E.

Démonstration. Les F_i étant des sous-groupes du groupe additif E, on a $0 \in F_i$ pour tout $i \in I$; donc $0 \in F$ et $F \neq \emptyset$. Soient x et y des éléments de F ; alors pour tout $i \in I$, x et y appartiennent à F_i. Donc quels que soient les scalaires λ et μ de K, $\lambda x + \mu y \in F_i$ puisque F_i est un sous-espace vectoriel de E. Par suite $\lambda x + \mu y \in F$ et F est bien un sous-espace vectoriel de E.

On notera que la réunion d'une famille de sous-espaces n'est pas toujours un sous-espace (considérer par exemple deux droites distinctes dans le plan).

Mais si la réunion de deux sous-espaces quelconques de la famille est toujours contenue dans un élément de la famille, alors cette réunion est un sous-espace vectoriel.

Soit A une partie d'un K-espace vectoriel E. Il existe des sous-espaces vectoriels de E contenant A (par exemple E lui-même). L'intersection de tous ces sous-espaces vectoriels est le plus petit sous-espace vectoriel (pour l'inclusion) contenant A. On l'appelle le **sous-espace vectoriel engendré par** A et on le note $\mathrm{Vect}(A)$.

Si $\mathrm{Vect}(A) = E$, on dit que A est une **partie génératrice de** E.

6.2.3. ESPACES VECTORIELS QUOTIENTS

Soit E un espace vectoriel sur le corps K et soit F un sous-espace vectoriel de E. La relation

$$x \equiv y \pmod{F} \iff x - y \in F$$

est une relation d'équivalence sur E (à vérifier !) compatible avec la loi de groupe de E, c'est-à-dire :

$$x \equiv y \text{ et } x' \equiv y' \pmod{F} \Longrightarrow x + x' \equiv y + y' \pmod{F}.$$

Dans l'ensemble quotient, noté E/F, des classes d'équivalence $\overline{x} = x + F$ modulo F, définissons une loi interne en posant

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Cette loi confère à E/F une structure de groupe abélien (voir le Théorème 3.4.2.3).

Posons de plus

$$\lambda\overline{x} = \overline{\lambda x}$$

quels que soient $\overline{x} \in E/F$ et $\lambda \in K$.

Cette définition sera justifiée si nous montrons que la classe obtenue ne dépend que de $\overline{x}$ et de λ et non du représentant x choisi. Soient donc x et y deux représentants d'une même classe ; on a $x - y \in F$. Alors $\lambda(x-y) = \lambda x - \lambda y \in F$ puisque F est un sous-espace vectoriel de E. On a donc bien $\lambda x \equiv \lambda y \pmod{F}$, c'est-à-dire $\overline{\lambda x} = \overline{\lambda y}$.

On vérifie facilement que E/F, muni de ces deux lois, est un K-espace vectoriel. On l'appelle l'**espace vectoriel quotient de** E par F.

6.2.4. SOMME DE SOUS-ESPACES VECTORIELS

Nous avons observé que la réunion de deux sous-espaces vectoriels d'un K-espace vectoriel E n'est pas, en général, un sous-espace vectoriel de E. On est donc amené à introduire une autre opération : la somme d'une famille de sous-espaces vectoriels.

6.2.4.1. Définition

Soit $E_1, ..., E_n$ une famille finie de sous-espaces vectoriels d'un K-espace vectoriel E. On appelle **somme** *des sous-espaces $E_1, ..., E_n$, et on note $E_1 + ... + E_n$, ou $\sum_{i=1}^{n} E_i$, l'ensemble des éléments x de E qui sont de la forme*

$$x = x_1 + ... + x_n \text{ où } x_1 \in E_1, ..., x_n \in E_n.$$

Plus généralement, si $(E_i)_{i \in I}$ est une famille de sous-espaces vectoriels de E, on appelle **somme** *des sous-espaces E_i et on note $\sum_{i \in I} E_i$, l'ensemble des sommes finies de la forme $\sum_{i \in J} x_i$ où J est une partie finie de I et où pour tout $i \in J, x_i \in E_i$.*

6.2.4.2. Théorème

Soient E un K-espace vectoriel et $E_1, ..., E_n$ $(n \geq 2)$, n sous-espaces vectoriels de E. La somme $E_1 + ... + E_n$ est le sous-espace vectoriel engendré par $E_1 \cup E_2 \cup ... \cup E_n$.

Démonstration. Montrons d'abord que $\mathcal{S} = E_1 + ... + E_n$ est un sous-espace vectoriel de E.

Il est clair que $0 \in \mathcal{S}$ donc $\mathcal{S} \neq \emptyset$. Soient x et y deux éléments de $\mathcal{S}$; on a :

$$x = x_1 + ... + x_n \text{ et } y = y_1 + ... + y_n$$

avec $x_i \in E_i$ et $y_i \in E_i$ $(1 \leq i \leq n)$.

Quels que soient les scalaires λ et μ,

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1) + ... + (\lambda x_n + \mu y_n).$$

Chaque E_i étant un sous-espace vectoriel, $\lambda x_i + \mu y_i \in E_i$ pour tout indice $i \in \{1, ..., n\}$. Donc $\lambda x + \mu y \in \mathcal{S}$ et $\mathcal{S}$ est bien un sous-espace vectoriel de E.

Montrons maintenant que $\mathcal{S}$ est le plus petit sous-espace vectoriel de E (au sens de l'inclusion) contenant la réunion $E_1 \cup ... \cup E_n$.

Soit $x_i \in E_i$; on a $x_i = 0 + ... + 0 + x_i + 0 + ... + 0$ donc $E_i \subset \mathcal{S}$ pour tout i et par suite

$$E_1 \cup ... \cup E_n \subset \mathcal{S}.$$

De plus, si F est un sous-espace vectoriel de E contenant $E_1 \cup ... \cup E_n$, alors pour tout $i \in \{1, ..., n\}, x_i \in E_i \Longrightarrow x_i \in F$, donc $x_1 + ... + x_n \in F$ puisque F est un sous-espace vectoriel de E, et par suite $\mathcal{S} \subset F$.

Ainsi, $\mathcal{S}$ est le plus petit sous-espace vectoriel de E contenant $E_1 \cup ... \cup E_n$.

Si $x = x_1 + ... + x_n$ est un vecteur de $E_1 + ... + E_n$, il n'est pas dit que les vecteurs $x_1, ..., x_n$ sont uniques. Nous sommes ainsi conduits à examiner les conditions pour que la décomposition soit unique.

Conservons les notations précédentes. Tout élément x de $E_1 + ... + E_n$ s'écrit sous la forme

(6.2.4.1) $\qquad x = x_1 + ... + x_n$ avec $x_i \in E_i$ pour tout i.

Considérons l'application $f : E_1 \times ... \times E_n \longrightarrow E$ définie par

(6.2.4.2) $\qquad f(x_1, ..., x_n) = x_1 + ... + x_n.$

f est un homomorphisme de groupes abéliens et par définition de la somme $\sum_{i=1}^{n} E_i$, on a $\mathrm{Im}(f) = \sum_{i=1}^{n} E_i$.

• Si $\mathrm{Ker}(f) \neq \{0\}$, c'est-à-dire si f n'est pas injectif, il existe un élément $(y_1, ..., y_n)$ non nul de $E_1 \times ... \times E_n$ tel que $y_1 + ... + y_n = 0$. Alors on peut écrire

$$x = (x_1 + y_1) + ... + (x_n + y_n) \text{ avec } x_i + y_i \in E_i \text{ pour tout } i,$$

ce qui montre que la décomposition (6.2.4.1) n'est pas unique.

• Si $\mathrm{Ker}(f) = \{0\}$ c'est-à-dire si f est injectif, et si x admet une autre décompoition

$$x = x'_i + ... + x'_n \text{ avec } x'_i \in E_i \text{ pour tout } i,$$

on a par soustraction :

$$(x_1 - x'_1) + (x_2 - x'_2) + ... + (x_n - x'_n) = 0,$$

d'où $(x_1 - x'_1,\ x_2 - x'_2, ..., x_n - x'_n) \in \mathrm{Ker}(f) = \{0\}$.

Par suite $x_1 = x'_1, x_2 = x'_2, ..., x_n = x'_n$ et tout $x \in E_1 + ... + E_n$ s'écrit de **manière unique** sous la forme $x = x_1 + ... + x_n$ avec $x_i \in E_i$ pour tout $i \in \{1, ..., n\}$.

Ces remarques nous amènent à poser la définition suivante :

6.2.4.3. Définition

Soit $(E_i)_{1 \leq i \leq n}$ une famille finie de sous-espaces d'un K-espace vectoriel E. On dit que les E_i sont **linéairement indépendants** *si l'application f est injective. On dit alors que la somme $E_1 + ... + E_n$ est* **directe** *et on écrit $E_1 \oplus ... \oplus E_n$.*

On a le théorème suivant :

6.2.4.4. Théorème

Soit $E_1, ..., E_n$ une famille finie de sous-espaces d'un K-espace vectoriel E. Les conditions suivantes sont équivalentes :

a) *Les sous-espaces $E_1, ..., E_n$ sont linéairement indépendants.*

b) $E_i \cap \sum_{j \neq i} E_j = \{0\}$ *pour tout* $i \in I = \{1, ..., n\}$.

Démonstration. a) $\Longrightarrow$ **b)** Fixons un entier $i \in I$ et soit $x \in E_i \cap \sum_{j \neq i} E_j$. On peut écrire x sous la forme $x = \sum_{j \neq i} x_j$, avec $x_j \in E_j$ pour $j \neq i$. Soit $y = (y_1, ..., y_n)$ l'élément de $E_1 \times ... \times E_n$ tel que $y_i = x$ et $y_j = -x_j$ si $j \neq i$. f désignant l'application définie par (6.2.4.2), on a $f(y_1, ..., y_n) = 0$. Donc $y = 0$, d'où $x = 0$ et **b)** est démontré.

b) $\Longrightarrow$ **a)** Supposons la condition **b)** vérifiée et soit $x = (x_1, ..., x_n)$ un élément de $E_1 \times ... \times E_n$ tel que $f(x_1, ..., x_n) = x_1 + x_2 + ... + x_n = 0$. Fixons un entier $i \in I$. On a $x_i = \sum_{j \in I, j \neq i} (-x_j)$. Comme $x_i \in E_i$ et $\sum_{j \in I, j \neq i} (-x_j) \in \sum_{j \neq i} E_j$, on obtient $x_i = 0$; ceci étant vrai pour tout $i \in I$, on a $x = 0$, c'est-à-dire $\mathrm{Ker}(f) = \{0\}$. □

6.2.4.5. Corollaire

Soit E un K-espace vectoriel et soient E_1 et E_2 deux sous-espaces vectoriels de E. Les conditions suivantes sont équivalentes :

a) *E_1 et E_2 sont linéairement indépendants.*

b) $E_1 \cap E_2 = \{0\}$.

6.2.4.6. Définition

On dit que deux sous-espaces vectoriels d'un K-espace vectoriel E sont **supplémentaires** *dans E s'ils sont linéairement indépendants i.e. si $E = E_1 \oplus E_2$.*

D'après ce qui précède, E_1 et E_2 sont supplémentaires dans E si et seulement si $E = E_1 + E_2$ et $E_1 \cap E_2 = \{0\}$.

6.2.4.7. Remarques

a) Un sous-espace vectoriel donné peut admettre plusieurs sous-espaces supplémentaires. Ainsi si $E = \mathbb{R}^2$, considérons les sous-espaces

$$E_1 = \{(x, 0) : x \in \mathbb{R}\}$$
$$E_2 = \{(0, x) : x \in \mathbb{R}\}$$
$$E_3 = \{(x, x) : x \in \mathbb{R}\}$$

On vérifie facilement que E_2 et E_3 sont des sous-espaces supplémentaires de E_1 dans E.

b) On démontre que tout sous-espace vectoriel F d'un espace vectoriel E admet (au moins) un sous-espace supplémentaire. Nous démontrerons ce résultat dans le cas des espaces vectoriels de dimension finie (voir le Théorème 8.1.3.1).

6.2.4.8. Exemple

Soit E l'espace vectoriel formé par les fonctions réelles d'une variable réelle. Soient E_1 l'ensemble des fonctions paires et E_2 l'ensemble des fonctions impaires. Alors E_1 et E_2 sont des sous-espaces vectoriels supplémentaires dans E. En effet, pour toute fonction f, $f(x)$ s'écrit de manière unique sous la forme: $f(x) = h(x) + g(x)$, où

$$h(x) = \frac{f(x) + f(-x)}{2} \in E_1 \text{ et } g(x) = \frac{f(x) - f(-x)}{2} \in E_2.$$

6.2.4.9. Exemple

Soient E_1 et E_2 deux espaces vectoriels sur le même corps K et soit $E = E_1 \times E_2$ l'espace vectoriel produit (voir l'Exemple 6.1.3.4). On peut considérer E_1 et E_2 comme des sous-espaces de E de la façon suivante: on identifie l'élément x_1 de E_1 et l'élément $(x_1, 0)$ de E; de même λx_1 et $(\lambda x_1, 0)$ seront identifiés pour tout $\lambda \in K$.

Pour E_2, on aurait de même

$$x_2 = (0, x_2), \quad \lambda x_2 = (0, \lambda x_2) \quad \text{pour tout } \lambda \in K.$$

Si $(x_1, x_2) \in E$, on peut écrire $(x_1, x_2) = (x_1, 0) + (0, x_2)$ avec $(x_1, 0) \in E_1$ et $(0, x_2) \in E_2$. Donc $E = E_1 + E_2$.

D'autre part, si $(x_1, x_2) \in E_1 \cap E_2$, alors la relation $(x_1, x_2) \in E_1$, entraîne $x_2 = 0$ et la relation $(x_1, x_2) \in E_2$ entraîne $x_1 = 0$; donc $(x_1, x_2) = 0$ et par suite $E_1 \cap E_2 = \{0\}$. Par conséquent, E_1 et E_2 sont deux sous-espaces supplémentaires dans E.

6.3. Familles génératrices. Familles libres. Bases

6.3.1. FAMILLES GÉNÉRATRICES

Si E est un K-espace vectoriel, on appelle **système de vecteurs** ou **famille finie de vecteurs** de E, toute partie finie de E.

6.3.1.1. Définition

Soient E un K-espace vectoriel et $\{x_1, ..., x_n\}$ une famille finie de n vecteurs de E. *On appelle* **combinaison linéaire** *de $x_1, ..., x_n$ tout vecteur $x \in E$* de la forme:

$$x = \lambda_1 x_1 + ... + \lambda_n x_n.$$

où $\lambda_1, ..., \lambda_n$ *sont des scalaires appelés* **coefficients** *de la combinaison linéaire.*

Plus généralement, soit A une partie d'un K-espace vectoriel E. On appelle **combinaison linéaire** *des éléments de A tout vecteur $x \in E$ possédant la*

propriété suivante : il existe un entier naturel n, une famille $x_1, ..., x_n$ de n vecteurs de A et une famille $\lambda_1, ..., \lambda_n$ de n scalaires de K tels que

$$x = \lambda_1 x_1 + ... + \lambda_n x_n.$$

6.3.1.2. Exemple

Dans $K^n (n \geq 2)$, considérons les n vecteurs

$$e_1 = (1, 0, ..., 0), \quad e_2 = (0, 1, 0, ..., 0), ..., \quad e_n = (0, ..., 0, 1).$$

Tout vecteur $x = (\lambda_1, ..., \lambda_n)$ de l'espace vectoriel K^n est combinaison linéaire de la famille $\{e_1, ..., e_n\}$ car

$$\begin{aligned}(\lambda_1, ..., \lambda_n) &= (\lambda_1, 0, ..., 0) + (0, \lambda_2, ..., 0) + ... + (0, ..., \lambda_n) \\ &= \lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n.\end{aligned}$$

Cette notion de combinaison linéaire va nous permettre de caractériser le sous-espace vectoriel engendré par une partie A d'un espace vectoriel E.

6.3.1.3. Théorème

Soient E un K-espace vectoriel et A une partie non vide de E. Alors, le sous-espace vectoriel engendré par A est l'ensemble des combinaisons linéaires des éléments de A.

Démonstration. Notons A' l'ensemble des combinaisons linéaires des éléments de A. si $x \in A$. on a $0 = x - x \in A'$, donc $A' \neq \emptyset$. Soient

$$x = \lambda_1 x_1 + ... + \lambda_n x_n \text{ et } y = \mu_1 y_1 + ... + \mu_m y_m$$

deux vecteurs de A'.

Alors pour tous scalaires λ et μ de K,

$$\lambda x + \mu y = \lambda\lambda_1 x_1 + ... + \lambda\lambda_n x_n + \mu\mu_1 y_1 + ... + \mu\mu_m y_m$$

est une combinaison linéaire des vecteurs $x_1, ..., x_n$, $y_1, ..., y_m$ de A. Donc $\lambda x + \mu y \in A'$ et par suite A' est un sous-espace vectoriel de E. En outre, $A \subset A'$ car pour tout $x \in A$, $x = 1 \cdot x \in A'$.

Soit F le sous-espace vectoriel engendré par A. F étant le plus petit sous-espace vectoriel contenant A, on a $F \subset A'$. Comme F est un sous-espace vectoriel contenant A, F contient toutes les combinaisons linéaires des éléments de A ; donc $A' \subset F$ et par suite $F = A'$.

6.3.1.4. Corollaire

Soient E un K-espace vectoriel, $x_1, ..., x_n$ des vecteurs de E. Le sous-espace vectoriel engendré par $x_1, ..., x_n$ est l'ensemble des combinaisons linéaires des x_i.

En particulier, pour tout vecteur non nul $x \in E$, le sous-espace engendré par x est la droite vectorielle $Kx = \{\lambda x : \lambda \in K\}$.

6.3.1.5. Définition

Soit E un K-espace vectoriel. On dit que les vecteurs $x_1, ..., x_n$ de E forment un **système de générateurs** *(ou une* **famille génératrice** *de E) si le sous-espace vectoriel engendré par $x_1, ..., x_n$ est égal à E, c'est-à-dire si pour tout x* de E, *il existe des scalaires $\lambda_1, ..., \lambda_n$ tels que $x = \lambda_1 x_1 + ... + \lambda_n x_n$.*

On dit que E est de **dimension finie**, s'il existe dans E une famille finie de générateurs de E. Dans le cas contraire, on dit que E est de **dimension infinie**.

6.3.2. FAMILLES LIBRES

6.3.2.1. Définition

Soit E un K-espace vectoriel. On dit que les vecteurs $x_1, ..., x_n$ de E sont **linéairement indépendants**, *ou que la* **famille** $\{x_1, ..., x_n\}$ *est* **libre** *si la relation*

$$\lambda_1 x_1 + ... + \lambda_n x_n = 0$$

entraîne $$\lambda_1 = \lambda_2 = ... = \lambda_n = 0.$$

On dit que les vecteurs $x_1, ..., x_n$ sont **linéairement dépendants**, *ou que la famille $\{x_1, ..., x_n\}$ est* **liée** *s'il existe des scalaires $\lambda_1, ..., \lambda_n$ non tous nuls tels que*

$$\lambda_1 x_1 + ... + \lambda_n x_n = 0.$$

6.3.2.2. Remarques

a) Toute sous-famille d'une famille libre est une famille libre.

b) Les éléments d'une famille libre sont non nuls.

c) Toute sur-famille d'une famille liée est une famille liée. Ces assertions résultent immédiatement des définitions.

6.3.2.3. Exemple

Dans l'espace vectoriel K^n, les n vecteurs $e_1, ..., e_n$ de l'Exemple 6.3.1.2 sont linéairement indépendants car la relation

$$\lambda_1 e_1 + ... + \lambda_n e_n = 0 \text{ entraîne } \lambda_1 = ... = \lambda_n = 0.$$

6.3.2.4. Exemple

Soient E un K-espace vectoriel, $x \in E$. Alors $\{x\}$ est libre si et seulement si $x \neq 0$. En effet, si la famille $\{x\}$ n'est pas libre, il existe un scalaire λ non nul tel que $\lambda x = 0$; λ étant inversible dans K (car $\lambda \neq 0$), on a

$$\lambda^{-1}(\lambda x) = 0 = (\lambda^{-1}\lambda)x = 1 \cdot x = x.$$

Réciproquement, si $x = 0$, on a $1 \cdot x = 0$ et la famille $\{x\}$ n'est pas libre.

6.3.2.5. Exemple

Dans l'espace vectoriel $\mathbb{R}^3$, les vecteurs $x_1 = (1,0,0)$, $x_2 = (0,1,0)$ et $x_3 = (1,1,0)$ sont linéairement dépendants car

$$x_1 + x_2 - x_3 = 0.$$

6.3.2.6. Théorème

Soient E un K-espace vectoriel et $x_1, ..., x_n$ des vecteurs de E. Alors pour que la famille $\{x_1, ..., x_n\}$ soit liée, il faut et il suffit que l'un des vecteurs x_i soit combinaison linéaire des autres.

Démonstration. Supposons que la famille $\{x_1, ..., x_n\}$ soit liée; alors il existe des scalaires $\lambda_1, ..., \lambda_n$ non tous nuls tels que

$$\lambda_1 x_1 + ... + \lambda_n x_n = 0.$$

Si par exemple $\lambda_1 \neq 0$, on peut écrire

$$x_1 = -\frac{\lambda_2}{\lambda_1} x_2 - ... - \frac{\lambda_n}{\lambda_1} x_n,$$

donc x_1 est combinaisons linéaire de $x_2, ..., x_n$.

Réciproquement, si par exemple $x_1 = \alpha_2 x_2 + ... + \alpha_n x_n$ avec $\alpha_2, ..., \alpha_n \in K$, on a

$$1 \cdot x_1 + (-\alpha_2)x_2 + ... + (-\alpha_n)x_n = 0$$

ce qui montre que la famille $\{x_1, ..., x_n\}$ est liée puisque le coefficient de x_1 est 1, donc non nul.

6.3.3. BASES D'UN ESPACE VECTORIEL

Nous venons d'étudier deux classes importantes de vecteurs d'un espace vectoriel: les familles génératrices et les familles libres. Les familles qui sont à la fois génératrices et libres vont jouer un rôle fondamental dans toute la suite du cours.

6.3.3.1. Définition

Soit E un K-espace vectoriel. On dit qu'une famille $\{e_1, ..., e_n\}$ de vecteurs de E est une **base** *de E si les vecteurs $e_1, ..., e_n$ sont linéairement indépendants et engendrent E.*

Le résultat suivant caractérise les bases de E.

6.3.3.2. Théorème

Soient $e_1, ..., e_n$ des vecteurs d'un K-espace vectoriel E. Pour que la famille $\{e_1, ..., e_n\}$ soit une base de E, il faut et il suffit que tout vecteur $x \in E$ s'exprime de façon unique comme combinaison linéaire des e_i.

Démonstration. Supposons que la famille $\{e_1, ..., e_n\}$ soit une base de E. Alors tout vecteur $x \in E$ est combinaison linéaire des e_i ; il existe donc des scalaires $\lambda_1, ..., \lambda_n$ tels que

$$x = \lambda_1 e_1 + ... + \lambda_n e_n.$$

S'il existe des scalaires $\mu_1, ..., \mu_n$ tels qu'on ait aussi

$$x = \mu_1 e_1 + ... + \mu_n e_n$$

alors par soustraction, on obtient $(\lambda_1 - \mu_1)e_1 + ... + (\lambda_n - \mu_n)e_n = 0$.

Comme la famille $\{e_1, ..., e_n\}$ est libre, on a

$$\lambda_1 - \mu_1 = ... = \lambda_n - \mu_n = 0$$

c'est-à-dire $\lambda_1 = \mu_1, ..., \lambda_n = \mu_n$. La décomposition de x est bien unique.

Réciproquement supposons que tout vecteur de E s'écrit de façon unique comme combinaison linéaire de $e_1, ..., e_n$; la famille $\{e_1, ..., e_n\}$ est donc génératrice. Montrons qu'elle est libre. Par hypothèse, le vecteur nul s'écrit de façon unique sous la forme

$$0 \cdot e_1 + ... + 0 \cdot e_n = 0.$$

Alors la relation $\lambda_1 e_1 + ... + \lambda_n e_n = 0$,

montre que $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$, d'où le résultat.

6.3.3.3. Définition

Soient E un K-espace vectoriel et $(e_1, ..., e_n)$ une base de E. Pour tout vecteur $x \in E$, il existe un famille unique $\{\lambda_1, ..., \lambda_n\}$ de scalaires telle que

$$x = \lambda_1 e_1 + ... + \lambda_n e_n.$$

Les scalaires $\lambda_1, ..., \lambda_n$ s'appellent les **coordonnées** *ou* **les composantes de x par rapport à la base** $(e_1, ..., e_n)$.

6.3.3.4. Remarque

On démontre que tout espace vectoriel sur un corps K possède au moins une base. Nous démontrerons plus tard ce résultat dans le cas des espaces vectoriels de dimension finie.

6.3.3.5. Exemple

Dans l'espace vectoriel K^n $(n \geq 2)$, les n vecteurs $e_1, ..., e_n$ de l'Exemple 6.3.1.2 sont linéairement indépendants et engendrent K^n. La famille $\{e_1, ..., e_n\}$ est une base de K^n. On l'appelle la **base canonique** de K^n.

6.3.3.6. Exemple

Soit n un entier ≥ 0. Notons $K_n[X]$ l'ensemble des polynômes à une indéterminée X, à coefficients dans un corps commutatif K, de degré $\leq n$. Nous savons déjà (Exemple 6.2.1.3) que $K_n[X]$ est un sous-espace vectoriel de $K[X]$; et c'est donc un K-espace vectoriel.

Montrons que la famille

(6.3.3.1) $$\mathcal{B} = \{1, X, X^2, ..., X^n\}$$

est une base de $K_n[X]$.

Par définition, tout polynôme $P = a_0 + a_1X + ... + a_nX^n$ de $K_n[X]$ est combinaison linéaire d'éléments de $\mathcal{B}$ donc $\mathcal{B}$ est une famille génératrice de $K_n[X]$. Par conséquent $K_n[X]$ est de dimension finie.

D'autre part, la relation $\lambda_0 \cdot 1 + \lambda_1 X + ... + \lambda_n X^n = 0$
implique $\lambda_0 = \lambda_1 = ... = \lambda_n = 0$
puisqu'un polynôme est identiquement nul si et seulement si tous ses coefficients sont nuls ; donc $\mathcal{B}$ est une famille libre.

6.3.4. FAMILLES INFINIES

Les notions de familles génératrices, de familles libres et de bases peuvent se généraliser au cas des familles infinies de vecteurs mais la situation est plus délicate.

6.3.4.1. Définition

Soit I un ensemble fini ou non et soit $(\lambda_i)_{i \in I}$ une famille d'éléments du corps K. On dit que la famille $(\lambda_i)_{i \in I}$ est à **support fini** *ou que les λ_i sont* **presque tous nuls,** *si l'ensemble des indices i tels que $\lambda_i \neq 0$ est fini.*

Bien entendu, si I est un ensemble fini, cette définition n'a pas d'intérêt.

On dit que la famille $(\lambda_i)_{i \in I}$ est **triviale** si $\lambda_i = 0$ pour tout $i \in I$.

6.3.4.2. Définition

Soit $(x_i)_{i \in I}$ une famille de vecteurs d'un K-espace vectoriel E. On dit qu'un vecteur $x \in E$ est **combinaison linéaire** *de la famille $(x_i)_{i \in I}$ s'il existe une famille $(\lambda_i)_{i \in I}$ de scalaires à support fini telle que*

(6.3.4.1) $$x = \sum_{i \in I} \lambda_i x_i.$$

La famille $(\lambda_i)_{i\in I}$ étant à support fini, on remarquera qu'un nombre fini seulement de termes $\lambda_i x_i$ sont non nuls dans la somme (6.3.4.1). Par définition, $\sum_{i\in I} \lambda_i x_i$ désigne la somme de ces termes non nuls.

Si $(x_i)_{i\in I}$ est une famille d'éléments d'un K-espace vectoriel E, on démontre facilement (*cf.* démonstration du Théorème 6.3.1.3) que l'ensemble des combinaisons linéaires des x_i est le plus petit sous-espace vectoriel de E contenant tous les x_i pour tout $i \in I$. On l'appelle le **sous-espace vectoriel engendré par la famille** $(x_i)_{i\in I}$.

On dit que la famille $(x_i)_{i\in I}$ est une **famille génératrice** si le sous-espace vectoriel qu'elle engendre est égal à E.

La notion d'indépendance linéaire se généralise comme suit.

6.3.4.3. Définition

Soit $(x_i)_{i\in I}$ une famille de vecteurs d'un K-espace vectoriel E. On appelle **relation linéaire entre les** x_i, *toute famille $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls tels que*

$$\sum_{i\in I} \lambda_i x_i = 0.$$

On appelle **relation triviale**, toute famille triviale de scalaires (qui est toujours une relation linéaire entre les x_i).

On dit qu'une famille $(x_i)_{i\in I}$ de vecteur d'un K-espace vectoriel est **libre** ou que les x_i $(i \in I)$ sont **linéairement indépendants**, si la seule relation linéaire entre les x_i est la relation triviale.

Autrement dit, la famille $(x_i)_{i\in I}$ est libre si pour toute partie finie J de I, la relation $\sum_{i\in J} \lambda_i x_i = 0$ entraîne $\lambda_i = 0$ pour tout $i \in J$.

Un famille qui n'est pas libre est dite **liée**.

On appelle **base** de E, toute famille $(e_i)_{i\in I}$ d'éléments de E à la fois libre et génératrice.

Le théorème suivant se démontre exactement comme le théorème 6.3.3.2.

6.3.4.4. Théorème

Soit $(e_i)_{i\in I}$ une famille de vecteurs d'un K-espace vectoriel E. Pour que la famille $(e_i)_{i\in I}$ soit une base de E, il faut et il suffit que tout vecteur de E s'exprime de façon unique comme combinaison linéaire des e_i.

Si $(e_i)_{i\in I}$ est une base de E, pour tout vecteur $x \in E$, il existe une famille unique $(\lambda_i)_{i\in I}$ de scalaires presque tous nuls telle que

$$x = \sum_{i\in I} \lambda_i x_i.$$

Les scalaires λ_i s'appellent les **coordonnées** ou les **composantes** de x par rapport à la base $(e_i)_{i\in I}$.

Chapitre 7 : APPLICATIONS LINÉAIRES

En mathématiques, on est souvent amené à associer des « morphismes » à une structure donnée. Dans la théorie des espaces vectoriels, les morphismes sont des applications qui sont compatibles avec la structure de K-espace vectoriel.

Après avoir défini les applications linéaires d'un K-espace vectoriel dans un autre (ou dans lui-même) et donné quelques exemples élémentaires, nous examinons quelques propriétés générales de ces applications. En particulier, nous montrons que si E et F sont des K-espaces vectoriels l'ensemble $\mathcal{L}(E, F)$ des applications linéaires de E dans F est un K-espace vectoriel.

Nous étudions enfin un exemple important d'endomorphisme : les projecteurs.

7.1. Généralités

7.1.1. DÉFINITIONS

7.1.1.1. Définition

Soient E et F deux espaces vectoriels sur le même corps K. On dit qu'une application $u : E \longrightarrow F$ est **K-linéaire** ou est un **homomorphisme** si l'on a :

a) $u(x + y) = u(x) + u(y)$

b) $u(\lambda x) = \lambda\, u(x)$

quels que soient $x, y \in E$ et $\lambda \in K$.

Lorsqu'il n'y a pas d'ambiguïté sur le corps K, on dit simplement que u est une **application linéaire** ou un **morphisme d'espaces vectoriels.**

Une application linéaire de E dans lui-même s'appelle un **endomorphisme** de E ou un **opérateur linéaire dans** E. On appelle **automorphisme** de E tout endomorphisme bijectif de E.

Une application linéaire de E dans K s'appelle une **forme linéaire** sur E.

Une application linéaire bijective $u : E \longrightarrow F$ s'appelle un **isomorphisme** d'espace vectoriels. S'il existe un isomorphisme de E sur F on dit alors que les espaces vectoriels E et F sont **isomorphes** et on écrit $E \approx F$.

L'ensemble des applications K-linéaires de E dans F se note $\mathcal{L}_K(E, F)$ ou simplement $\mathcal{L}(E, F)$ si aucune confusion n'est à craindre. Cet ensemble est aussi noté $\mathrm{Hom}(E, F)$.

L'ensemble des endomorphismes de E est noté $\mathcal{L}_K(E)$ ou $\mathcal{L}(E)$. On le note aussi $\mathrm{End}(E)$.

L'ensemble des automorphisme de E est noté $GL_K(E)$ ou $GL(E)$ et s'appelle le **groupe linéaire général** de E (nous justifierons plus loin au Corollaire 7.2.1.2 cette dénomination).

7.1.1.2. Remarques

a) Si dans la condition **a)** de la Définition 7.1.1.1, on pose $x = 0$, on obtient $u(0) = 0$. De même, en prenant $\lambda = -1$ dans la condition **b)**, on obtient $u(-x) = -u(x)$.

b) Une application $u : E \longrightarrow F$ est linéaire si et seulement si $u(\lambda x + \mu y) = \lambda u(x) + \mu u(y)$ quels que soient $x, y \in E$, $\lambda, \mu \in K$.

7.1.2. EXEMPLES

7.1.2.1. Exemple

Soient E et F deux K-espaces vectoriels. L'application $0 : E \longrightarrow F$ définie par $0(x) = 0$ pour tout $x \in E$ est linéaire. On l'appelle **l'application nulle** de E dans F.

7.1.2.2. Exemple

L'application identique, notée 1_E ou Id_E, d'un K-espace vectoriel E est linéaire. C'est même un automorphisme de E.

7.1.2.3. Exemple

Soit E un K-espace vectoriel et soit $\propto$ un élément non nul de K. On appelle **homothétie** de rapport $\propto$ l'application $h_\propto : E \longrightarrow E$ telle que $h_\propto(x) = \propto \cdot x$ pour tout $x \in E$. $h_\propto$ est un élément de $GL(E)$.

7.1.2.4. Exemple

Soient E un K-espace vectoriel et F un sous-espace de E. L'application canonique $\pi : E \longrightarrow E/F$ qui, à tout vecteur x de E associe sa classe $\dot{x}$ dans l'espace vectoriel quotient E/F, est K-linéaire d'après la définition de la structure vectorielle de E/F. On l'appelle le **morphisme canonique.**

7.1.2.5. Exemple

Soient $E_1, ..., E_n$ des espaces vectoriels sur le même corps K et $E = E_1 \times ... \times E_n$ leur produit (*cf.* Exemple 6.1.3.4).

Pour $1 \leq i \leq n$, l'application

$$pr_i : E_1 \times ... \times E_n \longrightarrow E_i$$

définie par $pr_i(x_1, ..., x_n) = x_i$ est linéaire. On l'appelle la $i^{\text{ème}}$ **projection.**

7.2. Propriétés des applications linéaires

Nous donnons dans ce paragraphe quelques propriétés générales des applications linéaires. D'autres propriétés classiques seront exposées lorsque nous étudierons les espaces vectoriels de dimension finie.

7.2.1. COMPOSÉE DE DEUX APPLICATIONS LINÉAIRES

7.2.1.1. Théorème

Soient E, F et G trois espaces vectoriels sur le corps K. Soient $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, G)$. Alors :

a) *L'application composée vou est une application linéaire de E dans G.*

b) *Si u est un isomorphisme de E sur F, l'application réciproque u^{-1} est un isomorphisme de F sur E.*

Démonstration.

a) De la linéarité de u et de v, nous déduisons, quels que soient $x, y \in E$, $\lambda, \mu \in K$,

$$\begin{aligned}(vou)(\lambda x + \mu y) &= v\left[u(\lambda x + \mu y)\right] = v\left[\lambda u(x) + \mu u(y)\right] \\ &= \lambda v\left(u(x)\right) + \mu v\left(u(y)\right) \\ &= \lambda(vou)(x) + \mu(vou)(y).\end{aligned}$$

b) L'application réciproque d'une application bijective étant bijective, il suffit de montrer que u^{-1} est linéaire.

Quels que soient les éléments x et y de F, il existe des éléments x' et y' uniques de E tels que $u(x') = x$ et $u(y') = y$. Quels que soient $\lambda, \mu \in K$, on a alors

$$\begin{aligned}u^{-1}(\lambda x + \mu y) &= u^{-1}\left(\lambda u(x') + \mu u(y')\right) \\ &= u^{-1}\left(u(\lambda x' + \mu y')\right) \\ &= \lambda x' + \mu y' \quad (\text{car } u^{-1}ou = \mathrm{Id}_E) \\ &= \lambda u^{-1}(x) + \mu u^{-1}(y)\end{aligned}$$

d'où la linéarité de u^{-1}.

7.2.1.2. Corollaire

L'ensemble $GL(E)$ des automorphismes d'un K-espace vectoriel E est un groupe pour la loi de composition des applications.

On sait que la composée de deux bijections est un bijection et que la composée de deux applications linéaires est linéaire.

Donc, si $u, v \in GL(E)$, alors $uov \in GL(E)$.

D'autre part, d'après le Théorème 7.2.1.1 **b)**, si $u \in GL(E)$, alors $u^{-1} \in GL(E)$.

Nous avons ainsi démontré que $GL(E)$ (qui est non vide puisque l'application identique $1_E \in GL(E)$) est un sous-groupe du groupe des permutations de E.

7.2.1.3. Remarque

Si $u, v \in GL(E)$, on a d'après le Théorème 2.2.4.2 **d)** :

$$(v \circ u)^{-1} = u^{-1} \circ v^{-1}$$

7.2.2. IMAGE ET NOYAU D'UNE APPLICATION LINÉAIRE

7.2.2.1. Théorème

Soient E et F deux K-espaces vectoriels et soit $u \in \mathcal{L}(E, F)$. Alors :

a) *L'image par u d'un sous-espace vectoriel de E est un sous-espace vectoriel de F.*

b) *L'image réciproque par u d'un sous-espace vectoriel de F est un sous-espace vectoriel de E.*

Démonstration. a) Soit A un sous-espace vectoriel de E. Comme $0 \in A$, $0 = u(0) \in u(A)$ et $u(A) \neq \emptyset$. Soient $y, z \in u(A)$, $\lambda, \mu \in K$. Il existe x et x' dans A tels que $y = u(x)$ et $z = u(x')$. Comme u est linéaire, on a

$$\lambda y + \mu z = \lambda u(x) + \mu u(x') = u(\lambda x + \mu x').$$

Or $\lambda x + \mu x' \in A$ puisque A est un sous-espace vectoriel de E. Donc $\lambda y + \mu z \in u(A)$ et $u(A)$ est un sous-espace vectoriel de F.

Démontrons **b)**. Soit B un sous-espace vectoriel de F. $u^{-1}(B)$ contient 0, puisque $u(0) = 0 \in B$. Donc $u^{-1}(B) \neq \emptyset$.

Soient x et y deux éléments de $u^{-1}(B)$, λ et μ deux scalaires. On a par définition $u(x) \in B$ et $u(y) \in B$. D'où

$$u(\lambda x + \mu y) = \lambda u(x) + \mu u(y) \in B$$

car B est un sous-espace vectoriel de F. Donc $\lambda x + \mu y \in u^{-1}(B)$.

7.2.2.2. Définition

Soient E et F deux K-espaces vectoriels et soit $u \in \mathcal{L}(E, F)$.

a) *On appelle* **image** *de u, et on note* $\mathrm{Im}(u)$, *le sous-espace vectoriel $u(E)$ de F.*

b) *On appelle* **noyau** *de u, et on note* $\mathrm{Ker}(u)$, *le sous-espace vectoriel $u^{-1}(\{0\})$ de E.*

7.2.2.3. Théorème

Soient E et F deux K-espaces vectoriels et $u \in \mathcal{L}(E, F)$.

a) *u est injective si et seulement si* $\mathrm{Ker}(u) = \{0\}$.

b) *u est surjective si et seulement si* $\mathrm{Im}(u) = F$.

Démonstration. a) découle aussitôt du Théorème 3.3.2.4 puisque u est un morphisme de groupes.

b) résulte immédiatement de la définition de $\mathrm{Im}(u)$.

7.2.3. APPLICATIONS LINÉAIRES ET FAMILLES DE VECTEURS

7.2.3.1. Théorème

Soient E et F deux K-espaces vectoriels et $u \in \mathcal{L}(E, F)$.

a) *Si $(x_i)_{i \in I}$ est une famille génératrice de E, la famille $\big(u(x_i)\big)_{i \in I}$ est une famille génératrice de* $\mathrm{Im}(u)$.

b) *Si $(x_i)_{i \in I}$ est une famille liée de vecteurs de E,* la famille $\big(u(x_i)\big)_{i \in I}$ *est une famille liée de vecteurs de F.*

Démonstration. a) Soit $y \in \mathrm{Im}(u)$; il existe $x \in E$ tel que $y = u(x)$. Puisque $(x_i)_{i \in I}$ est une famille génératrice, il existe une famille $(\lambda_i)_{i \in I}$ de scalaires presque tous nuls telle que

$$x = \sum_{i \in I} \lambda_i x_i .$$

On en déduit (puisque u est linéaire et la famille de scalaires à support fini) :

$$u(x) = \sum_{i \in I} \lambda_i u(x_i),$$

donc $u(x)$ est combinaison linéaire des $u(x_i)$.

b) Soit $(x_i)_{i\in I}$ une famille liée de vecteurs de E. Il existe donc une famille non triviale de scalaires $(\lambda_i)_{i\in I}$ telle que $\sum_{i\in I}\lambda_i x_i = 0$. D'où $u\left(\sum_{i\in I}\lambda_i x_i\right) = \sum_{i\in I}\lambda_i u(x_i) = 0$ car u est linéaire et la famille de scalaires à support fini. Par suite la famille de vecteurs $\left(u(x_i)\right)_{i\in I}$ est liée.

Attention. L'image d'une famille génératrice de E n'est une famille génératrice de F que si u est surjective.

L'image d'une famille libre de E n'est pas, en général, une famille libre de F. Toutefois on a le résultat suivant.

7.2.3.2. Théorème

Soient E et F deux K-espaces vectoriels et soit $u \in \mathcal{L}(E, F)$. Les propositions suivantes sont équivalentes :

a) *u est injective.*

b) *L'image par u de toute famille libre de E est une famille libre de F.*

Démonstration. Démontrons que **a)** $\Longrightarrow$ **b)**. Soit $(x_i)_{i\in I}$ une famille libre de E et soit $(\lambda_i)_{i\in I}$ une famille de scalaires presque tous nuls telle que

$$\sum_{i\in I}\lambda_i u(x_i) = 0,$$

ou encore, puisque u est linéaire :

$$u\left(\sum_{i\in I}\lambda_i x_i\right) = 0.$$

u étant injective, on en déduit

$$\sum_{i\in I}\lambda_i x_i = 0,$$

puisque $\mathrm{Ker}(u) = \{0\}$.

La famille $(x_i)_{i\in I}$ étant libre, la relation linéaire $(\lambda_i)_{i\in I}$ est la relation triviale. La famille $\left(u(x_i)\right)_{i\in I}$ est donc libre.

b) $\Longrightarrow$ **a)** Soit $x \in \mathrm{Ker}(u)$. L'image de la famille $\{x\}$ est la famille $\{0\}$ qui est liée ; la famille $\{x\}$ est donc liée, *i.e.* $x = 0$ et u est injective.

7.2.3.3. Théorème

Soient E et F deux K-espaces vectoriels et $u \in \mathcal{L}(E, F)$. Les propositions suivantes sont équivalentes :

a) *u est un isomorphisme de E sur F.*

b) *L'image par u de toute base de E est une base de F.*

Démonstration. a) $\Longrightarrow$ **b)** Supposons que u soit un isomorphisme de E sur F et soit $(e_i)_{i\in I}$ une base de E. Alors, d'après les Théorèmes 7.2.3.1 et 7.2.3.2, $\big(u(e_i)\big)_{i\in I}$ est une base de F puisque u est à la fois injectif et surjectif, donc **b)** est vérifiée.

b) $\Longrightarrow$ **a)** Soit $(e_i)_{i\in I}$ une base de E dont l'image par u est une base de F. Montrons que u est injective. Soit $x \in \mathrm{Ker}(u)$; on a $x = \sum_{i\in I} x_i e_i$ où $(x_i)_{i\in I}$ est une famille de scalaires presque tous nuls. Par linéarité, on a $u(x) = \sum_{i\in I} x_i u(e_i) = 0$. La famille $\big(u(e_i)\big)_{i\in I}$ étant libre, la famille $(x_i)_{i\in I}$ est la famille triviale, donc $x = 0$ et u est bien injective.

Montrons que u est surjective. Soit $y \in F$. $\big(u(e_i)\big)_{i\in I}$ étant une base de F, y s'écrit de façon unique $y = \sum_{i\in I} \lambda_i u(e_i)$ où $(\lambda_i)_{i\in I}$ est une famille de scalaires presque tous nuls. Alors $y = u(x)$ avec $x = \sum_{i\in I} \lambda_i e_i$, donc u est bien surjective.

7.2.3.4. Théorème

Soient E et F deux K-espaces vectoriels. Soit $(e_i)_{i\in I}$ une base de E et soit $(y_i)_{i\in I}$ une famille de vecteurs de F indexée par le même ensemble d'indices I.

a) *Il existe une application linéaire et une seule u de E dans F telle que $u(e_i) = y_i$ pour tout $i \in I$.*

b) *u est injective si et seulement si $(y_i)_{i\in I}$ est une famille libre de F.*

c) *u est surjective si et seulement si $(y_i)_{i\in I}$ est une famille génératrice de F.*

d) *u est un isomorphisme de E sur F si et seulement si $(y_i)_{i\in I}$ est une base de F.*

Démonstration. a) Tout vecteur x de E s'écrit de façon unique sous la forme

$$x = \sum_{i\in I} \lambda_i e_i$$

où les scalaires $(\lambda_i)_{i\in I}$ sont presque tous nuls.

En posant

$$u(x) = \sum_{i\in I} \lambda_i y_i,$$

on définit une application u de E dans F et il est clair que $u(e_i) = y_i$ pour tout i, puisque $e_i = \sum_{j\in I} \lambda_j e_j$ avec $\lambda_i = 1$ et $\lambda_j = 0$ si $j \neq i$.

Montrons que u est linéaire.

Soient $x = \sum_{i \in I} \lambda_i e_i$ et $y = \sum_{i \in I} \mu_i e_i$ deux vecteurs de E. Quels que soient les scalaires $\propto$ et λ, on a, par définition de u :

$$\begin{aligned} u(\propto x + \lambda y) &= u\left(\sum_{i \in I} (\propto \lambda_i + \lambda \mu_i) e_i\right) = \sum_{i \in I} (\propto \lambda_i + \lambda \mu_i) y_i \\ &= \propto \sum_{i \in I} \lambda_i y_i + \lambda \sum_{i \in I} \mu_i y_i = \propto u(x) + \lambda u(y). \end{aligned}$$

On a ainsi établi l'existence et la linéarité de u.

Soit $v \in \mathcal{L}(E, F)$ telle que $v(e_i) = y_i$ pour tout $i \in I$. Pour tout vecteur $x = \sum_{i \in I} \lambda_i e_i$, on a

$$v(x) = \sum_{i \in I} \lambda_i v(e_i) = \sum_{i \in I} \lambda_i y_i = u(x).$$

Donc $v = u$, d'où l'unicité de u.

b) Supposons u injective. Soit $(\lambda_i)_{i \in I}$ une famille de scalaires presque tous nuls telle que

$$\sum_{i \in I} \lambda_i y_i = 0.$$

Cette relation s'écrit $\sum_{i \in I} \lambda_i u(e_i) = 0$, ou encore, puisque u est linéaire $u\left(\sum_{i \in I} \lambda_i e_i\right) = 0$. Comme u est injective, on en déduit $\sum_{i \in I} \lambda_i e_i = 0$. Comme $(e_i)_{i \in I}$ est une famille libre, la relation linéaire $(\lambda_i)_{i \in I}$ est la relation triviale, donc la famille $(y_i)_{i \in I}$ est libre.

Réciproquement, supposons la famille $(y_i)_{i \in I}$ libre et montrons que u est injective. Soit $x = \sum_{i \in I} \lambda_i e_i$ un élément de $\mathrm{Ker}(u)$, où la famille $(\lambda_i)_{i \in I}$ est à support fini. On a

$$u(x) = \sum_{i \in I} \lambda_i y_i = 0.$$

Comme $(y_i)_{i \in I}$ est une famille libre, la relation linéaire $(\lambda_i)_{i \in I}$ est triviale, donc $x = 0$ et u est injective.

c) On a les équivalences suivantes :
u est surjective $\iff$ pour tout $y \in F$, il existe $x \in E$ tel que $y = u(x) \iff$ pour tout $y \in F$, il existe une famille $(\lambda_i)_{i \in I}$ à support fini telle que $y = u\left(\sum_{i \in I} \lambda_i e_i\right) = \sum_{i \in I} \lambda_i y_i$, puisque u est linéaire.

Ainsi u est surjective si et seulement si la famille $(y_i)_{i\in I}$ est génératrice.

d) résulte immédiatement de **b)** et **c)**.

7.2.4. DÉCOMPOSITION CANONIQUE D'UNE APPLICATION LINÉAIRE

7.2.4.1. Théorème

Soient E et F deux K-espaces vectoriels, $u \in \mathcal{L}(E, F)$ et N le noyau de u.

La relation $x\mathcal{R}y \iff u(x) = u(y)$ est une relation d'équivalence dans E. Soit $\pi : E \longrightarrow E/N$ le morphisme canonique et soit $j : u(E) \longrightarrow F$ l'injection canonique. Alors, il existe un isomorphisme unique $\overline{u}$ de l'espace vectoriel quotient E/N sur le sous-espace $u(E)$ de F tel que :

$$j \circ \overline{u} \circ \pi = u.$$

Démonstration. On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence. De plus

$$\begin{aligned} x\mathcal{R}y &\iff u(x) = u(y) \iff u(x) - u(y) = u(x - y) = 0 \\ &\iff x - y \in N. \end{aligned}$$

Comme N est un sous-espace vectoriel de E, E/N est un K-espace vectoriel.

D'après l'Exemple 7.1.2.4, l'application canonique π est linéaire.

Rappelons que si X et Y sont deux ensembles tels que $X \subset Y$, l'injection canonique $j : X \longrightarrow Y$ est définie par $j(x) = x$ pour tout $x \in X$. Si on prend pour X, le sous-espace $u(E)$ de F, et pour Y l'espace F, alors il est évident que l'injection canonique est linéaire.

Rappelons que l'application $\overline{u} : E/N \longrightarrow u(E)$ est définie en posant :

$$\overline{u}\,(\overline{x}) = u(x)$$

pour tout $\overline{x} \in E/N$, où x est un représentant de la classe $\overline{x}$. $\overline{u}$ est une bijection ; c'est l'application déduite de u par passage au quotient (voir le Théorème 1.4.2.6).

Montrons que $\overline{u}$ est K-linéaire.

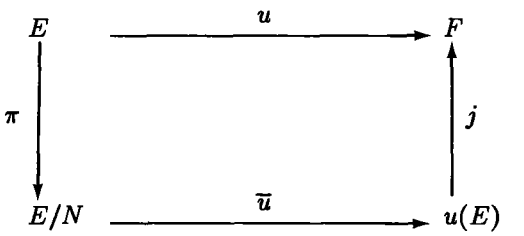
Soient $\overline{x}, \overline{y} \in E/N$. Quels que soient les scalaires λ et μ, on a :

$$\begin{aligned} \overline{u}(\lambda\overline{x} + \mu\overline{y}) &= \overline{u}\,\overline{(\lambda x + \mu y)} = u(\lambda x + \mu y) = \lambda u(x) + \mu u(y) \\ &= \lambda\overline{u}\,(\overline{x}) + \mu\overline{u}\,(\overline{y})\,. \end{aligned}$$

Ainsi $\overline{u}$ est une application linéaire bijective, c'est-à-dire un isomorphisme de E/N sur $u(E)$. La factorisation canonique de u s'écrit :

$$u = j \circ \overline{u} \circ \pi$$

et on a le diagramme suivant



appelé diagramme de **décomposition canonique** de u.

La bijection $\bar{u}$ s'appelle l'**isomorphisme canonique.**

7.2.4.2. Théorème

Soient E un K-espace vectoriel et E_1 un sous-espace de E. Si E_2 et E_3 sont deux sous-espaces supplémentaires de E_1 dans E, c'est-à-dire si $E = E_1 \oplus E_2 = E_1 \oplus E_3$, alors E_2 et E_3 sont isomorphes.

Démonstration. Par hypothèse, pour tout $x \in E$, il existe (x_1, x_2) unique dans $E_1 \times E_2$ tel que

$$x = x_1 + x_2.$$

De même il existe (x_1', x_3) unique dans $E_1 \times E_3$ tel que $x = x_1' + x_3$.

Soient u et v les endomorphismes de E définis par

$$u(x) = x_2 \text{ et } v(x) = x_3.$$

On a

$$\mathrm{Ker}(u) = \mathrm{Ker}(v) = E_1$$

et

$$\mathrm{Im}(u) = E_2, \ \mathrm{Im}(v) = E_3.$$

La décomposition canonique de u et v montre que E_2 et E_3 sont isomorphes à l'espace vectoriel quotient E/E_1. Donc E_2 et E_3 sont isomorphes.

7.3. L'espace vectoriel $\mathcal{L}(E, F)$

Soient E et F deux espaces vectoriels sur un corps commutatif K. Nous allons munir l'ensemble $\mathcal{L}(E, F)$ des applications linéaires de E dans F d'une structure de K-espace vectoriel. Pour cela, il nous faut définir la somme de deux applications linéaires et le produit d'une application linéaire par un scalaire.

7.3.1. ADDITION DANS $\mathcal{L}(E, F)$

7.3.1.1. Définition

Soient u et v deux éléments de $\mathcal{L}(E, F)$. On appelle **somme** *de u et v, et on note $u + v$, l'application de E dans F définie par :*

$$(u + v)(x) = u(x) + v(x) \quad \textit{pour tout } x \in E.$$

Montrons que $u + v$ est linéaire.

Quels que soient les vecteurs x, y de E et quels que soient les scalaires $\propto$ et β, on a :

$$\begin{aligned}(u + v)(\propto x + \beta y) &= u(\propto x + \beta y) + v(\propto x + \beta y)\\ &= \propto u(x) + \beta u(y) + \propto v(x) + \beta v(y)\\ &= \propto (u + v)(x) + \beta(u + v)(y).\end{aligned}$$

Muni de cette addition $(u, v) \longmapsto u + v$, $\mathcal{L}(E, F)$ est un groupe abélien ; on vérifie en effet facilement les relations suivantes :

$$\begin{aligned}(u + v) + w &= u + (v + w),\\ u + v &= v + u,\\ 0 + u &= u + 0,\\ u + (-u) &= 0\end{aligned}$$

l'application $-u$ étant définie par $(-u)(x) = -u(x)$ pour tout $x \in E$ et 0 étant l'application nulle (*cf.* Exemple 7.1.2.1).

7.3.2. PRODUIT D'UNE APPLICATION LINÉAIRE PAR UN SCALAIRE

7.3.2.1. Définition

Soit $u \in \mathcal{L}(E, F)$. On appelle **produit** *de u par le scalaire λ, et on note λu, l'application de E dans F, définie par*

$$(\lambda u)(x) = \lambda u(x) \quad \textit{pour tout } x \in E.$$

Montrons que λu est linéaire.

Soient x et y deux vecteurs de E et soient $\propto$ et β deux scalaires ; on a :

$$\begin{aligned}(\lambda u)(\propto x + \beta y) &= \lambda u(\propto x + \beta y) = \lambda\left(\propto u(x) + \beta u(y)\right)\\ &= \lambda \propto u(x) + \lambda\beta u(y) = \propto (\lambda u)(x) + \beta(\lambda u)(x).\end{aligned}$$

On vérifie facilement que quels que soient les éléments u et v de $\mathcal{L}(E, F)$ et quels que soient les scalaires λ et μ,

$$\lambda(u + v) = \lambda u + \lambda v, \quad (\lambda + \mu)u = \lambda u + \mu u$$
$$(\lambda\mu)u = \lambda(\mu u), \quad 1 \cdot u = u.$$

On peut donc énoncer le

7.3.2.2. Théorème

Soient E et F deux K-espaces vectoriels. L'ensemble $\mathcal{L}(E, F)$ des applications linéaires de E dans F, muni des lois de compositions

$$(u, v) \longmapsto u + v \text{ et } (\lambda, u) \longmapsto \lambda u$$

est un K-espace vectoriel.

7.3.3. CAS PARTICULIER : $E = F$

Si $E = F$, le Théorème 7.3.2.2 montre que $\mathcal{L}(E)$ est un espace vectoriel sur K. D'après le Théorème 7.2.1.1, la loi de composition des applications est une loi interne dans $\mathcal{L}(E)$.

Si u, v, w sont des éléments de $\mathcal{L}(E)$, on a :

$$\begin{aligned} (u \circ v) \circ w &= u \circ (v \circ w), \\ u \circ (v + w) &= u \circ v + u \circ w, \\ (v + w) \circ u &= v \circ u + w \circ u. \end{aligned}$$

Vérifions par exemple le deuxième résultat. Soit $x \in E$; on a, en utilisant la linéarité de u et la définition de $v + w$:

$$\begin{aligned} \left[u \circ (v + w)\right](x) &= u\left((v + w)(x)\right) = u\left(v(x) + w(x)\right) \\ &= u\left(v(x)\right) + u\left(w(x)\right) \\ &= (u \circ v)(x) + (u \circ w)(x) = (u \circ v + u \circ w)(x). \end{aligned}$$

D'où

$$u \circ (v + w) = u \circ v + u \circ w.$$

Ainsi, $\mathcal{L}(E)$, muni des lois de composition $(u, v) \longmapsto u + w$ et $(u, v) \longmapsto u \circ v$ est un anneau (non commutatif en général), l'élément unité étant l'application identique de E.

On a de plus, pour tout $\lambda \in K$:

$$\lambda(u \circ v) = (\lambda u) \circ v = u \circ (\lambda v).$$

En effet, pour tout $x \in E$, on a :

$$\left(\lambda(u \circ v)\right)(x) = \lambda(u \circ v)(x) = \lambda\left(u(v(x))\right) = \left((\lambda u) \circ v\right)(x),$$

d'où

$$\lambda(u \circ v) = (\lambda u) \circ v.$$

On démontrerait de même que $\lambda(u \circ v) = u \circ (\lambda v)$.

Ces propriétés de $\mathcal{L}(E)$ nous amènent à poser la définition suivante.

7.3.3.1. Définition

Soit K un corps commutatif. On dit qu'un ensemble A est une **algèbre** *sur K, ou une K-***algèbre,** *si les conditions suivantes sont vérifiées :*

a) *A est muni d'une structure de K-espace vectoriel.*

b) *Il existe une loi interne dans A, appelée* **multiplication** *et notée $(x, y) \longmapsto x \cdot y$ telle que $(A, +, \cdot)$ soit un anneau.*

c) *Quels que soient les vecteurs x et y de A et pour tout scalaire λ on a :*

$$\lambda(x \cdot y) = (\lambda x) \cdot y = x \cdot (\lambda y).$$

Si la loi $(x, y) \longmapsto x \cdot y$ est commutative, on dit que l'algèbre A est **commutative.**

Ainsi $\mathcal{L}(E)$ est un algèbre sur K. On l'appelle l'**algèbre des endomorphismes de** E.

7.4. Projecteurs

7.4.1. DÉFINITION

7.4.1.1. Définition

Soit E un espace vectoriel sur le corps K. On dit qu'un endomorphisme p de E est un **projecteur** *si $p \circ p = p$.*

Soit I un ensemble non vide. On dit qu'une famille $(p_i)_{i \in I}$ de projecteurs est **orthogonale** *si $p_i \circ p_j = 0$ pour $i \neq j$.*

Soit E un K-espace vectoriel. Si E est somme directe d'une famille finie $(E_i)_{1 \leq i \leq n}$ de sous-espaces, tout $x \in E$ s'écrit d'une manière unique sous la forme

$$x = x_1 + \ldots + x_n \text{ avec } x_i \in E_i \text{ pour } 1 \leq i \leq n.$$

Définissons l'application p_i de E dans E en posant :

$$p_i(x) = x_i. \tag{7.4.1.1}$$

Pour tout $x \in E$, $p_i(x)$ est donc l'unique vecteur de E_i tel que $x - p_i(x)$ appartienne au sous-espace engendré par $E_1, \ldots, E_{i-1}, E_{i+1}, \ldots, E_n$. On dit que $p_i(x)$ est **la projection de x sur E_i.**

Nous allons montrer que $(p_i)_{1 \leq i \leq n}$ est une famille orthogonale de projecteurs. On dit que p_i est le **projecteur de E sur E_i parallèlement à** $\bigoplus_{j \neq i} E_j$.

7.4.2. PROPRIÉTÉS DES PROJECTEURS

7.4.2.1. Théorème

Conservons les notations qui viennent d'être introduites. Alors :

a) p_i *est un endomorphisme de* E *et* $p_1 + \ldots + p_n = \mathrm{Id}_E$.

b) $\mathrm{Ker}(p_i) = \bigoplus_{j \neq i} E_j$ et $\mathrm{Im}(p_i) = E_i$.

c) $p_i o p_j = \begin{cases} p_i & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}$

Démonstration. a) Soient $x = x_1 + \ldots + x_n$ et $y = y_1 + \ldots + y_n$ deux éléments de E avec $x_i, y_i \in E_i$ pour $1 \leq i \leq n$. On a, par définition de p_i :

$$p_i(x) = x_i \text{ et } p_i(y) = y_i.$$

Pour tout couple (λ, μ) de scalaires, on a :

$$\lambda x + \mu y = (\lambda x_1 + \mu y_1) + \ldots + (\lambda x_n + \mu y_n).$$

D'où

$$p_i(\lambda x + \mu y) = \lambda x_i + \mu y_i = \lambda p_i(x) + \mu p_i(y),$$

et p_i est linéaire.

Comme tout vecteur x de E s'écrit de façon unique

$$x = x_1 + \ldots + x_n \text{ avec } x_i \in E_i \text{ pour } 1 \leq i \leq n,$$

on a $\mathrm{Id}_E(x) = p_1(x) + \ldots + p_n(x) = (p_1 + \ldots + p_n)(x)$, d'où

$$\mathrm{Id}_E = p_1 + \ldots + p_n.$$

Démontrons **b)** Si $x \in E$ est tel que $p_i(x) = 0$, on a

$$x = x_1 + \ldots + x_{i-1} + x_{i+1} + \ldots + x_n$$

et par suite

$$\mathrm{Ker}(p_i) \subset \bigoplus_{j \neq i} E_j.$$

Réciproquement tout vecteur $x \in \bigoplus_{j \neq i} E_j$ s'écrit de façon unique sous la forme

$$x = x_1 + \ldots + x_{i-1} + 0 + x_{i+1} + \ldots + x_n$$

avec $0 \in E_i$ et $x_j \in E_j$ pour $j \neq i$.

On en déduit $p_i(x) = 0$, d'où $\bigoplus_{j \neq i} E_j \subset \mathrm{Ker}(p_i$.

Par suite, on a l'égalité $\mathrm{Ker}(p_i) = \bigoplus_{j \neq i} E_j$.

De la définition de p_i, il résulte que $p_i(x) \in E_i$ pour tout $x \in E$; d'où $\mathrm{Im}(p_i) \subset E_i$.

Inversement, tout $x \in E_i$ s'écrit de façon unique

$$x = 0 + \ldots + 0 + x + 0 + \ldots + 0$$

avec $x \in E_i$ et $0 \in E_j$ pour $j = 1, \ldots, i-1, i+1, \ldots, n$.

On en déduit: $p_i(x) = x$ pour tout $x \in E_i$, d'où $E_i \subset \mathrm{Im}(p_i)$. Finalement, on a $\mathrm{Im}(p_i) = E_i$.

Démontrons enfin c).

Nous venons de voir que si $x \in E_i$, alors $p_i(x) = x$. Réciproquement, soit $x \in E$ tel que $p_i(x) = x$. Comme $p_i(x) \in E_i$ nécessairement $x \in E_i$.

Comme $p_i(x) \in E_i$ pour tout $x \in E$, on a $p_i\left(p_i(x)\right) = p_i(x)$, c'est-à-dire

$$p_i o p_i = p_i.$$

D'autre part, pour tout $x \in E$, $p_j(x) \in E_j$; donc $p_i\left(p_j(x)\right) = 0$ si $i \neq j$, c'est-à-dire

$$p_i o p_j = 0 \quad \text{si } i \neq j.$$

Le théorème suivant établit la réciproque du résultat précédent.

7.4.2.2. Théorème

Soit $(p_i)_{1 \leq i \leq n}$ une famille finie orthogonale de projecteurs d'un K-espace vectoriel E, telle que $p_1(x) + \ldots + p_n(x) = x$ pour tout $x \in E$. Alors E est somme directe des sous-espaces $E_i = p_i(E)$.

Démonstration. La relation

$$p_1(x) + \ldots + p_n(x) = x$$

pour tout $x \in E$, montre que E est somme des sous-espaces E_i.

Pour montrer que la somme est directe, il suffit de montrer que la relation $x_1 + \ldots + x_n = 0$ où $x_i \in E_i$ pour $1 \leq i \leq n$, entraîne $x_1 = \ldots = x_n = 0$.

Considérons donc des $x_i \in E_i$ tels que

$$x_1 + \ldots + x_n = 0. \tag{7.4.2.1}$$

Puisque $x_j \in E_j = p_j(E)$, il existe $z_j \in E$ tel que $x_j = p_j(z_j)$; on a alors :

$$p_i(x_j) = p_i\left(p_j(z_j)\right) = \begin{cases} p_i(z_i) = x_i & \text{si} \quad i = j \\ 0 \quad \text{si} \quad i \neq j \end{cases}$$

On en déduit de là, en appliquant p_i à la relation (7.4.2.1), $x_i = 0$ pour $i = 1, \ldots, n$, ce qui prouve que E est somme directe des E_i.