الجمهوريـــة الجزائـــريـــة الديمقراطيـــة الشعبيـــة
**République Algérienne Démocratique et Populaire**
وزارة التعليـــــم العالـــي والبحـــث العلمـــي
**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**N° Ref :……**

**Centre Universitaire de Mila**

**Institut des sciences et de la technologie** **Département de Mathématiques et Informatique**

# Algèbre des fractions rationnelles

**Mémoire préparé En vue de l'obtention du diplôme de licence en Mathématiques**

**Préparé par :**
**Boutaghane Razika**
**Debbache Houda**
**Derbala Somia**

**Encadré par :**
**Kecies Mohamed**

**Filière** : **mathématiques**

**Année universitaire : 2012/2013**

# *** Remerciements ***

*Nous tenons à remercier en premier et avant tout, notre créateur <<ALLAH>>, qui nous aide à réaliser ce travail.*

*Nos sincères gratitudes et remerciements à notre encadreur Mohamed Kecies pour le grand soutient moral et leur aides précieuses qui nous apportez durant tout ce travail.*

*Nous adressons, également, mes remerciements chaleureux aux membres de l'institut des sciences et de la technologie et à tous ceux qui ont pris part de près ou de loin, à la réalisation de ce travail.*

*Razika, Houda et Somia*

# Table des matières

**Introduction Générale** **2**

**1 Structures algébriques** **3**
1.1 Groupes . . . . . 3
1.1.1 Loi de composition interne . . . . . 3
1.1.2 Loi de composition externe . . . . . 6
1.2 Anneaux . . . . . 9
1.3 Corps . . . . . 11
1.4 Espaces vectoriels . . . . . 12
1.5 $K$-algébres . . . . . 13

**2 Etude générale de l'ensemble $K[x]$** **15**
2.1 Opérations dans $K[X]$ et structures algébriques de $K[X]$ . . . . . 16
2.1.1 Opérations sur les polynômes . . . . . 16
2.1.2 Structures algébriques de $K[X]$ . . . . . 17
2.2 Arithmétique des polynômes . . . . . 21
2.3 Polynômes irréductibles et décomposition d'un polynôme . . . . . 28

**3 Algèbre des fractions rationnelles** **31**
3.1 Construction de l'ensemble des fractions rationnelles . . . . . 31
3.2 Décomposition en éléments simples d'une fraction rationnelle . . . . . 42
3.2.1 Décomposition dans le cas complexe . . . . . 50
3.2.2 Décomposition dans le cas réel . . . . . 51
3.2.3 Méthodes pratiques de décomposition . . . . . 51
3.2.4 Exemple de la décomposition dans $\mathbb{R}(X)$ . . . . . 52
3.2.5 Exemple de la décomposition dans $\mathbb{C}(X)$ . . . . . 54

**Bibliographie** **54**

# Introduction Générale

Les polynômes sont des objets centraux en mathématiques : ils interviennent aussi bien en analyse, sous la forme des « fonctions polynomiales », qui forment la plus petite classe de fonctions d'une variable réelle à valeur réelle stable par combinaison linéaire, par produit, contenant les fonctions constantes et l'identité ; qu'en algèbre, où à un problème linéaire peut souvent être associé un « polynôme caractéristique» dont les racines traduisent certaines caractéristiques du problèmes (valeurs propres, module et pulsation d'un système dynamique). Qui plus est, des outils de nature arithmétique interviennent aussi dans l'étude des polynômes.

Ce mémoire est réparti sur l'introduction générale, et trois chapitres. Dans le premier chapitre on donne des notions préliminaires sur les groupes, les anneaux, les corps, et les espaces vectoriels et leurs propriétés. On donne aussi les notions d'inversibles et d'intégrité. Nous terminons ce chapitre par les algèbres sur un corps et des exemples de référence.

Le deuxième chapitre est une étude générale de la structure de l'ensemble de polynômes $K[X]$. On donne la notion d'un polynôme, degré, racine d'un polynôme, les polynômes scindés et le théorème de D'Alembert. On calcul le pgcd et le ppcm des polynômes. On établit l'existence de la décomposition des polynômes dans le cas réel et complexe.

Enfin, dans le dernier chapitre, On construit l'ensemble des fractions rationnelles $K(X)$ à partir de l'ensemble $K[X]$ et on étudie aussi la structure de corps et de l'algèbre de cet ensemble. On termine ce chapitre par le calcul de la décomposition en élément simple d'une fraction dans le cas réel et complexe.

# Chapitre 1

# Structures algébriques

Les objectifs de ce chapitre sont :

Rappeler la structure de groupe, les règles de calculs. Définir les notions de morphisme, de noyau, de sous groupe. Rappeler la structure d'anneau, les règles de calculs, les notions d'inversibles et d'intégrité. Définir les notions de morphisme et de sous-anneau. Rappeler la structure de corps commutatif et de sous-corps. Rappeler la définition d'espace vectoriel et les exemples de référence. Rappeler la structure d'une algèbre. Définir les notions de morphisme et de sous algèbres.

## 1.1 Groupes

### 1.1.1 Loi de composition interne

**Définition 1.1.1**

*1) On appelle loi de composition interne (ou opération interne) (en abrégé : LCI) sur un ensemble non vide $E$, toute application $*$ de $E \times E$ dans $E$.*

*2) L'image $*(x, y)$ est souvent notée $x * y$.*

**Exemple 1.1.2**

*1) Les opérations usuelles $+, .$ sont des lois de composition internes sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.*

*2) La composition $\circ$ est une loi de composition interne sur l'ensemble $\mathcal{F}(E, E)$ des applications de $E$ dans $E$.*

*3) $\cap, \cup, \triangle$ (intersection, union, différence symétrique) sont des lois de composition internes sur $\mathcal{P}(E)$*

**Définition 1.1.3**

*1) Un ensemble $E$ muni d'une ou plusieurs loi de composition internes est appelé structure*

*algébrique.*
*2) Le couple $(E, *)$ est appelé un magma.*

**Remarque 1.1.4** *Si les lois sont notées $*_1, *_2, ..., *_n$, alors la structure, algébrique est notée $(E, *_1, *_2, ..., *_n)$.*

**Définition 1.1.5** *Soit $*$ une loi de composition interne sur $E$.*
*1) Une partie $A$ de $E$ est dite stable pour $*$ si et seulement si*

$$\forall x, y \in A : x * y \in A$$

*2) Si $A$ une partie stable de $E$ pour $*$, alors la lci dans $A$ définie par* $\begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x * y \end{array}$ *est appelée lci induite sur $A$ par $*$ de $E$. Autrement dit la restriction de la loi $*$ à $A \times A$ définit une loi de composition interne sur $A$.*

**Exemple 1.1.6**
*1) $\mathbb{R}^+$ une partie de $\mathbb{R}$ est stable pour la multiplication.*
*2) $\mathbb{R}^-$ une partie de $\mathbb{R}$ n'est pas stable pour la multiplication.*

**Définition 1.1.7** *Soient $*$, $T$ deux LCI sur un ensemble non vide $E$. Alors, On dit que*
*1) La loi $*$ est commutative, si et si $\forall x, y \in E : x * y = y * x$.*
*2) La loi $*$ est associative, si et si $\forall x, y, z \in E : (x * y) * z = x * (y * z)$.*
*3) $e$ de $E$ est neutre à droite (resp : à gauche) pour $*$ si et si $\forall x \in E : x * e = x$. (resp : $\forall x \in E : e * x = x$)*
*4) $e$ de $E$ est dit élément neutre (ou élément unité) pour $*$ si et si $e$ est neutre à droite et à gauche. C'est-à-dire*

$$\forall x \in E : x * e = e * x = x$$

*5) $x$ de $E$ possède :*
*i) Un symétrique à gauche noté $x'_g$ si et si $x' * x = e$. On dit alors que $x$ est symétrisable à gauche.*
*ii) Un symétrique à droite noté $x'_d$ si et si $x * x' = e$. On dit alors que $x$ est symétrisable à droite.*
*iii) Un symétrique $x'$ si et si $x * x' = x' * x = e$. On dit alors que $x$ est symétrisable.*
*6) $T$ est distributive à gauche (resp : à droite) par rapport à $*$ si et si*

$$\begin{aligned} \forall x, y, z \quad &\in \quad E : xT\,(y * z) = (xTy) * (xTz) \\ (resp \quad &: \quad (y * z)\,Tx = (yTx) * (zTx)\,) \end{aligned}$$

*7) $T$ est ditributive par rapport à $*$ si et si $T$ est distributive à gauche et à droite.*

**Notation 1.1.8**
*1) Lorsque la loi est notée additivement $+$, l'élément neutre est noté $0_E$ et le symétrique de $x$ est noté $-x$ (appelé opposé de $x$)*
*2) Si la loi notée multiplicativement ., alors l'élément neutre est noté $1_E$ et le symétrique de $x$ est noté $x^{-1}$ ou $\frac{1}{x}$ (appelé inverse de $x$).*

**Exemple 1.1.9**
*1) La somme $+$ et le produit .sur $\mathbb{C}$ (donc sur ses sous-ensembles) est associative et commutative, et admettent pour neutres respectifs $0$ et $1$.*
*2) La composition $\circ$ sur $\mathcal{F}(E)$ est une loi associative, admettant $Id_E$ comme élément neutre, et les seuls éléments inversibles sont les applications bijectives.*
*3) Les lois $\cup, \cap, \triangle$ sur $\mathcal{P}(E)$ sont associatives et commutatives. Elles admettent pour neutres respectifs $\phi, E, \phi$.*
*4) Seul $\phi$ (resp : $E$) est inversible dans $(\mathcal{P}(E), \cup)$ (resp : $(\mathcal{P}(E), \cap)$).*

**Proposition 1.1.10** *Soit $E$ un ensemble muni d'une loi de composition interne $*$, alors*
*1) L'élément neutre $e$, s'il existe, il est unique.*
*2) Si $*$ est associative et admet un élément neutre $e$, alors l'élément inverse $x^{-1}$ de $x$, s'il existe il est unique, de plus si $x, y \in E$ sont inversibles alors $x * y$ est inversible et*

$$\begin{cases} (x*y)^{-1} = y^{-1} * x^{-1} \\ (x^{-1})^{-1} = x \end{cases}$$

**Preuve.**
1) Supposons $e'$ un autre élément neutre de $*$, alors $e * e' = e$ et comme $e$ est aussi un élément neutre alors $e * e\prime = e\prime$, d'où l'égalité $e' = e$.
2) Supposons $x'$ un autre inverse de $x$, alors $x' * x = e$, ainsi

$$x^{-1} = (x' * x) * x^{-1} = x' * (x * x^{-1}) = x'$$

donc l'inverse est unique.
On a $x * x^{-1} = e = x^{-1} * x$, et puisque l'inverse est unique, alors $x$ est l'inverse de $x^{-1}$, c.à.d $(x^{-1})^{-1} = x$.
Supposons que $x, y \in E$ sont inversibles. Alors

$$\begin{cases} (y^{-1} * x^{-1}) * (x * y) = y^{-1} * x^{-1} * x * y = e \\ (x * y) * (y^{-1} * x^{-1}) = x * y * y^{-1} * x^{-1} = e \end{cases}$$

et puisque l'inverse est unique, alors $(y^{-1} * x^{-1})$ est l'inverse de $x * y$, c.à.d $(x * y)^{-1} = y^{-1} * x^{-1}$. ■

### 1.1.2 Loi de composition externe

**Définition 1.1.11** *Soient $E$ et $X$ des ensembles. On appelle loi de composition externe (LCE) sur $E$ toute application notée $T$ définie par*

$$\begin{array}{rccc} T: & X \times E & \longrightarrow & E \\ & (\alpha, x) & \longmapsto & \alpha T x \end{array}$$

*Les éléments de $X$ sont appelés opérateurs (ou scalaires) et on dit que $E$ est muni d'une loi de composition externe à opérateurs dans $X$.*

**Remarque 1.1.12** *La loi $T$ peut être notée multiplicativement à l'aide d'un point.*

**Définition 1.1.13** *Soit $E$ un ensemble muni d'une loi de composition externe $T$ à opérateurs dans $X$. Soit $F$ une partie de $E$.*
*1) On dit que $F$ est stable par $T$ si*

$$\forall \alpha \in X, \forall x \in F, \alpha T x \in F$$

*2) Si $F$ est une partie stable par $T$ , alors la restriction de $T$ à $F$ est une loi de composition externe sur $F$ dite loi induite par $T$ dans $F$.*

**Définition 1.1.14** *On dit que $(G, *)$ est un groupe si la loi $*$ est associative, et admet un élément neutre $e$ et tout élément de $G$ est inversible (symétrisable).*
*Si en plus $*$ est commutative, alors le groupe $G$ est dit commutatif ou abélien.*

**Exemple 1.1.15**
*1) Les structures $(\mathbb{Q}^*, .), (\mathbb{R}^*, ) (\mathbb{C},^*, .)$ sont des groupes commutatifs.*
*2) $(P(E), \cap)$ n'est pas un groupe, puisque l'inverse de $\phi$ n'existe pas.*
*3) Si $E$ un ensemble. On note $\sigma(E)$ l'ensemble des bijections de $E$ dans $E$. Alors $(\sigma(E), \circ)$ est un groupe (en général non abélien).*
*4) $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$ est un groupe abélien.*

**Définition 1.1.16** *On dit qu'un groupe $(G, *)$ est fini si l'ensemble $G$ est fini. Dans ce cas, le cardinal de $G$ est appelé ordre de $G$ et noté $ord(G), |G|$ .*

**Exemple 1.1.17** *$G = (\mathbb{Z}/n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$ est un groupe fini d'ordre $n$.*

**Définition 1.1.18** ***Puissances entières dans un groupe :***
*Soit $(G, *)$ un groupe, $n \in \mathbb{Z}$ et $a \in G$. On définit les puissance entières ($n^{ème}$) de $a$ de la*

*façon suivante*

$$\begin{cases} a^0 = e \\ a^n = a * a^{n-1}, n > 0 \\ a^n = \left(a^{-n}\right)^{-1}, n < 0 \end{cases}$$

*Pour $n$ strictement positif, on a donc* $a^n = \underbrace{a * a * ... * a}_{n\ fois}$ *et pour $n$ strictement négatif,* $a^n = \underbrace{a^{-1} * a^{-1} * ... * a^{-1}}_{n\ fois}$.

*Si la loi est notée additivement, alors on note $na$ au lieu de $a^n$. On a alors*

$$\begin{cases} 0a = e \\ na = a + (n-1)\, a, n > 0 \\ na = -\left(-na\right), n < 0 \end{cases}$$

*On obtient ainsi les "règles de calcul" suivantes :*

$$\forall x, y \in (G, .), \forall m, n \in \mathbb{Z} : \begin{cases} x^n x^m = x^{n+m} = x^{m+n} = x^m x^n \\ \left(x^n\right)^m = x^{nm} = x^{mn} = \left(x^m\right)^n \end{cases}$$

$$\forall x, y \in (G, +), \forall m, n \in \mathbb{Z} : \begin{cases} (n+m)\, x = nx + mx \\ (nm)\, x = n\,(mx) \end{cases}$$

**Définition 1.1.19** *On appelle sous groupe d'un groupe $(G, *)$ toute partie non vide $H$ ■de $G$ ■qui est elle même un groupe pour la loi restreinte à $H$. Autrement dit $H$ est sous groupe de $(G, *)$ si et si*

$$\begin{cases} i) e \in H \\ ii) \forall x \in H : x^{-1} \in H \\ iii) \forall x, y \in H : x * y \in H \end{cases} \Longleftrightarrow \begin{cases} i) e \in H \\ ii) \forall x, y \in H : x * y^{-1} \in H \end{cases}$$

**Exemple 1.1.20**

1) *Si $(G, *)$ est un goupe, alors $\{e\}$ et $G$ sont des sous groupes de $G$ appelés sous groupes trivaux.*

2) $(\{-1, 1\}, \cdot)$ *est un sous groupe de groupe* $(\mathbb{R}^*, \cdot)$.

3) *Les sous groupes de* $(\mathbb{Z}, +)$ *sont* $n\mathbb{Z} = \{na, a \in \mathbb{Z}\}$ *où* $n \in \mathbb{N}^*$.

**Définition 1.1.21** *Soient $(G_1, *), (G_2, \top)$ deux groupes et $f : (G_1, *) \longrightarrow (G_2, \top)$ une application, on dit que $f$ est un morphisme de groupe $G_1$ dans $G_2$ si et seulement si*

$$\forall x, y \in G_1 : f(x * y) = f(x) \top f(y)$$

*On dit de plus que $f$ est un :*
*Endomorphisme lorsque $G_1 = G_2$ et $* = \top$.*
*Isomorphisme lorsque $f$ est bijective. On dit que $G_1$ et $G_2$ sont isomorphe, $G_1 \approx G_2$.*
*Automorphisme lorsque $f$ est un endomorphisme bijective.*

**Exemple 1.1.22**
*1) L'application $f : (\mathbb{C}^*, .) \longrightarrow (\mathbb{R}^*, .)$ telle que $f(z) = |z|$ est un morphisme de groupes. Car*

$$\forall z, z' \in \mathbb{C}^* : f(z.z') = |z.z'| = |z| \,.\, |z'| = f(z) \,.f(z')$$

*2) Pour tout élément $a$ d'un groupe $(G, *)$, l'application $f_a : (G, *) \longrightarrow (G, *)$ telle que $f_a(x) = a * x * a^{-1}$ est un automorphisme du groupe $(G, *)$.*

**Remarque 1.1.23**
*1) Si $f : (G, *) \longrightarrow (G', T)$ est un morphisme du groupes, alors*
*a) $f(e) = e'$ ( $e$ et $e'$ sont respectivement les éléments neutres de $G$ et $G'$).*
*b) Pour tout $x \in G : f(x^{-1}) = (f(x))^{-1}$.*
*2) Si $f : (G_1, *) \longrightarrow (G_2, \top)$ et $g : (G_2, \top) \to (G_3, \triangle)$ deux morphismes de groupes ,alors : $g \circ f : (G_{1,*}) \to (G_3, \triangle)$ est un morphisme de groupes.*
*3) Si $f : (G_1, *) \longrightarrow (G_2, \top)$ est un isomorphisme de groupes, alors $f^{-1} : (G_2, \top) \longrightarrow (G_1, *)$ est un isomorphisme de groupe.*

**Définition 1.1.24** *Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes. On note $e_1$ l'élément neutre de groupe $G_1$ et $e_2$ l'élément neutre de groupe $G_2$. Alors*
*1) On appelle noyau de $f$, et on note $\ker(f)$ l'ensemble*

$$\ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}(\{e_2\})$$

*2) On appelle image de $f$, et on note $\mathrm{Im}(f)$ l'ensemble*

$$\mathrm{Im}(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\} = f(G_1)$$

**Proposition 1.1.25** *Soit $f : (G_1, *) \longrightarrow (G_2, \top)$ un morphisme de groupe. Alors*
*1) L'image directe d'un sous-groupe de $G_1$ par $f$ est un sous-groupe de $G_2$. En particulier $\mathrm{Im}(f)$ est un sous groupe de $G_2$.*
*2) L'image réciproque d'un sous-groupe de $G_2$ par $f$ est un sous-groupe de $G_1$. En particulier $\ker(f)$ est un sous groupe de $G_1$.*

**Théorème 1.1.26** *Soit $f : (G_1, *) \longrightarrow (G_2, \top)$ un morphisme de groupes. Alors*
*1) $f$ est injective si et seulement si $\ker(f) = \{e_1\}$.*
*2) $f$ est surjective si et seulement si $\mathrm{Im}(f) = G_2$.*

**Preuve.**
1) Supposons que $f$ est injectif. Comme $f$ est un morphisme, on a $e_1 \in \ker(f)$. Comme $f$ est injectif, alors $e_1$ est le seul élément de $e_2$ dans $G_1$, ce qui prouve que $\ker f = \{e_1\}$. Réciproquement, supposons que $\ker f = \{e_1\}$. Soient $x, y \in G_1$ tel que $f(x) = f(y)$. Montrons que $x = y$. On multiplie à droite l'égalité $f(x) = f(y)$ par $(f(y))^{-1}$. On obtient

$$f(x) \intercal (f(y))^{-1} = f(y) \intercal (f(y))^{-1} = e_2$$

D'après les propriétés des morphismes de groupes, on a $f(x * y^{-1}) = e_2$. Donc $x * y^{-1} \in \ker(f)$ et forcément $x * y^{-1} = e_1$. On multiplie à droite par $y$ les deux membres de cette égalité et on obtient $x = y$, ce qui prouve que $f$ est injectif.
2) La preuve de cette propriété est immédiate, sachant que $\mathrm{Im}(f) = f(G_1)$. ■

## 1.2 Anneaux

**Définition 1.2.1** *Soit $A$ un ensemble possédant deux lois internes notée $+$ et $.$. Alors on dit que $(A, +, .)$ est un anneau si et seulement si :*
*1) $(A, +)$ est un groupe commutatif.*
*2) La loi $.$ est associative : $\forall x, y, z \in A : x.(y.z) = (x.y).z$.*
*3) La loi $.$ est distributive à gauche et à droite par rapport à $+$*

$$\forall x, y, z \in A : \begin{cases} x.(y+z) = x.y + x.z \\ (y+z).x = y.x + z.x \end{cases}$$

*Si la loi $.$ admet un élément neutre, on dit que l'anneau est unitaire.*
*Si la loi $.$ est commutative, on dit que l'anneau est commutatif.*

**Remarque 1.2.2** *Puisque la première loi de $A$ est notée additivement $+$ ; alors son élément neutre est noté $0_A$ et pour la même raison le symétrique d'un élément $x$ par rapport à cette loi est noté $-x$ et appelé opposé. Puisque la deuxième loi de $A$ est notée multiplicativement. ; alors son élément neutre (s'il existe) est noté $1_A$ et pour la même raison le symétrique d'un élément $x$ par rapport à cette loi (s'il existe) est noté $x^{-1}$ et appelé inverse.*

**Exemple 1.2.3**
*1) $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ et $(\mathbb{C}, +, .)$ sont des anneaux commutatifs unitaires .*
*2) Pour tout ensemble $E$, on a $(\mathcal{P}(E), \triangle, \cap)$ est un anneau commutatif et unitaire.*

**Règles de calculs dans un anneau :**

Soit $(A,+,.)$ un anneau, on note $0_A$ le neutre de $+$, $1_A$ le neutre de $.$, alors
1) $\forall x \in A : x.0_A = 0_A.x = 0_A$.
2) $\forall x \in A : (-1_A)\, x = x.\,(-1_A) = -x$.
3) $\forall x, y, z \in A : (x-y)\,.z = xz - yz$ et $z.\,(x-y) = z.x - z.y$.
4) $\forall x, y \in A$, si $x$ et $y$ commutent (i.e. $x.y = y.x$), alors on a la formule du binôme de Newton

$$\forall n \in \mathbb{N} : (x+y)^n = \sum_{k=0}^{n} C_n^k x^k.y^{n-k}$$

où $x^0 = y^0 = 1_A$.

**Définition 1.2.4**
*1) Si l'élément $x$ d'un anneau possède un inverse pour la deuxième loi de cet anneau, on dira que $x$ est un élément inversible de cet anneau et on notera $x^{-1}$ son .inverse.*
*2) L'ensemble des éléments inversibles d'un anneau possède une structure de groupe pour la multiplication de l'anneau est appelé groupe des unités de $A$ et noté $U(A)$,*

**Définition 1.2.5** *On appelle sous anneau d'un anneau $(A,+,.)$ toute partie non vide $B$ de $A$ qui est elle même un anneau pour les lois $+,.$ restreintes à $B$. Ceci est équivalent à :*

$$B \text{ est un sous anneau de } A \iff \begin{cases} 1)(B,+) \text{ est un sous groupe de groupe}(A,+) \\ 2)B \text{ est stable pour la loi.} : \forall x, y \in B : x.y \in B \end{cases}$$

$$\iff \begin{cases} 1)0_A \in B \\ 2)\forall x, y \in B : x - y \in B \\ 3)\forall x, y \in B : x.y \in B \end{cases}$$

**Remarque 1.2.6** *Une intersection de sous-anneaux de $(A,+,.)$ est un sous-anneau de $A$.*

**Exemple 1.2.7**
*1) Si $A$ est un anneau, $A$ et $\{0_A\}$ sont des sous anneaux de $A$.*
*2) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ qui est un sous-anneau de $\mathbb{R}$.*
*3) $(n\mathbb{Z},+,.)$ avec $n \in \mathbb{N}^*$, sont des sous anneaux de $\mathbb{Z}$.*

**Définition 1.2.8** *Soit $(A,+,.)$ un anneau non réduit à $0_A$ et $a \in A - \{0_A\}$. Alors*
*1) On dit que $a$ est un diviseur de zéro s'il existe $b \in A - \{0_A\}$ tel que $ba = 0_A$ ou $ab = 0_A$.*
*2) On dit que $A$ est intègre si $A$ est commutative et sans diviseurs de zéro, i.e.*

$$\forall a, b \in A : ab = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A$$

**Exemple 1.2.9**
*1)* $(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$ *et* $(\mathbb{C},+,.)$ *sont des anneaux intègres.*
*2) Dans* $\mathbb{Z}/6\mathbb{Z}$, *on a* $\dot{2},\dot{3},\dot{4}$ *sont des diviseurs de zéro, donc* $(\mathbb{Z}/6\mathbb{Z},+,.)$ *n'est pas intègre.*
*3) Dans* $M_2(\mathbb{R})$, *on a* $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ *et* $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ *sont des diviseurs de zéro.*

**Définition 1.2.10** *Soit* $f : (A,+,.) \longrightarrow (B,+,.)$ *une application d'un anneau* $A$ *dans un anneau* $B$, *on dit que* $f$ *est un morphisme d'anneaux lorsque :*
*1)* $\forall x,y \in A : f(x+y) = f(x) + f(y)$.
*2)* $\forall x,y \in A : f(x.y) = f(x).f(y)$.

**Exemple 1.2.11** *L'application* $f : (\mathbb{Z},+,.) \longrightarrow (\mathbb{Z}/n\mathbb{Z},+,.)$ *telle que* $f(x) = \dot{x}$ *est un morphisme d'anneaux.*

## 1.3 Corps

**Définition 1.3.1** *Soit* $K$ *un ensemble muni de deux lci* $+$ *et* $.$. *On dit que* $(K,+,.)$*et un corps si et seulement si :*
*1)* $(K,+,.)$ *est un anneau unitaire. (*$1_A$ *est le neutre pour la loi* $.$*) .*
*2) Tout élément de* $K^* = K - \{0_A\}$ *admet un symétrique (inverse) pour la loi* $.$ *dans* $K$ *:*

$$\forall x \in K^*, \exists x^{-1} \in K^* : x.x^{-1} = x^{-1}.x = 1_A$$

*Si de plus* $.$ *est commutative, alors on dit que* $(K,+,.)$ *est un corps commutatif.*

**Remarque 1.3.2**
*1) Si* $(K,+,.)$ *est un corps alors* $(K^*,.)$ *est un groupe.*
*2) Tout corps commutatif* $K$ *est un anneau intègre. Puisque*

$$a.b = 0_K \Longrightarrow \begin{cases} a^{-1}ab = a^{-1}0_K \\ abb^{-1} = 0_K b^{-1} \end{cases} \Longrightarrow \begin{cases} b = 0_K \\ a = 0_K \end{cases}$$

**Définition 1.3.3** *Soit* $(K,+,.)$ *un corps et* $L \subset K$ *, on dit* $L$ *est un sous corps de* $K$ *si et seulemet si :*

$$\begin{cases} 1)1_K \in B \\ 2\,(L,+,.) \text{ est un sous anneau de} (K,+,.) \\ 3)\forall x \in L^* : x^{-1} \in L \end{cases} \Longleftrightarrow \begin{cases} 1)0_K, 1_K \in L \\ 2)\forall x,y \in L : x - y \in L \\ 3)\forall x,y \in L : x.y \in L \\ 4)\forall x \in L^* : x^{-1} \in L \end{cases}$$

## 1.4 Espaces vectoriels

**Définition 1.4.1**

*1) On appelle espace vectoriel sur le corps $K$ tout ensemble $E$ muni d'une loi de composition interne $+$ (addition)* $\begin{array}{rccc} +: & E\times E & \longrightarrow & E \\ & (x,y) & \longmapsto & x+y \end{array}$ *et d'une loi de composition externe* $\cdot$ *(multiplication)* $\begin{array}{rccc} .: & K\times E & \longrightarrow & E \\ & (\lambda,x) & \longmapsto & \lambda.x \end{array}$ *tels que :*

*a)* $(E,+)$ *et un groupe commutatif.*

*b)* $\forall \alpha,\beta\in K, \forall x,y\in E$, *on a :*

*i)* $(\alpha+\beta).x=\alpha.x+\beta.x$ .

*ii)* $(\alpha.\beta).x=\alpha.(\beta.x)$.

*iii)* $\alpha.(x+y)=\alpha.x+\alpha.y$ .

*iiii)* $1_K\cdot x=x$.

*2) On dit alors que* $(E,+,\cdot)$ *est un* $K-$ *espace vectoriel, les éléments de* $K$ *sont appelés scalaires, ceux de* $E$, *vecteurs. L'élément neutre de* $(E,+)$, $0_E$ *est applé vecteur nul .*

**Exemple 1.4.2**

*1) Notons* $S(K)$ *l'ensemble des suites à coefficients dans* $K$. *Avec les lois* $\begin{array}{rccc} +: & S(K)\times S(K) & \longrightarrow & S(K) \\ & ((x_n),(y_n)) & \longmapsto & (x_n+y_n) \end{array}$ *et* $\begin{array}{rccc} .: & K\times S(K) & \longrightarrow & S(K) \\ & (\lambda,(x_n)) & \longmapsto & (\lambda.x_n) \end{array}$ *. Alors* $(S(K),+,.)$ *est un* $K-$*espace vectoriel. Son vecteur nul est la suite constante nulle.*

*2) Soit* $X$ *un ensemble non vide et soit* $E$ *un* $K-$*espace vectoriel. On définit sur l'ensemble* $\mathcal{F}(X,E)$ *des applications définies sur* $X$ *à valeurs dans* $E$ *:*

*Une addition* $\begin{array}{rccc} +: & \mathcal{F}(X,E)\times\mathcal{F}(X,E) & \longrightarrow & \mathcal{F}(X,E) \\ & (f,g) & \longmapsto & (f+g) \end{array}$ *donnée par* $\forall x\in X:(f+g)(x)=f(x)+g(x)$.

*Une multiplication par un scalaire* $\begin{array}{rccc} .: & K\times\mathcal{F}(X,E) & \longrightarrow & \mathcal{F}(X,E) \\ & (\lambda,F) & \longmapsto & \lambda.f \end{array}$ *donnée par* $\forall x\in X:(\lambda.f)(x)=\lambda.f(x)$. *Muni de ces lois, l'ensemble* $(\mathcal{F}(X,E),+,\cdot)$ *est un* $K-$*espace vectoriel. Son vecteur nul est l'application identiquement nulle sur* $X$ *à valeurs dans* $E$.

**Définition 1.4.3** *Soit* $E$ *un espace vectoriel sur* $K$ *, soit* $F$ *une partie de* $E$. *On dit que* $F$ *est un sous espace vectoriel de* $E$ *si et seulement si :*

*1)* $0_E\in F$.

*2)* $\forall\,(u,v)\in F^2, \forall\,(\lambda,\mu)\in K^2$ *:* $\lambda u+\mu v\in F$.

## 1.5 $K$-algébres

**Définition 1.5.1** *On appelle une $K-$algèbre tout ensemble $A$ muni d'une loi interne notée $+$, d'une loi externe* $\begin{array}{ccc} K\times A & \longrightarrow & A \\ (\lambda,x) & \longmapsto & \lambda.x \end{array}$ *et d'une loi interne (appelée 3ème loi) notée $*$ telles que :*
*1) $(A,+,.)$ est un espace vectoriel sur $K$*
*2) $*$ est distributive sur $+$*
*3) $\forall\lambda\in K,\forall x,y\in A:\lambda.(x*y)=(\lambda.x)*y=x*(\lambda.y)$*

**Notation 1.5.2** *On note une $K-$algèbre par $(A,+,*,.)$*

**Définition 1.5.3** *Une $K-$algèbre est dite :*
*1) commutative si et si la loi $*$ est commutative.*
*2) associative si et si la loi $*$ est associative.*
*3) unitaire ou unifère si et si $*$ admet un neutre.*

**Exemple 1.5.4**
*1) Tout corps commutatif $K$ est une $K-$algèbre commutative, associative et unitaire en prenant pour la 3ème loi la multiplication.*
*2) $\mathbb{R}$ est une $\mathbb{R}-$algèbre commutative, associative et unitaire pour les lois usuelles et $\mathbb{C}$ aussi.*
*3) $\mathbb{C}$ est une $\mathbb{C}-$algèbre.*
*4) $(\mathcal{L}(E),+,\circ,.)$ l'ensemble des endomorphismes est une $K-$algèbre associative et unitaire, dont la 3ème loi est la loi $\circ$ de composition.*

**Définition 1.5.5**
*Soit $(A,+,*,.)$ une $K-$algèbre et $B\subset A$, on dit que $B$ est une sous algèbre de $A$ si et si*
*1) $B$ est un sous espace vectoriel de $A$.*
*2) $\forall x,y\in B:x*y\in B$*
*Ceci est équivalent à*
*1) $B\neq\varnothing$*
*2) $\forall x,y\in B:x+y\in B$*
*3) $\forall\lambda\in K,\forall x\in B:\lambda.x\in B$*
*4) $\forall x,y\in B:x*y\in B$*

**Exemple 1.5.6** *$\mathcal{F}(\mathbb{R},\mathbb{R})$ est une $\mathbb{R}-$algèbre pour les lois usuelles et la 3ème loi est la mutiplication et l'ensemble $B$ des applications bornées de $\mathbb{R}$ dans $\mathbb{R}$ est une sous algèbre de$\mathcal{F}(\mathbb{R},\mathbb{R})$.*

**Définition 1.5.7** *Soient* $(A,+,*,.),(B,+,*,.)$ *deux* $K-$*algèbres et* $f : A \longrightarrow B$ *une application. On dit que* $f$ *est un morphisme d'algèbres si et si*
*1)* $\forall x,y \in A : f(x+y) = f(x) + f(y)$
*2)* $\forall \lambda \in K, \forall x \in A : f(\lambda.x) = \lambda.f(x)$
*3)* $\forall x,y \in A : f(x*y) = f(x) * f(y)$

**Remarque 1.5.8** $f$ *est un morphisme d'algèbres si et si* $f$ *est un morphisme d'espaces vectoriels ( ou linéaire ) et* $f$ *est un morphisme pour la loi* $*$.

**Exemple 1.5.9** *L'ensemble des suites convergentes est une sous algèbre de la* $\mathbb{R}-$*algèbre des suites réelles, et l'application qui à une suite convergente associe sa limite est un morphisme d'algèbre.*

# Chapitre 2

# Etude générale de l'ensemble $K[x]$

Les objectifs sont : définir la notion de polynômes, étudier la structure de K[X]. Définir la notion de degré d'un polynôme et aborder la notion de racine, de polynômes scindés et le théorème de D'Alembert. Calcul de pgcd et ppcm des polynômes est ses propriétés. Établir l'existence de la décomposition des polynômes dans le cas réel et complexe

Dans tout ce chapitre, $K$ désigne un corps commutatif.

**Définition 2.0.10** *On appelle polynôme à coefficients dans $K$ toute suite d'éléments de $K$ nulle à partir d'un certain rang. Les termes d'une telle suite sont appelés : coefficients du polynôme, et la suite nulle est appelée polynôme nul noté $0$. Si tous les termes sont nuls sauf un, le polynôme est appelé monôme. Si tous les termes sont nuls à partir de l'indice $1$, on dit que le polynôme est constant.*

**Notation 2.0.11**
*1) Les polynômes à une indéterminée et à coefficients dans $K$ sont notés $P = \sum_{k=0}^{+\infty} a_k X^k$ où il existe un entier naturel $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k > n$.*
*2) L'ensemble des polynômes à coefficients dans $K$ est noté $K[X]$, on a donc :*

$$K[X] = \{(a_n) \in \mathcal{F}(\mathbb{N}, K) : \exists n_0 \in \mathbb{N}, n > n_0 \Longrightarrow a_n = 0\}$$

**Remarque 2.0.12** *Deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients (égalité de deux suites).*

## 2.1 Opérations dans $K[X]$ et structures algébriques de $K[X]$

### 2.1.1 Opérations sur les polynômes

**Définition 2.1.1** *Soient $P=(a_n)_n$, $Q=(b_n)_n$ deux polynômes de $K[X]$, et $\lambda \in K$ alors on définit les opérations suivantes sur les polynômes :*
*1)* ***Addition (loi interne) :*** *$P+Q=(a_n+b_n)_n$.*
*2)* ***Multiplicatin par un scalaire (loi externe) :*** *$\lambda.P=(\lambda a_n)_n$*
*3)* ***Produit (loi interne) :*** *$P\times Q=(c_n)_n$ où la suite $(c_n)_n$ est définie par $c_n=\sum_{k=0}^{n} a_k b_{n-k}=\sum_{p+q=n} a_p b_q$*

**Remarque 2.1.2** *Si $P=\sum_{i=0}^{p} a_i X^i$ et $Q=\sum_{i=0}^{q} b_i X^i$, alors $P\times Q=\sum_{i=0}^{r} c_i X^i$ avec $r=p+q$, et pour $k\in\{0,1,...,r\}$*

$$c_k=\sum_{i=0}^{k} a_i b_{k-i}=\sum_{i=0}^{k} a_{k-i} b_i=\sum_{i+j=k} a_i b_j$$

**Remarque 2.1.3** *L'addition et la multiplication par un scalaire précédemment définies coïncident avec l'addition et la multiplication définie sur l'espace des suites à coefficients dans K,i.e : $\mathcal{F}(\mathbb{N},K)$. Ce n'est pas par contre le cas de la multiplication entre polynômes, qui ne coïncident pas avec celle définie entre les suites.*

**Définition 2.1.4** *Soit $P=\sum_{n=0}^{+\infty} a_n X^n \in K[X]$. Alors :*
*1) Si $P\neq 0$, on appelle degré de $P$ l'entier naturel $max\{n\in\mathbb{N} : a_n\neq 0\}$, noté $\deg(P)$.*
*2) Soit $d=\deg(P)$, $a_d$ est appelé le coefficient dominant de $P$.*
*3) On dit que $P$ est normalisé ou unitaire si et seulement si $a_d=1$.*
*4) Si $P=0$, on pose $\deg(P)=-\infty$.*
*5) Si $P,Q\in K[X]$, et $\lambda\in K^*$, alors*

$$\begin{cases} \deg(P+Q)\leq \max\{\deg(P),\deg(Q)\} \\ \deg(P+Q)=\max\{\deg(P),\deg(Q)\}, \text{ si } \deg(P)\neq\deg(Q)) \\ \deg(P\times Q)=\deg(P)+\deg(Q) \\ \deg(\lambda.P)=\deg(P) \end{cases}$$

**Définition 2.1.5** *(Polynômes paires et impaires) On dit qu'un polynôme $P\in K[X]$ est pair (resp : impair) si $P(-X)=P(X)$ (resp : $P(-X)=-P(X)$).*

**Notation 2.1.6** *Soit $n \in \mathbb{N}$, on note $K_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à $n$ :*

$$K_n[X] = \{P \in K[X] : \deg(P) \leq n\}$$

### 2.1.2 Structures algébriques de $K[X]$

Rappelons que l'ensemble $\mathcal{F}(\mathbb{N}, K)$ des suites d'éléments de $K$ munie de l'addition et de la multiplication externe forme un espace vectoriel sur $K$, et $E$ l'ensemble des suite d'éléments de $K$ nulles à partir d'un certain rang est un sous espace vectoriel de l'espace précédent.

**Proposition 2.1.7** *$(K[X], +, \times)$ est un anneau commutatif unitaire et intègre.*

**Preuve.**

1) Montrons que $(K[X], +)$ est un groupe commutatif.

a) Le polynôme nul est clairement l'élément neutre pour l'addition.

b) Si $P = a_0 + a_1X + .... + a_{n-1}X^{n-1} + a_nX^n$, le polynôme $(-P) = -a_0 - a_1X + .... + -a_{n-1}X^{n-1} - a_nX^n$ vérifie $P + (-P) = 0$, donc $(-P)$ est le symétrique de $P$.

c) L'associativité et la commutativité résultent de celles de l'addition sur $K$. Par conséquent $(K[X], +)$ est un groupe commutatif.

2) Reste à étudier les propriétés de la multiplication $\times$ :

a) De la définition de la multiplication sur $K[X]$, on déduit facilement que le polynôme $P = 1$ est l'élément neutre pour la multiplication.

b) Commutativité : Considérons $P = \sum_{i=0}^{p} a_iX^i$ et $Q = \sum_{i=0}^{q} b_iX^i$. Notons $r = p + q$, alors

$$P \times Q = \sum_{i=0}^{r} c_iX^i, Q \times P = \sum_{i=0}^{r} d_iX^i$$

Donc, on a

$$\forall k \in \{0, 1, ..., r\} : \begin{cases} c_k = \sum_{i=0}^{k} a_ib_{k-i} = \sum_{i+j=k} a_ib_j \\ d_k = \sum_{i=0}^{k} b_{k-i}a_i = \sum_{j+i=k} b_ja_i \end{cases} \Longrightarrow \forall k \in \{0, 1, ..., r\} : c_k = d_k$$

$$\Longrightarrow \quad P \times Q = Q \times P$$

c)Associativité : Soient $P=(a_n)_n, Q=(b_n)_n, R=(c_n)_n \in K[X]$. Alors

$$\begin{aligned} PQ &= (d_n)_n \text{ où } \forall n \in \mathbb{N} : d_n = \sum_{k=0}^{n} a_k b_{n-k} \\ (PQ)R &= (e_n)_n \text{ où } \forall n \in \mathbb{N} : e_n = \sum_{k=0}^{n} d_k c_{n-k} \end{aligned}$$

Et

$$QR = (f_n)_n \text{ où } \forall n \in \mathbb{N} : f_n = \sum_{k=0}^{n} b_k c_{n-k}$$

Puis

$$P(QR) = (g_n)_n \text{ où } \forall n \in \mathbb{N} : g_n = \sum_{k=0}^{n} a_k f_{n-k}$$

On a pour tout $n \in \mathbb{N}$ :

$$\begin{aligned} g_n &= \sum_{i+p=n} a_i f_p = \sum_{i+p=n} a_i \left( \sum_{j+k=p} b_j c_k \right) = \sum_{i+(j+k)=n} a_i (b_j c_k) = \sum_{(i+j)+k=n} (a_i b_j) c_k = \sum_{q+k=n} \left( \sum_{i+j=q} a_i b_j \right) c_k \\ &= \sum_{q+k=n} d_k c_k = e_n \Longrightarrow P(QR) = (PQ)R \end{aligned}$$

c) Distributivité de la multiplication sur l'addition : Définissons $P, Q, R$ comme ci-dessus. Posons $U=(P+Q)R$ et $V=PR+QR$. Notons encore $d_l$ les coefficients de $U$, et $e_m$ ceux de $V$ . Alors on a

$$d_l = \sum_{i+j=l} (a_i + b_i) c_j = \sum_{i+j=l} (a_i c_j + b_i c_j) = \sum_{i+j=l} a_i c_j + \sum_{i+j=l} b_i c_j = e_l$$

donc $U=V$.
c) Montrons que $(K[X], +, \times)$ est intègre. Soient $P, Q \in K[X]$.
Supposons que $P \neq 0$ et $Q \neq 0$, alors

$$\deg(P \times Q) = \deg(P) + \deg(Q) \neq -\infty \Longrightarrow P \times Q \neq 0$$

Donc $(K[X], +, \times)$ est intègre. ■

**Proposition 2.1.8** *$(K[X], +, \times, \cdot)$ est une $K-$algèbre associative, commutative et unitaire.*

**Preuve.** On montre les axiomes suivants :
1) $(K[X], +, \cdot)$ est un espace vectoriel sur $K$.

2) $\times$ est distributive sur $+$.
3) $\forall \lambda \in K, \forall P_1, P_2 \in K[X] : \lambda \cdot (P_1 \times P_2) = (\lambda \cdot P_1) \times P_2 = P_1 \times (\lambda \cdot P_2)$
4) $\times$ est commutative, associative, et admet un neutre.
Alors
1)
*a*) D'après la proposition (2.1.7), on a $(K[X], +)$ est un groupe commutatif.
*b*) Soient $\lambda \in K, P_1 = (a_n)_n, P_2 = (b_n)_n \in K[X]$, alors

$$\begin{aligned} \lambda \cdot (P_1 + P_2) &= \lambda \cdot (a_n + b_n)_n = (\lambda (a_n + b_n))_n = (\lambda a_n + \lambda b_n)_n = \\ &= (\lambda a_n)_n + (\lambda b_n)_n = \lambda \cdot P_1 + \lambda \cdot P_2 \end{aligned}$$

*c*) Soient $\lambda_1, \lambda_2 \in K, P_1 = (a_n)_n \in K[X]$, alors

$$\begin{aligned} (\lambda_1 + \lambda_2) \cdot P_1 &= (\lambda_1 + \lambda_2) \cdot (a_n)_n = ((\lambda_1 + \lambda_2) a_n)_n = (\lambda_1 a_n + \lambda_2 a_n)_n = (\lambda_1 a_n)_n + (\lambda_2 a_n)_n = \\ &= \lambda_1 \cdot P_1 + \lambda_2 \cdot P_1 \end{aligned}$$

*d*) Soient $\lambda_1, \lambda_2 \in K, P_1 = (a_n)_n \in K[X]$, alors

$$(\lambda_1 \lambda_2) \cdot P_1 = (\lambda_1 \lambda_2) \cdot (a_n)_n = ((\lambda_1 \lambda_2) a_n)_n = (\lambda_1 (\lambda_2 a_n))_n = \lambda_1 \cdot ((\lambda_2 \cdot a_n))_n = \lambda_1 \cdot (\lambda_1 \cdot P_1)$$

*e*) Soit, $P_1 = (a_n)_n \in K[X]$, alors

$$1_K \cdot P_1 = 1_K \cdot (a_n)_n = (a_n)_n = P_1$$

Donc $(K[X], +, \cdot)$ est un espace vectoriel sur $K$.
2) D'après la proposition (2.1.7), on a $\times$ est distributive sur $+$..
3) Soient $\lambda \in K, P_1 = (a_n)_n, P_2 = (b_n)_n \in K[X]$, alors

$$\lambda \cdot (P_1 \times P_2) = \lambda \cdot (c_n)_n = (\lambda . c_n)_n, c_n = \sum_{k=0}^{n} (a_k b_{n-k})$$

On a

$$\lambda . c_n = \lambda . \sum_{k=0}^{n} (a_k b_{n-k}) = \sum_{k=0}^{n} (\lambda a_k) b_{n-k} = \sum_{k=0}^{n} a_k (\lambda . b_{n-k})$$

$$\Longrightarrow \lambda \cdot (P_1 \times P_2) = (\lambda \cdot P_1) \times P_2 = P_1 \times (\lambda \cdot P_2)$$

4) D'après la proposition (2.1.7), on a $\times$ est commutative, associative, et admet un neutre.
■

**Proposition 2.1.9** *(Plongement de $K$ dans $K[X]$ )*

*L'application*

$$\begin{array}{rccl} f: & K & \longrightarrow & K[X] \\ & \lambda & \longmapsto & f(\lambda) = \lambda.X^0 = \lambda.1 = \lambda \end{array}$$

*est un morphisme d'algèbre injectif. De plus* $f(1) = 1$.

Ceci permet d'identifier $K$ à $K_0[X]$ où $K_0[X]$ est l'ensemble des polynômes de degré au plus 0 (i.e : $K$ à sont image par $f$). Par conséquent $0_K$ est identifié au polynôme nul 0, et l'élément unité de $K$ est identifié au polynôme constant 1.

Ainsi $K$ est considéré comme (un sous ensemble) une sous algèbre unitaire de $K[X]$, en particulier $K[X]$ est un sous anneau de $K[X]$, et $K$ est un sous espace vectoriel de $K-$espace vectoriel $K[X]$.

**Preuve.**

1. Soient $\lambda \in K, \alpha_1, \alpha_2 \in K[X]$, alors :
   (a) $f(\alpha_1 + \alpha_2) = (\alpha_1 + \alpha_2).1 = \alpha_1.1 + \alpha_2.1 = f(\alpha_1) + f(\alpha_2)$.
   (b) $f(\alpha_1.\alpha_2) = (\alpha_1.\alpha_2).1 = (\alpha_1.\alpha_2) = (\alpha_1.1).(\alpha_2.1) = f(\alpha_1).f(\alpha_2)$.
   Donc $f$ est un morphisme d'algèbre.
   (c) On a
   $$f(1) = f(1_K) = 1_K.1_{K(X)} = 1 = 1_{K(X)}$$
2. On a
   $$\begin{array}{rcl} f(\alpha_1) = f(\alpha_2) & \Longrightarrow & \alpha_1.1 = \alpha_2.1 \\ & \Longrightarrow & \alpha_1 = \alpha_2 \end{array}$$
   Donc $f$ est injective.

■

**Proposition 2.1.10** *Les éléments inversibles de l'anneau* $K[X]$ *est l'ensemble des polynômes constants non nuls* $(K^*)$.

**Preuve.** Si $P$ est inversible dans $K[X]$, alors il existe un polynôme $Q$ tel que $P \times Q = 1$. Alors $P \neq 0$ et $Q \neq 0$ puisque $K[X]$ est intègre. On obtient

$$\deg(P \times Q) = \deg(P) + \deg(Q) = 0 \Longrightarrow \deg(P) = \deg(Q) = 0$$

Alors il existe $c \in K^* : P = c.1 = c$.
Réciproquement : Il est clair que pour tout $\lambda \in K^*$, le polynôme $P = \lambda$ est inversible et a pour inverse $\lambda^{-1}$. ■

**Définition 2.1.11** *Soit $P = a_0 + a_1X + ... + a_{n-1}X^{n-1} + a_nX^n$ un polynôme de $K[x]$. On appelle la fonction polynômiale associée à $P$, la fonction $\widetilde{P}$ définie par :*

$$\begin{array}{rccl} \widetilde{P}: & K & \longrightarrow & K \\ & x & \longmapsto & \widetilde{P}(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n \end{array}$$

**Remarque 2.1.12**
*1) On ne pas confondre la variable $x$, qui est un élément de $K$, avec l'indéterminée $X$ (qui n'appartient pas à $K$).*
*2) Pour tous $\alpha \in K, P, Q \in K[X]$, on a*

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}, \widetilde{\alpha.P} = \alpha.\widetilde{P}$$

**Définition 2.1.13**
*1) Soit $P = \sum_{k=0}^{n} a_kX^k \in K[X]$. On appelle polynôme dérivé de $P$, le polynôme noté $P'$ défini par $P' = \sum_{k=1}^{n} ka_kX^{k-1} = \sum_{k=0}^{n-1} (k+1)\, a_{k+1}X^k$.*
*2) On note $P^{(0)} = P$, $\forall n \in \mathbb{N} : P^{(n+1)} = [P^{(n)}]'$.*

**Remarque 2.1.14**
*1)*

$$\forall P \in K[X] : \deg(P') = \begin{cases} \deg(P) - 1, \ si \ \deg(P) \geq 1 \\ -\infty, \ si \ \deg(P) < 0 \end{cases}$$

*2) $\forall \alpha \in K, P, Q \in K[X] : (P+Q)' = P' + Q', (P \times Q)' = P' \times Q + P \times Q', (\alpha.P)' = \alpha.P'$.*

## 2.2 Arithmétique des polynômes

**Définition 2.2.1** *Soient $A, B \in K[X]$. On dit que le polynôme $B$ divise $A$ et on note $B \mid A$ s'il existe un polynôme $Q$ tel que $A = BQ$. Dans ce cas, on dit que $A$ est un multiple de $B$ (ou que $B$ est un diviseur de $A$).*
*Dans le cas ou $A$ et $B$ sont tous les deux non nuls, $B \mid A$ entraîne $\deg(B) \leq \deg(A)$.*

On a les propriétés suivantes :
1) $\forall A \in K[X] : A \mid A, A \mid 0$.
2) $\forall A \in K[X] : 0 \mid A \Longleftrightarrow A = 0$
3) $\forall A, B, C \in K[X] : \begin{cases} A \mid B \wedge B \mid C \Longrightarrow A \mid C \\ A \mid B \Longrightarrow A \mid B \times C \\ A \mid B \wedge A \mid C \Longrightarrow A \mid B + C \end{cases}$

4) $\forall A, B, C, D \in K[X] : A \mid B \wedge C \mid D \Longrightarrow A \times C \mid B \times D$

**Proposition 2.2.2** *Soit $A$ et $B$, deux polynômes non nuls. Si $A \mid B$ et $B \mid A$ alors il existe $\lambda \in K^*$ tel que $A = \lambda B$. On dit que $A$ et $B$ sont associés.*

**Preuve.** Or $A$ et $B$ sont non nuls, et $A \mid B$ et $B \mid A$ alors $\deg(A) \leq \deg(B)$ et $\deg(B) \leq \deg(A)$. Donc $A$ et $B$ sont de même degré. Comme $B \mid A$, on en déduit que $A = BQ$ avec $\deg(Q) = 0$. Autrement dit $Q$ est un polynôme constant et non nul car $A$ n'est pas nul. ■

**Théorème 2.2.3** ***(Définition) Division Euclidienne (division suivant les puissances décroissantes)***
*Soient $A$ et $B$ deux éléments de $K[X]$, avec $B \neq 0$. Il existe un unique couple $(Q, R)$ de polynomes de $(K[X])^2$ tel que :*

$$\begin{cases} A = QB + R \\ \deg(R) < \deg(B) \end{cases}$$

*Le polynôme $Q$ (resp :$R$ ) s'appelle le quotient (resp : le reste ) de la division euclidienne de $A$ par $B$.*
*Si $R = 0$, on dit que $B$ divise $A$.*

**Preuve.** Voir [1] ■

**Théorème 2.2.4** ***(Définition) Division suivant les puissances croissantes***
*Soient $n \in \mathbb{N}$, $A, B \in K[X]$ tel que $\widetilde{B}(0) \neq 0$. Il existe un couple unique $(Q, R) \in (K[X])^2$ tels que :*

$$\begin{cases} A = BQ + X^{n+1}R \\ \deg(Q) < n \end{cases}$$

*Le polynôme $Q$ (resp :$R$ ) s'appelle le quotient (resp : le reste ) de la division de $A$ par $B$ suivant les puissances croissantes de $X$ jusqu'à l'ordre $n$.*

**Preuve.** Voir [1] ■

**Exemple 2.2.5**
*1) Divisions $A = 2X^4 + X^3 - X^2 + X + 1$ par $B = 2X^2 - X - 2$ de $\mathbb{R}[X]$, on obtient*

$$A = 2X^4 + X^3 - X^2 + X + 1 = \left(2X^2 - X - 2\right)\left(X^2 + X + 1\right) + 4X + 3$$

*2) Divisions* $A = 1 + 3X + 2X^2 - 7X^3$ *par* $B = 1 + X - 2X^2$*, jusqu'à l'ordre* 3 *alors*

$$A = 1 + 3X + 2X^2 - 7X^3 = \left(1 + X - 2X^2\right)\left(1 + 2X + 2X^2 - 5X^3\right) + X^4(9 - 10X)$$

*où* $R = 9 - 10X$.

**Définition 2.2.6** *Soient* $P \in K[X]$ *et* $a \in K$*. On dit que* $a$ *est une racine de* $P$ *si et seulement si* $\widetilde{P}(a) = 0$.

**Proposition 2.2.7** *Soient* $P \in K[X]$ *et* $a \in K$*. Alors* $a$ *est une racine de* $P$ *si et seulement si* $X - a \mid P$.

**Preuve.**
1) Soit $a$ une racine de $P$. Alors $\widetilde{P}(a) = 0$. Par division euclidienne, il existe $(Q, R) \in (K[X])^2$ tels que $P = (X - a)Q + R$ tel que $\deg(R) < \deg(X - a) = 1$. On a alors deux possibilités, soit $\deg(R) = -\infty$, soit $\deg(R) = 0$, c'est à dire $R = 0$. Montrons que la première n'est pas possible :
Si $\deg(R) = 0$, alors il existe $\lambda \in K^*$ tel que $R = \lambda$, on obtient $P = (X - a)Q + \lambda$, mais alors $\widetilde{P}(a) = \widetilde{R}(a) = \lambda \neq 0$, ce qui est une contradiction. On a donc $R = 0$ et $P = (X - a)Q$.
2) Supposons que $X - a \mid P$. Alors il existe $Q \in K[X]$ tel que $P = (X - a)Q$. Par conséquent $\widetilde{P}(a) = 0$, ce qui prouve que $a$ est une racine de $P$. ■

**Définition 2.2.8** *Soient* $P \in K[X]$*, un polynôme* $a \in K, r \in \mathbb{N}^*$.
*On dit que* $a$ *est une racine d'ordre* $r$ *(ou de multiplicité* $r$*) de* $P$ *si selement si* $(X-a)^r \mid P$ *et* $(X - a)^{r+1} \not| P$.
*Il est équivalent de dire que* $P(a) = P^{(1)}(a) = P^{(2)}(a) = ... = P^{(r-1)}(a) = 0, P^{(r)}(a) \neq 0$.
*Si* $r = 1$*. On dit que* $a$ *est une racine simple.*
*Si* $r = 2$*. On dit que* $a$ *est une racine multiple.*
*Si* $r = 3$*, on dit que* $a$ *est racine triple, etc.*

**Remarque 2.2.9**
*1) Si* $P \neq 0$*, alors toutes les racines de* $P$ *sont de multiplicité inférieure ou égale à* $\deg(P)$.
*2) Si* $P \neq 0$*, alors la somme des ordres de multiplicité des racines de* $P$ *est inférieure ou égale à* $\deg(P)$.
*3) Soit* $P$ *un polynôme non nul admettant les racines* $a_1, ..., a_k$ *avec multiplicité* $r_1, ..., r_k$.
*Alors* $\prod_{i=1}^{k} (X - a_i)$ *divise* $P$.

*4) Le polynôme nul ayant une infinité de racines.*
*5) Si $a$ est une racine de $P$ d'ordre $r \geq 1$, alors $a$ est une racine de $P'$ d'ordre $r-1$.*
*6) Si $a$ est une racine complexe de $P$ d'ordre $k$ alors le conjugué $\bar{a}$ est une racine de $P$ d'ordre $k$. En effet : Si $P \in \mathbb{R}[X]$ et si $a \in \mathbb{C}$, alors $P(\bar{a}) = \overline{P(a)} = 0$. (racine simple).*

**Définition 2.2.10** *(polynôme scindé)*
*Si $a_1, ..., a_n$ sont les racines distinctes de $P$ de multiplicités respectives $m_1, ..., m_n$, alors $\sum_{k=1}^{n} m_k \leq \deg(P)$. La quantité $\sum_{k=1}^{n} m_k$ (somme des multiplicités des racines) est appelée nombre de racines de $P$ comptées avec leur multiplicité. On dit que le polynôme $P$ est scindé sur $K$ lorsque cette quantité est égale au degré de $P$.*

**Remarque 2.2.11** *$P$ de degré $n$ est scindé si et seulement si il existe $\alpha, \lambda_1, \lambda_2, ..., \lambda_n \in K : P = \alpha(X - \lambda_1)(X - \lambda_2)...(X - \lambda_n)$*

**Exemple 2.2.12** *$P_1 = X^2 - 2$ est scindé sur $\mathbb{R}$, mais pas sur $\mathbb{Q}$. $P_2 = X^2 + 1$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.*

Le très important résultat suivant est connu sous le nom de théorème fondamental de l'algèbre ou théorème de d'Alembert-Gauss. Il existe de nombreuses preuves, Le théorème de d'Alembert-Gauss, simplement appelé théorème de d'Alembert ou encore théorème fondamental de l'algèbre, s'énonce de la façon suivante :

**Théorème 2.2.13** *Tout polynôme de $\mathbb{C}[X]$ de degré supérieur ou égal à $1$ $(n \geq 1)$ admet au moins une racine complexe.*
*En outre : Tout polynôme $P = a_0 + a_1X + ... + a_nX^n$ de $\mathbb{C}[X]$ de degré $n$ supérieur ou égalà $1$ admet $n$ racines distinctes ou confondues.*

**Preuve.** Voir [2] ■

**Conclusion 2.2.14** *Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.*

**Remarque 2.2.15** *Le théorème n'est plus vrai dans $\mathbb{R}[X]$. Exemple : $P = X^2 + 1$ n'a pas de racines réelles.*

**Définition 2.2.16** *(plus grand commun diviseur, plus petit commun multiple)*
*Soient $n \in \mathbb{N}^*, P_1, P_2, ..., P_n \in K[X] - \{0\}$. Alors*
*1) Il existe un polynôme et un seul $\triangle$, unitaire non nul, diviseur commun de $P_1, P_2, ..., P_n$ et de plus haut degré parmi les diviseurs communs de $P_1, P_2, ..., P_n$. $\triangle$ est appelé le plus grand commun diviseur (en abrégé : pgcd) de $P_1, P_2, ..., P_n$ et noté $pgcd(P_1, P_2, ..., P_n)$.*
*2) Il existe un polynôme et un seul $M$, unitaire non nul, multiple commun de $P_1, P_2, ..., P_n$ et de plus bas degré parmi les multiples communs de $P_1, P_2, ..., P_n$. $M$ est appelé le plus petit commun multiple (en abrégé : ppcm) de $P_1, P_2, ..., P_n$ et noté $ppcm(P_1, P_2, ..., P_n)$.*

**Notation 2.2.17** *Pour* $(P,Q) \in (K[X]-\{0\})^2$*, on note*

$$\begin{cases} pgcd\,(P,Q) = P \wedge Q \\ ppcm\,(P,Q) = P \vee Q \end{cases}$$

**Remarque 2.2.18**
*1)* $\wedge$ *et* $\vee$ *sont des lois de composition interne dans* $K[X]-\{0\}$*, commutatives et associatives. De plus pour tout polynôme unitaire* $P \in K[X]-\{0\}$ : $P \wedge P = P, P \vee P = P, P \wedge 1 = 1, P \vee 1 = 1$.
*2) Si* $n \in \mathbb{N}^*, P_1, P_2, ..., P_n, A \in K[X]-\{0\}, \alpha_1, ..., \alpha_n \in K-\{0\}$*, alors*

$$\begin{cases} pgcd\,\{\alpha_i P_i\}_{i=\overline{1,n}} = pgcd\,\{P_i\}_{i=\overline{1,n}}, & ppcm\,\{\alpha_i P_i\}_{i=\overline{1,n}} = ppcm\,\{P_i\}_{i=\overline{1,n}} \\ pgcd\,\{AP_i\}_{i=\overline{1,n}} = A.pgcd\,\{P_i\}_{i=\overline{1,n}}, & ppcm\,\{AP_i\}_{i=\overline{1,n}} = A.ppcm\,\{P_i\}_{i=\overline{1,n}} \end{cases}$$

**L'algorithme d'Euclide**

L'algorithme d'Euclide est un procédé itératif permettant de calculer le *pgcd* de deux polynômes. L'outil de base est la division euclidienne. L'algorithme repose sur l'idée suivante : $pgcd(A,B) = pgcd(B,R)$ où $R$ est le reste de la division euclidienne de $A$ par $B$. En raisonnant comme l'étude de l'algorithme d'Euclide dans $\mathbb{Z}$, on voit que le $pgcd\,(A,B)$ est le dernier reste non nul normalisé dans la suite des divisions euclidiennes successives. On effectue les divisions euclidiennes successives des quotients par leurs restes, jusqu'a arriver à un reste nul, alors le dernier reste non nul est un diviseur commun de A et B de degré minimal, ce reste une fois normalisé s'appelle le *pgcd* de $A$ et $B$.

**Lemme 2.2.19** *Soit* $B$ *un polynôme non nul, et* $A$ *un polynôme quelconque. Notons* $Q$ *et* $R$ *le quotient et le reste de la division euclidienne de* $A$ *par* $B$*. Alors on a* $pgcd(A,B) = pgcd(B,R)$.

**Preuve.** Soit $D$ divisant $A$ et $B$. Comme $R = A - BQ$, le polynôme $D$ divise aussi $R$. Donc $D$ divise $pgcd(B,R)$. En choisissant $D = pgcd(A,B)$, on conclut que $pgcd(A,B) \mid pgcd(B,R)$.
Soit maintenant $D$ un polynôme divisant $B$ et $R$. Comme $A = BQ + R$, on a aussi $D \mid A$. Donc $D \mid pgcd(A,B)$. On a donc finalement $pgcd(B,R) \mid pgcd(A,B)$. Les deux polynômes $pgcd(B,R)$ et $pgcd(A,B)$ sont unitaires et associés. Ils sont donc égaux. ■

Pour calculer le *pgcd*. $D$ de deux polynômes non nuls $A$ et $B$, on procède de la manière suivante. On commence par écrire $A = BQ_1 + R_1$ avec $\deg(R_1) < \deg(B)$. Si $R_1 = 0$, alors $D = B$.

Sinon on recommence

$B = R_1Q_2 + R_2$ avec $\deg(R_2) < \deg(R_1)$. Si $R_2 = 0$, alors $D = R_1$.

Sinon on recommence
$R_1 = R_2Q_3 + R_3$ avec $\deg(R_3) < \deg(R_2)$. Si $R_3 = 0$, alors $D = R_2$.
Sinon on recommence
.....
On finit par avoir, à un certain rang $N$
$R_N = R_{N+1}Q_{N+2} + R_{N+2}$ avec $\deg(R_{N+2}) < \deg(R_{N+1})$, $R_{N+2} \neq 0$
$R_{N+1} = R_{N+2}Q_{N+3} + R_{N+3}$ avec $R_{N+3} = 0$.
Donc $D = pgcd(A, B) = R_{N+2}$
et
$pgcd(A, B) = pgcd(B, R_1) = pgcd(R_1, R_2) = ... = pgcd(R_{N+2}, 0) = R_{N+2}$

| | $Q_1$ | $Q_2$ | $Q_3$ | | $Q_{N+2}$ | $Q_{N+3}$ |
|---|---|---|---|---|---|---|
| $A$ | $B$ | $R_1$ | $R_2$ | .... | $R_{N+1}$ | $R_{N+2}$ |
| $R_1$ | $R_2$ | $R_3$ | | | $R_{N+3} = 0$ | |

**Exemple 2.2.20** $A = X^5 + X + 1, B = X^4 - 2X^3 - X + 2$, *alors*

| | $Q_1 = X + 2$ | $Q_2 = \frac{1}{4}X - \frac{9}{10}$ | $Q_3 = 4X - 3$ |
|---|---|---|---|
| $A = X^5 + X + 1$ | $B = X^4 - 2X^3 - X + 2$ | $R_1 = 4X^3 + X^2 + X - 3$ | $R_2 = X^2 + X + 1$ |
| $R_1 = 4X^3 + X^2 + X - 3$ | $R_2 = \frac{5}{16}X^2 + \frac{5}{16}X + \frac{5}{16}$ | $R_3 = 0$ | |

*On obtient* $pgcd(A, B) = pgcd(B, R_1) = pgcd(R_1, R_2) = pgcd(R_2, 0) = R_2 = X^2 + X + 1$

**Proposition 2.2.21** *Pour tout couple* $(A, B)$ *de polynômes de* $K[X]$ *unitaires. On a la relation*

$$pgcd(A, B) \times ppcm(A, B) = AB$$

**Preuve.** Posons $D = pgcd(A, B)$ et $M = ppcm(A, B)$. Puisque $D$ divise $A$ et $B$, on peut écrire $A = DA_1$ et $B = DB_1$ avec $(A_1, B_1) \in K[X]$. Considérons alors le polynôme $P = DA_1B_1 = A_1B = AB_1$. Les polynômes $A$ et $B$ divisent $P$ donc $M$ divise $P$ puis $DM$ divise $DP = AB$. Inversement, puisque $AB$ est un multiple commun à $A$ et $B$, on peut écrire $AB = MQ$ avec $Q \in K[X]$. Or $M$ est un multiple de $A$ donc on peut écrire $M = AC$. La relation $AB = ACQ$ donne alors $B = CQ$. Ainsi $Q$ divise $B$. De façon analogue, on obtient que $Q$ divise $A$ et donc $Q$ divise $D$. On en déduit que $AB = MQ$ divise $MD$. Puisque $AB$ et $MD$ se divisent mutuellement et ces deux polynômes sont unitaires, ils sont donc égaux. ■

**Définition 2.2.22** *Soient* $n \in \mathbb{N}^*, P_1, P_2, ..., P_n \in K[X] - \{0\}$. *Alors :*
*1)Les polynômes* $P_1, P_2, ..., P_n$ *sont dits premiers entre eux si et seulement si leurs seuls*

*diviseurs communs sont les polynômes constants non nuls, c'est à dire si et seulement si* $pgcd(P_1, P_2, ..., P_n) = 1$.
*2) Les polynômes* $P_1, P_2, ..., P_n$ *sont dits premiers entre eux deux à deux si et seulement si*

$$\forall (i,j) \in \{1,2,...,n\}^2 : pgcd(P_i, P_j) = 1.$$

**Théorème 2.2.23**
*1) Théorème de Bézout généralisé : Soient* $P$ *et* $Q$ *deux polynômes de* $K[X]$. *Alors* $D = pgcd(P,Q)$ *si et seulement s'il existe deux polynômes* $U$ *et* $V$ *de* $K[X]$ *tels que* $PU+QV = D$.
*2) Théorème de Bézout : En particulier,* $P$ *et* $Q$ *sont premiers entre eux si et seulement s'il existe deux polynômes* $U$ *et* $V$ *de* $K[X]$ *tels que*$PU + QV = 1$

**Preuve.** Voir [5] ■

**Remarque 2.2.24** *Généralisation de Théorème de Bézout :*
*1) Soient* $P_1, P_2, ..., P_n, D \in K[X]$, *Alors*

$$D = pgcd(P_1, P_2, ..., P_n) \Longleftrightarrow \exists U_1, U_2, ..., U_n \in K[X] : U_1P_1 + U_2P_2 + ... + U_nP_n = D$$

*2)* $P_1, P_2, ..., P_n \in K[X]$ *sont premiers entre eux si et seulement s'il existe* $U_1, U_2, ..., U_n \in K[X]$ *tels que* $U_1P_1 + U_2P_2 + ... + U_nP_n = 1$.

**Exemple 2.2.25** *Les polynômes* $A = X^4 + 1$ *et* $B = X^3 - 1$ *de* $\mathbb{R}[X]$ *sont premier entre eux car il existe deux polynômes* $U$ *et* $V$ *de* $\mathbb{R}[X]$ *tels que* $AU + BV = 1$. *En effet :*
*On effectue l'algorithme d'Euclide, on obtient*

| | $Q_1 = X$ | $Q_2 = X^2 - X + 1$ |
|---|---|---|
| $A = X^4 + 1$ | $B = X^3 - 1$ | $R_1 = X + 1$ |
| $R_1 = X + 1$ | $R_2 = -2$ | |

*Donc*

$$\begin{aligned}
-2 &= X^3 - 1 - (X+1)\left(X^2 - X + 1\right) = X^3 - 1 - \left(\left(X^4+1\right) - X\left(X^3 - 1\right)\right)\left(X^2 - X + 1\right) = \\
&= \left(X^3 - X^2 + X + 1\right)\left(X^3 - 1\right) - \left(X^2 - X + 1\right)\left(X^4 + 1\right) \\
&\Longrightarrow \frac{-1}{2}\left(X^3 - X^2 + X + 1\right)\left(X^3 - 1\right) + \frac{1}{2}\left(X^2 - X + 1\right)\left(X^4 + 1\right) = 1 \\
&\Longrightarrow U = \frac{1}{2}\left(X^2 - X + 1\right), V = \frac{-1}{2}\left(X^3 - X^2 + X + 1\right)
\end{aligned}$$

Les résultats suivant sont des Conséquences (Première et deuxième conséquence) du théorème de Bézout

**Théorème 2.2.26** *(Gauss)*
*Soient $A, B, C \in K[X]$. Si $A$ divise $BC$ et $A$ est premier avec $B$, alors $A$ divise $C$.*

**Preuve.** $A$ divise $BC$ donc il existe $Q$ tel que $AQ = BC$. Or $A$ est premier avec $B$ donc il existe $U, V$ tels que $AU + BV = 1$. Alors $AUC + AQV = C$. Donc $A$ divise $C$. ■

**Corollaire 2.2.27** *Soient $A, B \in K[X]$ tels que $pgcd(A, B) = 1$. Si $A$ divise $C$ et $B$ divise $C$ alors $AB$ divise $C$.*

**Preuve.** $A$ divise $C$ donc il existe $Q$ tel que $AQ = C$ , $B$ divise $C = AQ$ et $B$ premier avec $A$ donc (Gauss) $B$ divise $Q$. Il existe alors $P$ tel que $Q = BP$. D'où $C = ABP$ et $AB$ divise $C$. ■

## 2.3 Polynômes irréductibles et décomposition d'un polynôme

Dans cette partie, nous allons introduire une classe de polynômes qui jouent dans $K[X]$ le même rôle que les nombres premiers dans $\mathbb{Z}$ : les polynômes irréductibles.

**Définition 2.3.1** *Soit $P$ un polynôme non constant de $K[X]$. On dit que $P$ est irréductible ou premier dans $K[X]$ si et seulement si ses seuls diviseurs dans $K[X]$ sont les polynômes constants non nuls $\lambda \in K^*$ et les polynômes associés à $P$, c'est à dire les $\lambda P$, avec $\lambda$ dans $K^*$.*

**Exemple 2.3.2**
*Les polynômes de degré 1 sont irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.*
*$X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, le même polynôme est réductible dans $\mathbb{C}[X]$.*

**Proposition 2.3.3** *Tout polynôme $P$ de $K[X]$ de degré 1 est irréductible dans $K[X]$.*

**Preuve.** Soit $P$ de degré 1, et $Q$ un diviseur de $P$. Alors $\deg(Q) \in \{0, 1\}$. Si $\deg(Q) = 0$, alors $Q$ est une constante, si $\deg(Q) = 1$, alors $\deg(Q) = \deg(P)$ donc $P$ et $Q$ sont associés. ■

**Remarque 2.3.4** *La notion de polynôme irréductible dépend du corps $K$, par exemple $P = X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans $\mathbb{R}[X]$.*

**Proposition 2.3.5**

*1) Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1.

*2) Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont :*

- *les polynômes de degré* 1.
- *les polynômes de degré* 2 *dont le discriminant est négatif (Trinômes).*

**Preuve.**

1) D'après le théorème de d'Alembert-Gauss.

2) i) Soit $P \in \mathbb{R}[X]$, tel que $\deg(P) \geq 0$. Comme $P \in \mathbb{C}[X]$, alors le théorème de d'Alembert-Gauss montre que $P$ admet au moins une racine $a$ dans $\mathbb{C}$. Si $a \in \mathbb{R}$, alors $(X-a) \mid P$ dans $\mathbb{R}[X]$ ce qui contredit l'irréductibilité de $P$ dans $\mathbb{R}[X]$. Donc $a \in \mathbb{C}-\mathbb{R}$. D'autre part, on sait que $\bar{a}$ est une racine aussi de $P$. Alors on pose $T = (X-a)(X-\bar{a})$. On a $T$ divise $P$ dans $\mathbb{C}[X]$. Mais $T = X^2 - 2Ré(a)X + |a|^2 \in \mathbb{R}[X]$, on obtient que $T \mid P$. Or $P$ est irréductible, alors il existe $\lambda \in K^*$ tel que $P = \lambda T$ et donc $P$ est un trinôme de degré 2 à discriminant $\triangle = (2Ré(a))^2 - |a|^2 = -|\mathrm{Im}(a)|^2 < 0$.

ii) Il est clair que les polynômes de degré 1 sont irréductibles dans $\mathbb{R}[X]$.

Supposons que $P = X^2 + aX + b$ ne soit pas irréductible dans $\mathbb{R}[X]$, alors

$$\exists A, B \in K[X] - \mathbb{R}^* : P = AB \Longrightarrow \deg(P) = 2 = \deg(A) + \deg(B)$$

Or $A, B$ ne sont pas inversibles, alors $\deg(A) = \deg(B) = 1$. Puisque $P$ est unitaire, il existe $a, b \in \mathbb{R}$ tels que $A = X - a, B = X - b$. Alors $P = AB = X^2 - (a+b)X + ab$ et le discriminant $\triangle = (a+b)^2 - 4ab = (a-b)^2 \geq 0$. Contradiction. ■

**Théorème 2.3.6** *Décomposition en facteurs irréductibles*

*Soit* $P = a_0 + a_1X + ... + a_nX^n \in \mathbb{R}[X]$ *de dégré* $n \geq 1$. *Soient* $x_1, x_2, ..., x_m$ *les racines réelles distinctes de* $P$ *d'ordres respectifs* $k_1, k_2, ..., k_m$. *Soient* $z_1, z_2, ..., z_l, \bar{z}_1, \bar{z}_2, ..., \bar{z}_l$ *les racines complexes distinctes de* $P$ *et* $r_1, r_2, ..., r_l$ *les ordres respectifs de* $z_1, z_2, ..., z_l$. *Alors* $P$ *admet une décomposition unique en produit de polynômes irréductibles :*

*1) Dans* $\mathbb{C}[X]$ *sous la forme*

$$\begin{aligned} P &= a_n (X-x_1)^{k_1} ... (X-x_m)^{k_m} . (X-z_1)^{r_1} ... (X-z_l)^{r_l} . (X-\bar{z}_1)^{r_1} ... (X-\bar{z}_l)^{r_l} \\ &= a_n \prod_{i=1}^{m} (X-x_i)^{ki} . \prod_{j=1}^{l} (X-z_j)^{rj} (X-\bar{z}_j)^{rj} \end{aligned}$$

*où* $k_1 + k_2 + ... + k_m + 2(r_1 + r_2 + ... + r_l) = n$.

*2) Dans $\mathbb{R}[X]$ sous la forme*

$$\begin{aligned} P &= a_n (X-x_1)^{k_1} ... (X-x_m)^{k_m} . \left(X^2+p_1X+q_1\right)^{r_1} . \left(X^2+p_2X+q_2\right)^{r_1} ... \left(X^2+p_lX+q_l\right)^{r_l} \\ &= a_n \prod_{i=1}^{m} (X-x_i)^{ki} . \prod_{j=1}^{l} \left(X^2+p_jX+q_j\right)^{rj} \end{aligned}$$

*Où*

$$\forall j \in \{1,2,...,l\} : p_j = -\left(z_j+\bar{z}_j\right), q_j = z_j.\bar{z}_j, \triangle_j = p_j^2 - 4q_j < 0.$$

**Preuve.** Voir [1] ■

**Exemple 2.3.7** *Donner la décomposition de $P = X^4+1$ en facteurs irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$. On a*

$$\begin{aligned} X^4+1 &= 0 \Longleftrightarrow X^4 = -1 = e^{i\pi} \\ &\Longleftrightarrow X \in \left\{\omega_1 = e^{i\frac{\pi}{4}}, \omega_2 = \bar{\omega}_1, \omega_3 = e^{i\frac{3\pi}{4}}, \omega_4 = \bar{\omega}_3\right\} \\ &\Longleftrightarrow X \in \left\{\omega_1 = \frac{1+i}{\sqrt{2}}, \omega_2 = \frac{1-i}{\sqrt{2}}, \omega_3 = -\frac{1-i}{\sqrt{2}}, \omega_4 = -\frac{1+i}{\sqrt{2}}\right\} \end{aligned}$$

*La factorisation dans $\mathbb{C}[X]$ est donc :*

$$P = X^4+1 = \left(X-\frac{1+i}{\sqrt{2}}\right)\left(X-\frac{1-i}{\sqrt{2}}\right)\left(X+\frac{1-i}{\sqrt{2}}\right)\left(X+\frac{1+i}{\sqrt{2}}\right)$$

*La factorisation dans $\mathbb{R}[X]$ est*

$$P = X^4+1 = \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right)$$

# Chapitre 3

# Algèbre des fractions rationnelles

Nous allons examiner dans ce chapitre une construction générale qui permet de construire un corps à partir d'un anneau, similaire à celle permettant de passer de $\mathbb{Z}$ à $\mathbb{Q}$, du corps des fractions rationnelles à une indéterminée. La construction envisagée ici utilise les notions de relation d'équivalence et de classes d'équivalence.

## 3.1 Construction de l'ensemble des fractions rationnelles

Dans l'ensemble $E = K[X] \times K[X] - \{0\} = \{(P, Q) : P, Q \in K[X], Q \neq 0\}$, on définit une relation binaire $\Re$ en posant :

$$\forall (P, Q), (R, S) \in E : (P, Q) \Re (R, S) \Longleftrightarrow PS = QR$$

**Proposition 3.1.1** *La relation $\Re$ est une relation d'équivalence sur $E$.*

**Preuve.**
i) Réflexivité : On a $\forall (P, Q) \in E : PQ = QP$. C'est à dire $(P, Q) \Re (P, Q)$, alors $\Re$ est réflexive.
ii) Symétrie : On a $\forall (P, Q), (R, S) \in E$ :

$$\begin{aligned} (P, Q) \Re (R, S) &\Longleftrightarrow PS = QR \Longleftrightarrow SP = RQ \\ &\Longleftrightarrow RQ = SP \\ &\Longrightarrow (R, S) \Re (P, Q) \end{aligned}$$

Donc $\Re$ est symétrique.
iii) Transitivité : On a soient $(P,Q),(R,S),(T,V) \in E$ :

$$\begin{cases} (P,Q)\,\Re\,(R,S) \\ (R,S)\,\Re\,(T,V) \end{cases} \Longleftrightarrow \begin{cases} PS = QR \\ RV = ST \end{cases}$$

Où $Q,S,V \in K[X]-\{0\}$, alors

$$\begin{aligned} PSRV &= QRST \Longrightarrow PSRV - QRST = 0 \\ &\Longrightarrow S\,(PRV - QRT) = 0 \end{aligned}$$

Comme $S \neq 0$ et $K[X]$ intègre, on a

$$PRV - QRT = 0 \Longrightarrow R\,(PV - QT) = 0$$

Si $R \neq 0$, alors

$$PV - QT = 0 \Longrightarrow PV = QT$$

Donc $(P,Q)\,\Re\,(T,V)$.
Si $R = 0$, alors

$$\begin{cases} PS = 0 \\ ST = 0 \end{cases}$$

Or $S \neq 0$, et $K[X]$ intègre, alors $P = T = 0$. On obtient

$$PV = QT = 0 \Longrightarrow (P,Q)\,\Re\,(T,V)$$

■

**Définition 3.1.2**
*1) On appelle fraction rationnelle à coefficients dans $K$ toute classe d'équivalence pour la relation $\Re$. La classe de $(P,Q)$ est notée $\frac{P}{Q}$ ( avec $P$ le numérateur et $Q$ le dénominateur), on a donc*

$$\frac{P}{Q} = \{(R,S) \in K[X] \times K[X] - \{0\} : PS = QR\}$$

*2) On dit que $(P,Q)$ est un représentant de la fraction $\frac{P}{Q}$.*
*3) L'ensemble des fractions rationnelles est noté $K(X)$ et la relation $\Re$ est appelée égalité des fractions rationnelles.*

$$\forall\,(P,Q),(R,S) \in E : \frac{P}{Q} = \frac{R}{S} \Longleftrightarrow PS = QR$$

*Autrement dit deux couples $(P,Q),(R,S)$ représentent la même fraction rationnelle si $PS = QR$.*

**Remarque 3.1.3** *L'ensemble quotient $E/\Re$ des classes d'équivalence modulo $\Re$ est noté $K(X)$ et ses éléments sont appelés fractions rationnelles (à une indéterminée sur $K$).*

**Définition 3.1.4** *Définissons trois lois de composition sur $K(X)$ :*
*1) Une loi interne (l'addition) $+$ :*
*On définit la somme de deux fractions en choisissant un représentant $\frac{P}{Q}$ et $\frac{R}{S}$ de chacune de ces fractions, en calculant $(PS+QR, QS)$ et en prenant la fraction rationnelle correspondante.*

$$\begin{array}{rccc} + : & K(X)\times K(X) & \longrightarrow & K(X) \\ & \left(\frac{P}{Q},\frac{R}{S}\right) & \longmapsto & \frac{P}{Q}+\frac{R}{S}=\frac{PS+QR}{QS} \end{array}$$

*2) Une loi interne (le produit) $\times$ :*
*On définit le produit de deux fractions par*

$$\begin{array}{rccc} \times : & K(X)\times K(X) & \longrightarrow & K(X) \\ & \left(\frac{P}{Q},\frac{R}{S}\right) & \longmapsto & \frac{P}{Q}\times\frac{R}{S}=\frac{PR}{QS} \end{array}$$

*3 Une loi externe (la multiplication par un scalaire) $\cdot$ :*
*On définit sur $K(X)$ une loi externe à coefficients dans $K$ par :*

$$\begin{array}{rccc} \cdot : & K\times K(X) & \longrightarrow & K(X) \\ & \left(\lambda,\frac{P}{Q}\right) & \longmapsto & \lambda\times\frac{P}{Q}=\frac{\lambda P}{Q} \end{array}$$

**Proposition 3.1.5** *Le résultat des opérations $+,\times$ et $\cdot$ définies sur $E$ ne dépend pas des représentants choisis ($+$ et $\times$ sont bien définies). Autrement dit la définition du produit (resp : de la somme) ne dépendant pas des polynômes $P$, $Q$, $R$ et $S$ mais seulement des classes d'équivalence des couples $(P,Q)$ et $(R,S)$. C'est à dire les fractions rationnelles $\frac{PS+QR}{QS}, \frac{PR}{QS}, \frac{\lambda P}{Q}$ restent inchangées si l'on remplace $(P,Q)$ et $(R,S)$ par d'autres représentants de $F=\frac{P}{Q}$,$G=\frac{R}{S}$ respectivement.*

**Preuve.** Soient $(P_1,Q_1)$,$(R_1,S_1),(P_2,Q_2),(R_2,S_2)\in E,\lambda\in K$ telles que

$$\begin{array}{rcl} \left(\frac{P_1}{Q_1},\frac{R_1}{S_1}\right) & = & \left(\frac{P_2}{Q_2},\frac{R_2}{S_2}\right) \\ \left(\lambda,\frac{P_1}{Q_1}\right) & = & \left(\lambda,\frac{P_2}{Q_2}\right) \end{array}$$

Alors

$$\begin{cases} \frac{P_1}{Q_1} = \frac{P_2}{Q_2} \\ \frac{R_1}{S_1} = \frac{R_2}{S_2} \end{cases} \tag{3.1}$$

1) Montrons que

$$\frac{P_1}{Q_1} + \frac{R_1}{S_1} = \frac{P_2}{Q_2} + \frac{R_2}{S_2} \Longleftrightarrow (P_1S_1 + Q_1R_1)\, Q_2S_2 = (P_2S_2 + Q_2R_2)\, Q_1S_1$$

D'après (3.1), on a $P_1Q_2 = Q_1P_2$ et $R_1S_2 = S_1R_2$, alors

$$(P_1S_1 + Q_1R_1)\, Q_2S_2 = P_1Q_2S_1S_2 + Q_1Q_2R_1S_2 = Q_1P_2S_1S_2 + Q_1Q_2S_1R_2 = Q_1S_1\,(P_2S_2 + Q_2R_2)$$

$$\Longrightarrow \frac{P_1}{Q_1} + \frac{R_1}{S_1} = \frac{P_2}{Q_2} + \frac{R_2}{S_2}$$

2) Montrons que

$$\frac{P_1}{Q_1} \times \frac{R_1}{S_1} = \frac{P_2}{Q_2} \times \frac{R_2}{S_2} \Longleftrightarrow P_1R_1Q_2S_2 = Q_1S_1P_2R_2$$

On a

$$P_1R_1Q_2S_2 = P_1Q_2R_1S_2 = Q_1P_2S_1R_2$$

$$\Longrightarrow P_1R_1Q_2S_2 = Q_1S_1P_2R_2$$

3) Montrons que

$$\lambda \times \frac{P_1}{Q_1} = \lambda \times \frac{P_2}{Q_2}$$

D'après (3.1), on trouve

$$\lambda \times \frac{P_1}{Q_1} = \frac{\lambda P_1}{Q_1} = \lambda \times \frac{P_2}{Q_2}$$

■

**Théorème 3.1.6** $(K(X), +, .)$ *est un corps commutatif, appelé corps des fractions rationnelles.*

**Preuve.** On montre que $(K(X), +, .)$ est un corps commutatif selon les étapes suivantes :

1) Pour l'addition :

*a*) Elle est commutative et associative. En effet :

Soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3} \in K(X)$, alors

$$\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1Q_2 + Q_1P_2}{Q_1Q_2} = \frac{Q_1P_2 + P_1Q_2}{Q_1Q_2} = \frac{P_2Q_1 + Q_2P_1}{Q_2Q_1} = \frac{P_2}{Q_2} + \frac{P_1}{Q_1}$$

Donc la loi + est commutative, car $(K[X], +, .)$ est un anneau commutatif.
D'autre part, on a

$$\left(\frac{P_1}{Q_1}+\frac{P_2}{Q_2}\right)+\frac{P_3}{Q_3}=\frac{P_1Q_2+Q_1P_2}{Q_1Q_2}+\frac{P_3}{Q_3}=\frac{P_1Q_2Q_3+Q_1P_2Q_3+Q_1Q_2P_3}{Q_1Q_2Q_3} \tag{3.2}$$

et

$$\frac{P_1}{Q_1}+\left(\frac{P_2}{Q_2}+\frac{P_3}{Q_3}\right)=\frac{P_1}{Q_1}+\frac{P_2Q_3+Q_2P_3}{Q_2Q_3}=\frac{P_1Q_2Q_3+Q_1P_2Q_3+Q_1Q_2P_3}{Q_1Q_2Q_3} \tag{3.3}$$

de (3.2) et (3.3), on conclut que la loi + est associative.
*b*) Elle admet un élément neutre $F=0=0_{K(X)}=\frac{0}{B}$, appelée fraction nulle. En effet
On pose $F=\frac{A}{B}$, alors

$$\begin{aligned}
\forall F_1 \quad &= \quad \frac{P}{Q}\in K(X): F_1+F=F_1 \Longrightarrow \frac{P}{Q}+\frac{A}{B}=\frac{P}{Q}\\
&\Longrightarrow \quad \frac{PB+QA}{QB}=\frac{P}{Q}\\
&\Longrightarrow \quad PBQ+Q^2A=PQB, Q\neq 0, B\neq 0\\
&\Longrightarrow \quad QA=0\\
&\Longrightarrow \quad A=0
\end{aligned}$$

Donc $F=\frac{0}{B}=0=0_{K(X)}$.
*c*) Toute fraction $F=\frac{P}{Q}\in K(X)$ admet un opposé (un symétrique) $F'=-F=\frac{-P}{Q}\in K(X)$. Car

$$\forall \frac{P}{Q}\in K(X): \frac{P}{Q}+\left(\frac{-P}{Q}\right)=\frac{PQ-PQ}{Q^2}=0=0_{K(X)}$$

Alors $(K(X),+)$ est un groupe commutatif.
2) Pour le produit :
*a*) La loi $\times$ est commutative et associative. En effet :
Soient $\frac{P_1}{Q_1},\frac{P_2}{Q_2},\frac{P_3}{Q_3}\in K(X)$, alors

$$\frac{P_1}{Q_1}\times\frac{P_2}{Q_2}=\frac{P_1P_2}{Q_1Q_2}=\frac{P_2P_1}{Q_2Q_1}\frac{P_2}{Q_2}\times\frac{P_1}{Q_1}$$

D'autre part, on a

$$\begin{aligned}
\left(\frac{P_1}{Q_1}\times\frac{P_2}{Q_2}\right)\times\frac{P_3}{Q_3} \quad &= \quad \left(\frac{P_1P_2}{Q_1Q_2}\right)\times\frac{P_3}{Q_3}=\frac{(P_1P_2)\,P_3}{(Q_1Q_2)\,Q_3}=\frac{P_1\,(P_2P_3)}{Q_1\,(Q_2Q_3)}=\frac{P_1}{Q_1}\times\left(\frac{P_2P_3}{Q_2Q_3}\right)=\\
&= \quad \frac{P_1}{Q_1}\times\left(\frac{P_2}{Q_2}\times\frac{P_3}{Q_3}\right)
\end{aligned}$$

*b*) La loi $\times$ admet un élément neutre qui est la fraction $F = \frac{P}{P} = 1 = 1_{K(X)}$, appelée fraction unité. En effet :
Posons $F = \frac{A}{B}$, alors

$$\begin{aligned}
\forall F_1 \quad &= \quad \frac{P}{Q} \in K(X) : F_1 \times F = F_1 \Longrightarrow \frac{P}{Q} \times \frac{A}{B} = \frac{P}{Q} \\
&\Longrightarrow \quad \frac{PA}{QB} = \frac{P}{Q} \\
&\Longrightarrow \quad PAQ = PQB, Q \neq 0, B \neq 0 \\
&\Longrightarrow \quad PA = PB \\
&\Longrightarrow \quad P\left(A - B\right) = 0, \forall P \in K\left[X\right] \\
&\Longrightarrow \quad A - B = 0 \\
&\Longrightarrow \quad A = B
\end{aligned}$$

On obtient $F = \frac{A}{A} = 1$.
*c*) Toute fraction non nulle $F = \frac{P}{Q} \in K\left(X\right) - \{0\}$, (i.e. $P \neq 0$) admet un inverse $F^{-1}$, et $F^{-1} = \left(\frac{P}{Q}\right)^{-1} = \frac{Q}{P} \in K\left(X\right) - \{0\}$. Car

$$\forall F = \frac{P}{Q} \in K(X) - \{0\} : F \times F^{-1} = \frac{P}{Q} \times \left(\frac{Q}{P}\right) = \frac{PQ}{QP} = 1$$

3) La loi $\times$ est distributive sur l'addition $+$. En effet :
Soient $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3} \in K(X)$, alors

$$\frac{P_1}{Q_1} \times \left(\frac{P_2}{Q_2} + \frac{P_3}{Q_3}\right) = \frac{P_1}{Q_1} \times \left(\frac{P_2Q_3 + Q_2P_3}{Q_2Q_3}\right) = \frac{P_1P_2Q_3 + P_1Q_2P_3}{Q_1Q_2Q_3} \tag{3.4}$$

D'autre part, on a

$$\left(\frac{P_1}{Q_1} \times \frac{P_2}{Q_2}\right) + \left(\frac{P_1}{Q_1} \times \frac{P_3}{Q_3}\right) = \frac{P_1P_2}{Q_1Q_2} + \frac{P_1P_3}{Q_1Q_3} = \frac{P_1P_2Q_3 + P_1Q_2P_3}{Q_1Q_2Q_3} \tag{3.5}$$

de (3.4) et (3.5), on obtient l'ègalité. ■

**Proposition 3.1.7** $(K(X), +, \times, \cdot)$ *est une* $K-$*algèbre associative, commutative et unitaire.*

**Preuve.** On montre les axiomes suivants :
1) $(K(X), +, \cdot)$ est un espace vectoriel sur $K$.
2) $\times$ est distributive sur $+$.

3) $\forall \lambda \in K, \forall F_1, F_2 \in K(X) : \lambda \cdot (F_1 \times F_2) = (\lambda \cdot F_1) \times F_2 = F_1 \times (\lambda \cdot F_2)$

4) $\times$ est commutative, associative, et admet un neutre.

Alors

1)

*a*) D'après le théorème (3.1.6), on a $(K(X), +)$ est un groupe commutatif.

*b*) Soient $\lambda \in K, F_1 = \frac{P_1}{Q_1}, F_2 = \frac{P_2}{Q_2} \in K(X)$, alors

$$\lambda \cdot (F_1 + F_2) = \lambda \cdot \left( \frac{P_1}{Q_1} + \frac{P_2}{Q_2} \right) = \lambda \cdot \left( \frac{P_1 Q_2 + Q_1 P_2}{Q_1 Q_2} \right) = \frac{\lambda P_1 Q_2 + \lambda Q_1 P_2}{Q_1 Q_2} = \frac{\lambda P_1}{Q_1} + \frac{\lambda P_2}{Q_2} = \lambda \cdot F_1 + \lambda \cdot F_2$$

*c*) Soient $\lambda_1, \lambda_2 \in K, F_1 = \frac{P_1}{Q_1} \in K(X)$, alors

$$(\lambda_1 + \lambda_2) \cdot F_1 = (\lambda_1 + \lambda_2) \cdot \frac{P_1}{Q_1} = \frac{(\lambda_1 + \lambda_2) P_1}{Q_1} = \frac{\lambda_1 P_1 + \lambda_2 P_2}{Q_1} = \lambda_1 \cdot \frac{P_1}{Q_1} + \lambda_2 \cdot \frac{P_1}{Q_1} = \lambda_1 \cdot F_1 + \lambda_2 \cdot F_1$$

*d*) Soient $\lambda_1, \lambda_2 \in K, F_1 = \frac{P_1}{Q_1} \in K(X)$, alors

$$(\lambda_1 \lambda_2) \cdot F_1 = (\lambda_1 \lambda_2) \cdot \frac{P_1}{Q_1} = \frac{(\lambda_1 \lambda_2) P_1}{Q_1} = \frac{\lambda_1 (\lambda_2 P_1)}{Q_1} = \lambda_1 \cdot \frac{(\lambda_2 P_1)}{Q_1} = \lambda_1 \cdot \left( \lambda_1 \cdot \frac{P_1}{Q_1} \right) = \lambda_1 \cdot (\lambda_1 \cdot F_1)$$

*e*) Soit, $F_1 = \frac{P_1}{Q_1} \in K(X)$, alors

$$1_K \cdot F_1 = 1_K \cdot \frac{1_K P_1}{Q_1} = \frac{P_1}{Q_1} = F_1$$

Donc $(K(X), +, \cdot)$ est un espace vectoriel sur $K$.

2) D'après le théorème (3.1.6), on a $\times$ est distributive sur $+$..

3) Soient $\lambda \in K, F_1 = \frac{P_1}{Q_1}, F_2 = \frac{P_2}{Q_2} \in K(X)$, alors

$$\lambda \cdot (F_1 \times F_2) = \lambda \cdot \left( \frac{P_1}{Q_1} \times \frac{P_2}{Q_2} \right) = \lambda \cdot \frac{P_1 P_2}{Q_1 Q_2} = \frac{\lambda P_1 P_2}{Q_1 Q_2} = \frac{(\lambda P_1) P_2}{Q_1 Q_2} =$$

$$\Longrightarrow \lambda \cdot (F_1 \times F_2) = \frac{(\lambda P_1)}{Q_1} \times \frac{P_2}{Q_2} = \left( \lambda \cdot \frac{P_1}{Q_1} \right) \times \frac{P_2}{Q_2} = (\lambda \cdot F_1) \times F_2 \qquad (3.6)$$

D'autre part, on a

$$\lambda \cdot (F_1 \times F_2) = \frac{\lambda P_1 P_2}{Q_1 Q_2} = \frac{P_1 (\lambda P_2)}{Q_1 Q_2} = \frac{P_1}{Q_1} \times \frac{\lambda P_2}{Q_2} = \frac{P_1}{Q_1} \times \left( \lambda \cdot \frac{P_2}{Q_2} \right) = F_1 \times (\lambda \cdot F_2) \quad (3.7)$$

De (3.6) et (3.7), on obtient

$$\lambda \cdot (F_1 \times F_2) = (\lambda \cdot F_1) \times F_2 = F_1 \times (\lambda \cdot F_2)$$

4) D'après le théorème (3.1.6), on a $\times$ est commutative, associative, et admet un neutre.
■

**Proposition 3.1.8** *(Plongement de $K[X]$ dans $K(X)$ )*
*L'application*

$$\begin{array}{rccc} f: & K[X] & \longrightarrow & K(X) \\ & P & \longmapsto & f(P) = \frac{P}{1} \end{array}$$

*est un morphisme d'algèbre injectif. De plus $f(1) = 1$.*

C'est à dire, on peut confondre ou identifier un polynôme $P$ et la fraction rationnelle (i.e : $K[X]$ à sont image par $f$, ou $K[X]$ est en bijection avec $f(K[X])) = \mathrm{Im}(f)$). Par conséquent la fraction nulle est identifiée au polynôme nul 0, et la fraction unité est identifiée au polynôme constant 1.

Ainsi $K[X]$ est considéré comme (un sous ensemble) une sous algèbre unitaire de $K(X)$, en particulier $K[X]$ est un sous anneau de corps $K(X)$, et $K[X]$ est un sous espace vectoriel de $K-$espace vectoriel $K(X)$.

**Preuve.**

1. Soient $\lambda \in K, P_1, P_2 \in K[X]$, alors :

   (a) $f(P_1 + P_2) = \frac{P_1+P_2}{1} = \frac{P_1}{1} + \frac{P_2}{1} = f(P_1) + f(P_2)$.
   (b) $f(P_1 \times P_2) = \frac{P_1 \times P_2}{1} = \frac{P_1}{1} \times \frac{P_2}{1} = f(P_1) \times f(P_2)$.
   (c) $f(\lambda \cdot P_1) = \frac{\lambda P_1}{1} = \lambda \cdot \frac{P_1}{1} = \lambda \cdot f(P_1)$
   Donc $f$ est un morphisme d'algèbre.
   (d) On a
   $$f(1) = f\left(1_{K[X]}\right) = \frac{1}{1} = 1 = 1_{K(X)}$$

2. On a

$$\begin{array}{rcl} f(P_1) & = & f(P_2) \Longrightarrow \frac{P_1}{1} = \frac{P_2}{1} \\ & \Longrightarrow & P_1 = P_2 \end{array}$$

   Donc $f$ est injective.

■

**Définition 3.1.9**
*1) On appelle degré d'une fraction rationnelle* $F = \frac{P}{Q} \in K(X) - \{0\}$ *l'entier rationnel défini par*

$$\deg(F) = \deg\left(\frac{P}{Q}\right) = \deg(P) - \deg(Q) \in \mathbb{Z}$$

*2) Si* $F = 0$ *(i.e :*$P = 0$*), alors* $\deg(F) = -\infty$.

**Remarque 3.1.10**
*1) Le degré de* $F = \frac{P}{Q} \in K(X)$ *est bien défini. Autrement dit la quantité* $\deg(P) - \deg(Q)$ *est indépendante du représentant* $(P, Q)$ *choisi pour F. En effet :*
*Supposons que* $F = \frac{P_1}{Q_1} = \frac{P_2}{Q_2}$*. Alors on a* $P_1Q_2 = P_2Q_1$.
*Ainsi*

$$\begin{aligned} \deg(P_1Q_2) &= \deg(P_2Q_1) \Longrightarrow \deg(P_1) + \deg(Q_2) = \deg(P_2) + \deg(Q_1) \\ &\Longrightarrow \deg(P_1) - \deg(Q_1) = \deg(P_2) - \deg(Q_2) \end{aligned}$$

*2) On remarque que l'application* $\deg : K(X) \longrightarrow \mathbb{Z} \cup \{-\infty\}$ *prolonge l'application* $\deg : K[X] \longrightarrow \mathbb{N} \cup \{-\infty\}$ *car*

$$\forall P \in K[X] : \deg\left(\frac{P}{1}\right) = \deg(P) - \deg(1) = \deg(P)$$

**Proposition 3.1.11** *Les degrés des fractions rationnelles vérifient les mêmes propriétés que ceux des polynômes :*
*1)* $\forall F_1, F_2 \in K(X) : \deg(F_1 \times F_2) \leq \deg(F_1) + \deg(F_2)$.
*2)* $\forall F_1, F_2 \in K(X) : \deg(F_1 + F_2) \leq \max\{\deg(F_1), \deg(F_2)\}$.
*3)* $\forall F_1 \in K(X), \forall \lambda \in K^* : \deg(\lambda F_1) = \deg(F_1)$.

**Preuve.** Posons $F_1 = \frac{P_1}{Q_1}, F_2 = \frac{P_2}{Q_2} \in K(X), \lambda \in K$, alors
1)

$$\deg(F_1 \times F_2) = \deg\left(\frac{P_1P_2}{Q_1Q_2}\right) = \deg(P_1P_2) - \deg(Q_1Q_2)$$

$$\begin{aligned} &\Longrightarrow \deg(F_1 \times F_2) = \deg(P_1) + \deg(P_2) - \deg(Q_1) - \deg(Q_2) = \\ &= (\deg(P_1) - \deg(Q_1)) + (\deg(P_2) - \deg(Q_2)) \\ &\Longrightarrow \deg(F_1 \times F_2) = \deg(F_1) + \deg(F_2) \end{aligned}$$

2) On a $F_1 + F_2 = \frac{P_1Q_2+Q_1P_2}{Q_1Q_2}$, alors

$$\deg(F_1 + F_2) = \deg(P_1Q_2 + Q_1P_2) - \deg(Q_1Q_2) =$$

Or

$$\deg(P_1Q_2 + Q_1P_2) \leq \max\{\deg(P_1Q_2), \deg(Q_1P_2)\}$$

On obtient

$$\begin{cases} \deg(F_1 + F_2) \leq \deg(P_1Q_2) - \deg(Q_1Q_2) \\ ou \\ \deg(F_1 + F_2) \leq \deg(Q_1P_2) - \deg(Q_1Q_2) \end{cases} \Longrightarrow \begin{cases} \deg(F_1 + F_2) \leq \deg(P_1) - \deg(Q_1) = \deg(F_1) \\ ou \\ \deg(F_1 + F_2) \leq \deg(P_2) - \deg(Q_2) = \deg(F_2) \end{cases}$$

$$\Longrightarrow \deg(F_1 + F_2) \leq \max\{\deg(F_1), \deg(F_2)\}$$

3) On a

$$\deg(\lambda F_1) = \deg\left(\lambda \cdot \frac{P_1}{Q_1}\right) = \deg\left(\frac{\lambda P_1}{Q_1}\right) = \deg(\lambda P_1) - \deg(Q_1) = \deg(P_1) - \deg(Q_1) = \deg(F_1)$$

■

**Remarque 3.1.12**

*1) Une fraction rationnelle constante non nulle a un degré nul, mais la réciproque est fausse, par exemple :*

$$F = \frac{X}{X+1}$$

*2) Si* $\deg(F_1) \neq \deg(F_2)$*, alors* $\deg(F_1 + F_2) = \max\{\deg(F_1), \deg(F_2)\}$.
*3)Une fraction* $F$ *est nulle ssi son degré vaut* $-\infty$.

**Définition 3.1.13** *Soit* $F = \frac{P}{Q} \in K(X)$*, on appelle fraction dérivée de* $F$ *la fraction notée* $F'$ *(ou* $\frac{dF}{dX}$*) définie par* $F' = \frac{P'Q-PQ'}{Q^2}$.
*Le résultat ne dépend pas du représentant de* $F$ *choisi. On définit également les dérivées successives de* $F$ *en posant* $F^{(0)} = F$ *et pour tout* $n \in \mathbb{N}$, $F^{(n+1)} = \left(F^{(n)}\right)'$

**Remarque 3.1.14**

*1) Contrairement aux polynômes le degré de* $F'$ *n'est pas toujours égal à* $\deg(F) - 1$*, par exemple* $F = \frac{X}{X+1}$*, on a* $\deg(F) = 0$ *et* $F' = \frac{1}{(X+1)^2}$ *donc* $\deg(F') = -2$*. Par contre on a toujour* $\deg(F') \leq \deg(F) - 1$.

*2) L'application*

$$\begin{array}{rccc} f_1: & K(X) & \longrightarrow & K(X) \\ & F & \longmapsto & F' \end{array}$$

*prolonge l'application*

$$\begin{array}{rccc} f_2: & K[X] & \longrightarrow & K[X] \\ & P & \longmapsto & P' \end{array}$$

*car*

$$\forall P \in K[X]: \left(\frac{P}{1}\right)' = \frac{P'.1 - 0.P}{1^2} = P'$$

*3) Si $F_1, F_2 \in K(X), \lambda \in K$, alors*

$$\begin{array}{rcl} (\lambda F_1)' & = & \lambda F_1', (F_1 + F_2)' = F_1' + F_2', (F_1 \times F_2)' = F_1' \times F_2 + F_1 \times F_2' \\ \left(\frac{F_1}{F_2}\right)' & = & \frac{F_1' \times F_2 - F_1 \times F_2'}{F_2^2}, \text{ si } F_2 \neq 0_{K(X)} \end{array}$$

**Définition 3.1.15** *On dit que la fraction $F = \frac{P}{Q}$ est sous forme irréductible ou simplifiée si le pgcd de $P$ et de $Q$ est égal à 1. On dit aussi que $\frac{P}{Q}$ est un représentant irréductible de $F$.*

**Notation 3.1.16** *On note par $I_{K(X)}$ l'ensemble des éléments irréductibles de $K(X)$.*

**Exemple 3.1.17** *Soit $F = \frac{X^3-1}{X^2-1}$, alors $\frac{X^2+X+1}{X+1}$ est une forme (ou un représentant) irréductible de $F$, c'est à dire $F = \frac{X^2+X+1}{X+1}$.*

**Proposition 3.1.18** *Toute fraction rationnelle $F$ possède un unique représentant irréductible de la forme $F = \frac{P}{Q}$ avec $pgcd(P, Q) = 1$ et $Q$ unitaire.*

**Preuve.**

**Existence :**

Soit $F = \frac{P_1}{Q_1}$ une écriture de $F$, montrons que $F$ admet un représentant $\frac{P}{Q}$ avec $pgcd(P, Q) = 1$. Supposons que $D = pgcd(P_1, Q_1)$, alors

$$\exists P, Q \in K[X]: \begin{cases} pgcd(P, Q) = 1 \\ P_1 = DP \\ Q_1 = DQ \end{cases}$$

*Où* $(P, Q)\Re(P_1, Q_1)$.

D'autre part, en mettant en facteur dans $P$ et $Q$ le coefficient du terme de plus haut degré de $Q$ et en simplifiant la fraction par ce coefficient, on peut supposer $Q$ unitaire.

**Unicité :** Supposons que $F = \frac{P_1}{Q_1} = \frac{P_2}{Q_2}$ avec $Q_1, Q_2$ unitaires et

$$pgcd(P_1, Q_1) = pgcd(P_2, Q_2) = 1$$

On a alors

$$\begin{cases} P_1 Q_2 = P_2 Q_1 \\ Q_2 \mid (P_2 Q_1) \end{cases}$$

Or $pgcd(P_2, Q_2) = 1$, alors d'après le théorème de Gauss, on a $Q_2 \mid Q_1$. De même, on a

$$\begin{cases} Q_1 \mid P_1 Q_2 \\ pgcd(P_1, Q_1) = 1 \end{cases} \Longrightarrow Q_1 \mid Q_2$$

Or $Q_1, Q_2$ sont unitaires, alors $Q_1 = Q_2$, en déduit que $P_1 = P_2$. ■

## 3.2 Décomposition en éléments simples d'une fraction rationnelle

L'objectif principal de cette section est le théorème de décomposition en éléments simples, utilisé notamment pour le calcul des primitives de fractions rationnelles.

**Définition 3.2.1** *(Pôles et racines)*
*Soit $F$ une fraction non nulle de $K(X)$, et soit $\frac{P}{Q}$ un représentant irréductible de $F$.*
*1) On dit que $\alpha \in K$ est une racine de $F$ de multiplicité $m \in \mathbb{N}^*$ lorsque $\alpha$ est une racine du numérateur $P$ de multiplicité $m$.*
*2) On dit que $\alpha \in K$ est un pôle de $F$ de multiplicité $m \in \mathbb{N}^*$ lorsque $\alpha$ est une racine du dénominateur $Q$ de multiplicité $m$.*

**Remarque 3.2.2**
*1) Puisque $\frac{P}{Q}$ est irréductible, on voit qu'un scalaire $\alpha$ ne peut pas être à la fois pôle et racine de $F$, sinon $P$ et $Q$ seraient divisibles par $(X - a)$.*
*2) $\alpha$ est un pôle de $F$ de multiplicité $m \in \mathbb{N}^*$ équivaut à dire que $\alpha$ est racine de multiplicité $m$ de la fraction $\frac{1}{F}$.*

**Exemple 3.2.3** *Prenons*

$$F = \frac{(X+1)^2 (X-i)}{(X^2+1)^3} = \frac{(X+1)^2}{(X-i)^2 (X+i)^3}$$

*On a* $p\gcd\left((X+1)^2 \wedge (X-i)^2 (X+i)^3\right) = 1$, *alors* $F$ *possède une racine réelle* $-1$ *d'ordre* 2, *deux pôles complexes :* $i$ *d'ordre* 2 *et* $(-i)$ *d'ordre* 3.

**Définition 3.2.4** *Soit* $F$ *une fraction rationnelle de forme irréductible* $\frac{P}{Q}$. *Notons* $\tilde{P}$ *et* $\tilde{Q}$ *les fonctions polynomiales associées à* $P$ *et* $Q$. *On appelle fonction rationnelle associée à* $F$ *la fonction notée* $\tilde{F} : K \longrightarrow K$ *définie par* $\tilde{F}(x) = \frac{\tilde{P}(x)}{\tilde{Q}(x)}$ *pour tout* $x \in K$ *tels que* $\tilde{Q}(x) \neq 0$, . *Autrement dit*

$$\begin{array}{rccc} \tilde{F}: & K - \{\text{pôle de } F\} & \longrightarrow & K \\ & x & \longmapsto & \tilde{F}(x) = \frac{\tilde{P}(x)}{\tilde{Q}(x)} \end{array}$$

**Exemple 3.2.5** *Soit* $F = \frac{X^3-2X^2+X}{X^2+X} \in \mathbb{R}(X)$, *alors la forme irréductible est* $F = \frac{X^2-2X+1}{X+1}$, *donc*

$$\begin{array}{rccc} \tilde{F}: & \mathbb{R} - \{-1\} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \tilde{F}(x) = \frac{(x-1)^2}{x+1} \end{array}$$

**Lemme 3.2.6** *(Partie entière)*
*Soit* $F = \frac{P}{Q} \in K(X)$, *alors il existe un couple unique* $(E, R)$ *de* $(K[X])^2$ *tels que*

$$\begin{cases} F = E + \frac{R}{Q} \\ \deg(R) < \deg(Q) \end{cases}$$

*De plus, si* $pgcd(P, Q) = 1$, *alors* $pgcd(R, Q) = 1$.
*Le polynôme* $E$ *est appelé la partie entière de* $F$, *la fraction rationnelle* $\frac{R}{Q}$ *est appelée la partie fractionnelle de* $F$.

**Preuve.**

1) **Existence :**

Par division euclidienne de $P$ par $Q$, il existe $(E, R)$ de $(K[X])^2$ tels que :

$$P = EQ + R, \deg(R) < \deg(Q)$$

$$\Longrightarrow \begin{cases} F = \frac{P}{Q} = E + \frac{R}{Q} \\ \deg(R) < \deg(Q) \end{cases}$$

D'autre part, d'après l'algorithme d'Euclide, si $pgcd(P, Q) = 1$, alors $pgcd(R, Q) = 1$.

2) **Unicité :**

Soient $(E_1, R_1), (E_2, R_2)$ de $(K[X])^2$ tels que

$$\begin{cases} F = E_1 + \frac{R_1}{Q} \\ \deg(R_1) < \deg(Q) \end{cases}, \begin{cases} F = E_2 + \frac{R_2}{Q} \\ \deg(R_2) < \deg(Q) \end{cases}$$

Alors

$$\begin{array}{rcl} E_1 - E_2 & = & \dfrac{R_2}{Q} - \dfrac{R_1}{Q} = \dfrac{R_2 - R_1}{Q} \Longrightarrow \deg(E_1 - E_2) = \deg(R_2 - R_1) - \deg(Q) < 0 \\ & \Longrightarrow & E_1 - E_2 = 0 \end{array}$$

Donc $E_1 = E_2$ et $R_1 = R_2$. ■

**Remarque 3.2.7** *On peut écrire le lemme* (3.2.6) *sous la forme : Si* $F \in K(X)$*, alors il existe un couple unique* $(E, G)$ *de* $K[X] \times K(X)$ *tels que*

$$\begin{cases} F = E + G \\ \deg(G) < 0 \end{cases}$$

**Exemple 3.2.8** *Soit* $F = \frac{X^2+X}{X+2} \in \mathbb{R}(X)$*, alors à l'aide de la division euclidienne on obtient*

$$F = X - 1 + \frac{2}{X+2}$$

**Proposition 3.2.9** *Notons* $\mathcal{F}^- = \{G \in K(X) : \deg(G) < 0\}$*, alors*
*1)* $\mathcal{F}^-$ *est un sous espace vectoriel de* $K(X)$*.*
*2 )* $K(X) = K[X] \oplus \mathcal{F}^-$*.*

**Preuve.**
1) i) Il esl clair que $0_{K(X)} \in \mathcal{F}^-$, car $\deg\left(0_{K(X)}\right) = -\infty < 0$.
ii) Soient $\alpha, \beta \in K, F, G \in \mathcal{F}^-$, alors

$$\begin{array}{rcl} \deg(\alpha F + \beta G) & \leq & \max\{\deg(\alpha F), \deg(\beta G)\} \\ & \leq & \max\{\deg(F), \deg(G)\} < 0 \end{array}$$

Alors $\alpha F + \beta G \in \mathcal{F}^-$.
2)i) On a

$$K[X] \cap \mathcal{F}^- = \left\{F \in K(X) : F \in K[X] \wedge F \in \mathcal{F}^-\right\} = \{F \in K(X) : F \in K[X] \wedge \deg(F) < 0\} = \left\{0_{K(X}\right.$$

ii) Or $K[X] + \mathcal{F}^-$ est un sous espace vectoriel de $K(X)$, alors $K[X] + \mathcal{F}^- \subset K(X)$.
D'autre part, d'après le lemme (3.2.6), on a

$$\begin{array}{rcl} \forall F & \in & K(X), \exists P \in K[X], \exists G \in \mathcal{F}^- : F = E + G \\ & \Longrightarrow & F \in K[X] + \mathcal{F}^- \\ & \Longrightarrow & K(X) \subset K[X] + \mathcal{F}^- \end{array}$$

■

**Définition 3.2.10** *On appelle élément simple de $K(X)$ :*
*1) Les monômes de $K[X]$.*
*2) Les éléments de $K(X)$ de la forme $\frac{P}{Q^n}$ tels que*

$$\begin{cases} Q \in K[X], \deg(Q) \geq 1, \ Q \text{ est irréductible} \\ n \geq 1 \\ P \in K[X] - \{0\}, \deg(P) < \deg(Q) \end{cases}$$

**Remarque 3.2.11**
*1) Éléments simples dans $\mathbb{C}(X)$ :*
*On sait que $I_{\mathbb{C}[X]} = \{X - a, a \in \mathbb{C}\}$, donc les éléments simples de $\mathbb{C}(X)$ sont les fractions :*

$$\frac{b}{(X-a)^n}, a, b \in \mathbb{R}, n \geq 1$$

*2) Éléments simples dans $\mathbb{R}(X)$ :*
*On sait que $I_{\mathbb{R}[X]} = \{X - a, a \in \mathbb{R}\} \cup \{X^2 + pX + q : p, q \in \mathbb{R}, \triangle = p^2 - 4q < 0\}$, donc les éléments simples de $\mathbb{R}(X)$ sont de deux types :*
*a) Eléments simples de première espèce :*

$$\frac{b}{(X-a)^n}, a, b \in \mathbb{C}, n \geq 1$$

*b) Eléments simples de seconde (deuxième) espèce :*

$$\frac{aX+b}{(X^2+pX+q)^n}, a, b, p, q \in \mathbb{R}, p^2 - 4q < 0, n \geq 1$$

**Exemple 3.2.12** *Dans $\mathbb{C}(X)$, on a $F_1 = \frac{3}{(X-i)^3}$, dans $\mathbb{R}(X)$, on a $F_2 = \frac{3X-2}{(X^2+X+1)^4}$ (seconde espèce).*

**Première Décomposition**

**Lemme 3.2.13** *Soient $P \in K[X], n \in \mathbb{N}^*, Q_1, Q_2, ..., Q_n \in K[X] - \{0\}$ tels que $Q_1, Q_2, ..., Q_n$ soient premiers entre eux deux à deux. Alors il existe $P_1, P_2, ..., P_n \in K[X]$ tels que*

$$\frac{P}{Q_1 Q_2 ... Q_n} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} + ... + \frac{P_n}{Q_n}$$

**Preuve.** Montrons par récurrence sur $n$.
La propriété est triviale pour $n = 1$.

Cas $n = 2$ :
Puisque $pgcd\,(Q_1, Q_2) = 1$, alors d'après le théorème de Bézout, il existe $U_1, U_2 \in K\,[X]$ tel que $U_1Q_1 + U_2Q_2 = 1$. Donc

$$\frac{P}{Q_1Q_2} = \frac{P\,(U_1Q_1 + U_2Q_2)}{Q_1Q_2} = \frac{PU_2}{Q_1} + \frac{PU_1}{Q_2} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}$$

Supposons la propriété est vraie pour $n \in \mathbb{N}^*$, et soient $Q_1, Q_2, ..., Q_n, Q_{n+1} \in K\,[X] - \{0\}$ premiers entre eux deux à deux. Alors

$$pgcd\,((Q_1Q_2...Q_n)\,, Q_{n+1}) = 1$$

D'après l'étude du cas $n = 2$, il existe $A_1, P_{n+1} \in K\,[X]$ tels que

$$\frac{P}{Q_1Q_2...Q_nQ_{n+1}} = \frac{A_1}{Q_1Q_2...Q_n} + \frac{P_{n+1}}{Q_{n+1}}$$

Puis, d'après l'hypothèse de récurrence, il existe $P_1, P_2, ..., P_n \in K\,[X]$ tels que

$$\frac{A_1}{Q_1Q_2...Q_n} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} + ... + \frac{P_n}{Q_n}$$

$$\Longrightarrow \frac{P}{Q_1Q_2...Q_nQ_{n+1}} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} + ... + \frac{P_n}{Q_n} + \frac{P_{n+1}}{Q_{n+1}}$$

■

Nous allons maintenant combiner les lemmes (3.2.6) et (3.2.13) pour obtenir le résultat suivant :

**Lemme 3.2.14** *Soient $P \in K\,[X]\,, n \in \mathbb{N}^*, Q_1, Q_2, ..., Q_n \in K\,[X] - \{0\}$ tels que $Q_1, Q_2, ..., Q_n$ soient premiers entre eux deux à deux. Alors il existe $(E, R_1, R_2, ..., R_n) \in (K\,[X])^{n+1}$ unique tels que*

$$\begin{cases} \frac{P}{Q_1Q_2...Q_n} = E + \frac{R_1}{Q_1} + \frac{R_2}{Q_2} + ... + \frac{R_n}{Q_n} \\ \forall i = \overline{1, n} : \deg\,(R_i) < \deg\,(Q_i) \end{cases}$$

*De plus $E$ est la partie entière de $\frac{P}{Q_1Q_2...Q_n}$.*

**Preuve.**

1) **Existence :**

D'après le lemme (3.2.13), il existe $P_1, P_2, ..., P_n \in K\,[X]$ tels que

$$\frac{P}{Q_1Q_2...Q_n} = \frac{P_1}{Q_1} + \frac{P_2}{Q_2} + ... + \frac{P_n}{Q_n}$$

Puis d'après le lemme (3.2.6), il existe $E_1, E_2, ..., E_n, R_1, R_2, ..., R_n \in K[X]$ tels que

$$\forall i = \overline{1,n} : \begin{cases} \frac{P_i}{Q_i} = E_i + \frac{Ri}{Q_i} \\ \deg(R_i) < \deg(Q_i) \end{cases}$$

En notant $E = E_1 + E_2 + ... + E_n$, on obtient le résulta voulu.
2) **Unicité :** Par récurrence sur $n$.
Le cas $n = 1$ est déjà vu (lemme (3.2.6)).
Cas $n = 2$ : Soient $E, R_1, R_2, D, T_1, T_2 \in K[X]$ tels que

$$\begin{cases} \frac{P}{Q_1Q_2} = E + \frac{R_1}{Q_1} + \frac{R_2}{Q_2} \\ \frac{P}{Q_1Q_2} = D + \frac{T_1}{Q_1} + \frac{T_2}{Q_2} \\ \forall i = \overline{1,2} : \begin{cases} \deg(R_i) < \deg(Q_i) \\ \deg(T_i) < \deg(Q_i) \end{cases} \end{cases}$$

Alors

$$\begin{aligned} E + \frac{R_1}{Q_1} + \frac{R_2}{Q_2} &= D + \frac{T_1}{Q_1} + \frac{T_2}{Q_2} \Longrightarrow E + \frac{R_1}{Q_1} - \frac{T_1}{Q_1} = D + \frac{T_2}{Q_2} - \frac{R_2}{Q_2} \\ &\Longrightarrow Q_2(R_1 - T_1) = Q_1Q_2(D - E) + Q_1(T_2 - R_2) \\ &\Longrightarrow Q_2(R_1 - T_1) = Q_1(Q_2(D - E) + (T_2 - R_2)) \\ &\Longrightarrow \begin{cases} Q_1 \mid Q_2(R_1 - T_1) \\ pgcd(Q_1, Q_2) = 1 \end{cases} \\ &\Longrightarrow Q_1 \mid (R_1 - T_1) \end{aligned}$$

Mais d'autre part $\deg(R_1 - T_1) < \deg(Q_1)$. On déduit

$$R_1 - T_1 = 0 \Longrightarrow R_1 = T_1$$

De même $R_2 = T_2$ et enfin $E = D$.
Supposons la propriété vraie pour $n \in \mathbb{N}^*$.
Soient $E, R_1, R_2, ..., R_{n+1}, D, T_1, T_2, ..., T_{n+1} \in K[X]$ tels que

$$\begin{cases} \frac{P}{Q_1Q_2...Q_{n+1}} = E + \sum_{i=1}^{n+1} \frac{R_i}{Q_i} = D + \sum_{i=1}^{n+1} \frac{T_i}{Q_i} \\ \forall i = \overline{1,n+1} : \begin{cases} \deg(R_i) < \deg(Q_i) \\ \deg(T_i) < \deg(Q_i) \end{cases} \end{cases}$$

En notant

$$Q = Q_1Q_2...Q_n, B = \sum_{i=1}^{n}\left(R_i\left(\prod_{\substack{j=i\\ j\neq i}}^{n} Q_j\right)\right), C = \sum_{i=1}^{n}\left(T_i\left(\prod_{\substack{j=i\\ j\neq i}}^{n} Q_j\right)\right)$$

On a

$$\begin{cases} pgcd\left(Q, Q_{n+1}\right) = 1 \\ \frac{P}{QQ_{n+1}} = E + \frac{B}{Q} + \frac{R_{n+1}}{Q_{n+1}} = D + \frac{C}{Q} + \frac{T_{n+1}}{Q_{n+1}} \end{cases}$$

D'après l'étude du cas $n = 2$, on déduit

$$D = E, C = B, T_{n+1} = R_{n+1}$$

Ainsi

$$\begin{cases} \sum_{i=1}^{n} \frac{R_i}{Q_i} = \sum_{i=1}^{n} \frac{T_i}{Q_i} \\ \forall i = \overline{1,n} : \begin{cases} \deg\left(R_i\right) < \deg\left(Q_i\right) \\ \deg\left(T_i\right) < \deg\left(Q_i\right) \end{cases} \end{cases}$$

Par l'hypothèse de récurrence $\forall i = \overline{1,n} : R_i = T_i$.
3) Comme

$$\deg\left(\frac{R_1}{Q_1} + \frac{R_2}{Q_2} + ... + \frac{R_n}{Q_n}\right) \leq \max\left\{\deg\left(\frac{R_i}{Q_i}\right), i = \overline{1,n}\right\} < 0$$

D'après le lemme (3.2.6), $E$ est la partie entière de $\frac{P}{Q_1Q_2...Q_n}$. ■

**Deuxième Décomposition**

**Lemme 3.2.15** *Soient $n \in \mathbb{N}^*, P \in K\left[X\right], Q \in K\left[X\right]$ tel que $\deg\left(Q\right) \geq 1$. Alors il existe $(E, P_1, P_2, ..., P_n) \in \left(K\left[X\right]\right)^{n+1}$ unique tels que*

$$\begin{cases} F = \frac{P}{Q^n} = E + \frac{P_1}{Q} + \frac{P_2}{Q^2} + ... + \frac{P_n}{Q^n} \\ \forall i = \overline{1,n} : \deg\left(P_i\right) < \deg\left(Q\right) \end{cases}$$

*De plus $E$ est la partie entière de $\frac{P}{Q^n}$.*

**Preuve.**

1) **Existence :**

On a

$$\begin{aligned} F &= \frac{P}{Q^n} = \frac{D_1 Q + P_n}{Q^n} \text{ (division euclidienne de } P \text{ par } Q) \\ \Longrightarrow\ & F = \frac{P}{Q^n} = \frac{D_1}{Q^{n-1}} + \frac{P_n}{Q^n},\ \deg(P_n) < \deg(Q) \end{aligned}$$

La division euclidienne de $D_1$ par $Q$ donne ensuite, de la même manière :

$$F = \frac{D_2}{Q^{n-2}} + \frac{P_{n-1}}{Q^{n-1}} + \frac{P_n}{Q^n}$$

Et ainsi de suite

$$F = \frac{D_{n-1}}{Q} + \frac{P_2}{Q^2} + ... + \frac{P_{n-1}}{Q^{n-1}} + \frac{P_n}{Q^n}$$

Enfin, la division euclidienne de $D_{n-1}$ par $Q$ donne

$$F = E + \frac{P_1}{Q} + \frac{P_2}{Q^2} + ... + \frac{P_n}{Q^n}$$

2) **Unicité :** Par récurrence sur $n$.
Le cas $n = 1$ a été vu (lemme (3.2.6)).
Supposons la propriété vraie pour $n \in \mathbb{N}^*$.
Soient $E_1, P_1, P_2, ..., P_{n+1}, E_2, D_1, D_2, ..., D_{n+1} \in K[X]$ tels que

$$\begin{cases} \frac{P}{Q^{n+1}} = E_1 + \frac{P_1}{Q} + \frac{P_2}{Q^2} + ... + \frac{P_n}{Q^n} + \frac{P_{n+1}}{Q^{n+1}} = E_2 + \frac{D_1}{Q} + \frac{D_2}{Q^2} + ... + \frac{D_n}{Q^n} + \frac{D_{n+1}}{Q^{n+1}} \\ \forall i = \overline{1, n+1} : \begin{cases} \deg(P_i) < \deg(Q) \\ \deg(D_i) < \deg(Q) \end{cases} \end{cases}$$

En multipliant par $Q^n$, on obtient

$$\begin{aligned} \frac{P}{Q} &= \left(E_1 Q^n + P_1 Q^{n-1} + P_2 Q^{n-2} + ... + P_{n-1} Q + P_n\right) + \frac{P_{n+1}}{Q} = \\ &= \left(E_2 Q^n + D_1 Q^{n-1} + D_2 Q^{n-2} + ... + D_{n-1} Q + D_n\right) + \frac{D_{n+1}}{Q} \end{aligned}$$

D'après le lemme (3.2.6), on déduit que $D_{n+1} = P_{n+1}$, puis en appliquant l'hypothèse de récurrence, on trouve

$$D_n = P_n, D_{n-1} = P_{n-1}, ..., D_1 = P_1, E_1 = E_2$$

On a

$$\deg\left(\frac{P_1}{Q} + \frac{P_2}{Q^2} + ... + \frac{P_n}{Q^n}\right) \leq \max\left\{\deg\left(\frac{P_i}{Q^i}\right), i = \overline{1, n}\right\} < 0$$

D'après le lemme (3.2.6), $E$ est la partie entière de $\frac{P}{Q^n}$. ■

**Définition 3.2.16** *Décomposer une fraction rationnelle $F$ non nulle, c'est l'écrire comme somme de sa partie entière et d'éléments simples.*

**Exemple 3.2.17** *$F = \frac{X^3}{X^2+1}$ sa partie entière est $X$, et on a $F = X + \frac{X}{X^2+1}$, c'est la décomposition de $F$ en éléments simples dans $\mathbb{R}(X)$, mais dans $\mathbb{C}(X)$, on a $F = X + \frac{\frac{-1}{2}}{X-i} + \frac{\frac{-1}{2}}{X+i}$*

Des lemmes précédents, on déduit le théorème de décomposition en éléments simples suivant :

**Théorème 3.2.18** *(Existence et unicité de la décomposition en éléments simples d'une fraction rationnelle)*
*Soit $F = \frac{P}{Q_1^{k_1} Q_2^{k_2} ... Q_n^{k_n}}$ où $n \in \mathbb{N}^*, k_1, k_2, ..., k_n \in \mathbb{N}^*$, $Q_1, Q_2, ..., Q_n \in K[X] - \{0\}$ sont irréductibles et premiers entre eux deux à deux, et $P \in K[X]$. Alors il existe une famille unique de polynômes $E, P_{k_1,1}, P_{k_1,2}, ..., P_{k_1,k_1}, P_{k_2,1}, P_{k_2,2}, ..., P_{k_2,k_2}, ..., P_{k_n,1}, P_{k_n,2}, ..., P_{k_n,k_n}$ de $K[X]$ telle que*

$$\begin{cases} F = E + \sum_{i=1}^{n} \left( \sum_{j=1}^{k_i} \frac{P_{k_i,j}}{Q_i^j} \right) \\ \\ \forall i \in \{1, 2, ..., n\}, \forall j \in \{1, 2, ..., k_i\} : \deg(P_{k_i,j}) < \deg(Q_i) \end{cases}$$

*Cette formule est appelée la décomposition en élément simple (en abrégé : DES) de la fraction rationnelle.*

### 3.2.1 Décomposition dans le cas complexe

Soit $F = \frac{P}{Q} \in \mathbb{C}(X)$, sous forme irréductible, soit $E$ sa partie entière et soit

$$Q = \prod_{k=1}^{r} (X - a_k)^{m_k}$$

la factorisation du dénominateur. Les complexes $a_k$ sont les pôles de $F$, et les entiers $m_k \geq 1$ sont les multiplicités respectives. D'après l'étude générale, la forme de la décomposition de $F$ sera :

$$F = E + \sum_{k=1}^{r} \left( \sum_{j=1}^{m_k} \frac{b_{j,k}}{(X - a_k)^j} \right)$$

La somme des éléments simples relatifs au pôle $a_k$ est appelée partie polaire de $F$ relative au pôle $a_k$, elle est notée $P_F(a_k)$. On a donc

$$P_F(a_k) = \sum_{j=1}^{m_k} \frac{b_{j,k}}{(X-a_k)^j}$$

**Remarque 3.2.19** *La forme de la décomposition de $F$ est :*

$$F = E + P_F(a_1) + P_F(a_2) + ... + P_F(a_r)$$

*C'est à dire : partie entière plus les parties polaires relatives aux pôles de $F$. La décomposition dans $\mathbb{C}(X)$ consiste donc à calculer des parties polaires.*

### 3.2.2 Décomposition dans le cas réel

Soit $F = \frac{P}{Q} \in \mathbb{R}(X)$ (sous forme irréductible), soit $E$ sa partie entière et soit

$$Q = \prod_{k=1}^{n} (X-a_k)^{m_k} \cdot \prod_{k=1}^{r} \left(X^2 + p_k X + q_k\right)^{l_k}$$

la factorisation de $Q$ en produit de facteurs irréductibles unitaires ($\triangle = p_k^2 - 4q_k < 0$). D'après l'étude générale, la forme de la décomposition de $F$ est :

$$F = E + \sum_{k=1}^{n} \left( \sum_{j=1}^{m_k} \frac{b_{j,k}}{(X-a_k)^j} \right) + \sum_{k=1}^{r} \left( \sum_{j=1}^{l_k} \frac{c_{j,k}X + d_{j,k}}{(X^2+p_kX+q_k)^j} \right)$$

La première somme est en fait la somme des parties polaires de $F$ relatives aux pôles réels de $F$. La seconde somme est la somme des éléments simples de seconde espèce.

**Remarque 3.2.20** *La décomposition sur $\mathbb{R}$ d'une fraction rationnelle sera obtenue à partir de sa décomposition sur $\mathbb{C}$ en regroupant 2 à 2 les parties principales relatives aux pôles complexes conjugués de même ordre.*

### 3.2.3 Méthodes pratiques de décomposition

Soit $F$ une fraction rationnelle quelconque , alors F se décompose en éléments simples selon les étapes suivantes :

- On commence par s'assurer que la fraction rationnelle $F = \frac{P}{Q}$ est irréductible, c'est à dire que le numérateur $P$ et le dénominateur $Q$ n'ont pas de zéro commun.

– Recherche de la partie entière dans le cas où le degré du numérateur est supérieur ou égal au degré du dénominateur. Pour cela il faut effectuer la division euclidienne et donc penser à développer le dénominateur (s'il est sous forme factorisé).
– Recherches des zéros du dénominateur (c'est-à-dire les pôles de la fraction rationnelle).
– Ecrire la forme générale de la décomposition en éléments simples en faisant apparaître les éléments de première espèce et ceux de seconde espèce si c'est une décomposition directe sur $\mathbb{R}$.

Le calcul des coefficients se fait en appliquant toutes les techniques suivantes :

1) Méthode simple d'identification.

2) Utilisation des conditions de parité : Si une fraction rationnelle est paire ou impaire, alors on exprime cette invariance par les transformations $X \longmapsto F(-X)$ ou $X \longmapsto -F(-X)$, et on déduit des relations sur les coefficients, cette idée permet donc de diminuer environ de moitié le nombre d'inconnues.

3) Choix de valeurs particulières de $X$ : les pôles.

4) Choix de certaines valeurs simples de $X$ autres que les pôles.

5) Utilisation d'une transformation laissant la fraction invariante : elle consiste à faire un changement de variable transformations, comme $X \longmapsto \alpha - X, X \longmapsto \alpha X, X \longmapsto \frac{1}{X}$, ou $X \longmapsto X + \frac{1}{X}$

6) Etude à la limite, Multiplions par $X$ puis faisons tendre $X$ vers l'infini.

### 3.2.4 Exemple de la décomposition dans $\mathbb{R}(X)$

**Exemple 3.2.21** *Soit $F = \frac{P}{Q} = \frac{X^3}{X^3-1}$, alors le numérateur et le dénominateur n'ont pas de racine commune, mais ils sont de même degré. On a*

$$F = \frac{X^3}{X^3-1} = 1 + \frac{1}{X^3-1}$$

*La factorisation de $Q$ est $Q = X^3 - 1 = (X-1)(X^2+X+1)$. D'après le théorème de décomposition en éléments simples il existe des constantes $a, b, c$ telles que*

$$\frac{1}{X^3-1} = \frac{1}{(X-1)(X^2+X+1)} = \frac{a}{X-1} + \frac{bX+c}{X^2+X+1}$$

*Pour identifier les constantes, on peut par exemple réduire au même dénominateur, on obtient l'identité :*

$$\frac{1}{X^3-1} = \frac{(a+b)X^2 + (a-b+c)X + a - c}{(X-1)(X^2+X+1)}$$

*Alors*

$$\begin{cases} a+b=0 \\ a-b+c=0 \\ a-c=1 \end{cases} \Longrightarrow a=\frac{1}{3}, b=-\frac{1}{3}, c=-\frac{2}{3}$$

*Ou bien : – on multiplie l'identité par* $(X-1)$ *et on prend la valeur en* $1$ *:*

$$\frac{1}{(X^2+X+1)}=a+\frac{(bX+c)(X-1)}{X^2+X+1} \Longrightarrow a=\frac{1}{3}$$

*– On multiplie par* $X$ *et on prend la limite en* $+\infty$ *:*

$$\begin{aligned} \frac{X}{X^3-1} &= \frac{aX}{X-1}+\frac{bX^2+cX}{X^2+X+1} \Longrightarrow 0=a+b \\ &\Longrightarrow b=-\frac{1}{3} \end{aligned}$$

*– On peut prendre la valeur en un point où la fraction est défini, par exemple* $0$*, et on obtient :*

$$\frac{1}{-1}=-a+c \Longrightarrow, c=-\frac{2}{3}$$

*Donc*

$$F=\frac{X^3}{X^3-1}=1+\frac{1}{3}.\frac{1}{X-1}-\frac{1}{3}.\frac{X+2}{X^2+X+1}$$

**Exemple 3.2.22** *Soit* $F=\frac{P}{Q}=\frac{1}{X^3(X^2-1)}$
*Les pôles sont* $0$ *triple,* $1$ *simple et* $-1$ *simple. La partie entière est nulle car* $\deg(P)<\deg(Q)$*. F est irréductible. La factorisation de Q est* $Q=X^3(X-1)(X+1)$*. Alors la forme générale de la décomposition de F est :*

$$F=\frac{a}{X^3}+\frac{b}{X^2}+\frac{c}{X}+\frac{d}{X-1}+\frac{e}{X+1}$$

*F étant impaire, on a* $F(-X)=-F(X)$*, ce qui donne :*

$$F=\frac{a}{X^3}+\frac{-b}{X^2}+\frac{c}{X}+\frac{d}{X+1}+\frac{e}{X-1}=\frac{a}{X^3}+\frac{-b}{X^2}+\frac{c}{X}+\frac{e}{X-1}+\frac{d}{X+1}$$

*L'unicité de la décomposition nous donne les relations* $b=0$ *et* $e=d$*.*
*On trouve a en multipliant par* $X^3$ *et substituant* $0$ *à* $X$*. Donc* $a=-1$*.*
*On trouve d en multipliant par* $(X-1)$ *et substituant* $1$ *à* $X$*. Donc* $d=\frac{1}{2}$*.*
*En faisant tendre* $X$ *vers* $+\infty$ *dans la fonction rationnelle* $XF(X)$*, on obtient la relation* $c+1=0$*, donc* $c=-1$*, finalement la décomposition de F est*

$$F=-\frac{1}{X^3}+-\frac{1}{X}+\frac{1}{2}.\frac{1}{X-1}+\frac{1}{2}.\frac{1}{X+1}$$

### 3.2.5 Exemple de la décomposition dans $\mathbb{C}(X)$

**Exemple 3.2.23** *Soit la fraction rationnelle* $F = \frac{1}{(X-1)^2(X+1)^2}$. *Elle admet deux pôles d'ordre* 2, *à savoir* $\alpha = 1$ *et* $\beta = -1$. *Sa décomposition s'écrit formellement*

$$F = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{(X+1)^2} + \frac{d}{X+1}$$

*Or la fraction rationnelle étant paire par rapport à la variable* $X$, *elle garde la même valeur quand on change* $X$ *en* $-X$. *Ainsi*

$$F = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{(X+1)^2} + \frac{d}{X+1} = \frac{a}{(X+1)^2} - \frac{b}{X+1} + \frac{c}{(X-1)^2} - \frac{d}{X-1}$$

*On obtient* $a = c$ *et* $b = -d$ . *Finalement, deux coefficients doivent être calculés.*
$F$ *s'écrit sous la forme*

$$F = \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{a}{(X+1)^2} - \frac{b}{X+1}$$

*On Choisit certaines valeurs simples de* $X$ *autres que les pôles par exemple* $X = 0$ *et* $X = 2$, *on trouve* $2a - 2b = 1$ *et* $10a + 6b = 1$.*Ainsi,* $a = \frac{1}{4}, b = -\frac{1}{4}, c = \frac{1}{4}, d = \frac{1}{4}$. *Finalement*

$$F = \frac{1}{4}.\frac{1}{(X-1)^2} - \frac{1}{4}.\frac{1}{X-1} + \frac{1}{4}.\frac{1}{(X+1)^2} + \frac{1}{4}.\frac{1}{X+1}$$

# Bibliographie


[1] Alain Soyeur, François Capaces, Emmanuel Vieillard-Baron, *Cours de Mathématiques, Sup MPSI PCSI PTSI TSI*. L'association Sésamath, 2010.

[2] Jean-Pierre Ramis, André Warusfel , Xavier Buff, Josselin Garnier, Emmanuel Halberstadt , Thomas Lachand-Robert , François Moulin, Jacques Sauloy, *Mathématiques tout en un pour la licence niveau L1,Cours complet et 270 exercices corrigés*. Dunod, Paris, 2006.

[3] Jean- Marie Monier. *Algèbre 1, cours et 600 exercices corrigés*. $1^{ere}$ année MPSI,PCSI, PTSI $2^{ème}$ édition. DUNOD, Paris 2000.

[4] Jean-Pierre Escofier, *Toute d'algèbre de la licence, Cours et exercices corrigés,* 2ème édition, Dunod, Paris, 2002, 2006.

[5] Xavier Dussau, Jean Esterle, Fouad Zarouf, Rachid Zarouf, *ESTIA $1^{ere}$ Année Mathématiques, Cours d'algèbre*. 2008

[6] Rémy Goblot, Guy Auliac, Jean Delcourt, *Mathématiques, algèbre et géométrie*. Dunod, Paris, 2005.