Chapitre 3

Polynômes et fractions rationnelles

Algèbre $\mathbb{K}_{[X]}$

Définitions et Vocabulaire

Définition

Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$. On appelle **support** de $(a_n)_{n\in\mathbb{N}}$ l'ensemble des $n \in \mathbb{N}$ tels que $a_n \neq 0$.

Exemples

Définition

On appelle **polynôme (à une indéterminée et à coefficients dans** $\mathbb{K}$) toute suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$ à support fini.
L'ensemble des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ (ou $\mathbb{K}^{(\mathbb{N})}$)
Autrement dit, un polynôme de $\mathbb{K}[X]$ est une suite à termes dans $\mathbb{K}$ nulle à partir d'un certain rang.

Exemples

Remarques et vocabulaire

1. Il est bien clair que $\mathbb{K}[X] \subsetneq \mathbb{K}^{\mathbb{N}}$.
2. On a
$$\begin{aligned} P &= (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \Longleftrightarrow (\exists N \in \mathbb{N}, \forall n \in \mathbb{N}, (n > N \Longrightarrow a_n = 0)) \\ &\Longleftrightarrow P = (a_0, a_1, \cdots, a_N, 0 \cdots, 0). \end{aligned}$$
3. La notation "bizzare" $\mathbb{K}[X]$ sera justifiée plus tard.
4. On note $0_{\mathbb{K}[X]}$ la suite constante nulle de $\mathbb{K}^{\mathbb{N}}$ définie par
$$\forall n \in \mathbb{N},\ a_n = 0;$$
appelée **polynôme nul**. Ainsi
$$0_{\mathbb{K}[X]} = (0, 0, \cdots, 0, 0 \cdots, 0).$$

5. On appelle **polynôme constant** toute suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ tels que

$$\forall n \geq 1, \quad a_n = 0,$$

c-à-d

$$P = (a_0, 0, \cdots, 0, 0 \cdots, 0).$$

6. On appelle **monôme** toute suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ tels qu'il existe $n_0 \in \mathbb{N}$ vérifiant

$$\forall n \in \mathbb{N}, \ (n \neq n_0 \Longrightarrow a_n = 0),$$

c-à-d

$$P = (0, 0, \cdots, a_{n_0}, 0 \cdots, 0).$$

7. Il résulte de la définition que deux polynômes $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ de $\mathbb{K}[X]$ sont égaux si et seulement si

$$\forall n \in \mathbb{N}, \ a_n = b_n.$$

8. Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$. On dit que P est **pair** si $a_{2n+1} = 0, \forall n \in \mathbb{N}$, et P est **impair** si $a_{2n} = 0, \forall n \in \mathbb{N}$

Degré et valuation

Définitions Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.

1. Si $P \neq 0_{\mathbb{K}[X]}$, on appelle **degré** de P et qu'on note $\deg(P)$ ou bien d^0P le plus grand entier naturel n tel que $a_n \neq 0$, l'élément $a_{\deg(P)}$ est appelé le coefficient du terme du plus haut degré.

2. On convient que $\deg(0_{\mathbb{K}[X]}) = -\infty$.

3. Si $P \neq 0_{\mathbb{K}[X]}$, on appelle **valuation** de P et qu'on note $val(P)$ le plus petit entier naturel n tel que $a_n \neq 0$, l'élément $a_{val(P)}$ est appelé le coefficient du terme du plus bas degré.

4. On convient que $val(0_{\mathbb{K}[X]}) = +\infty$.

5. On dit que P est **unitaire** ou **normalisé** si $a_{\deg(P)} = 1$.

Remarques : Soit $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$. Alors

1. $\deg(P) \in \mathbb{N} \cup \{-\infty\}$.

2. $val(P) \in \mathbb{N} \cup \{+\infty\}$

3. $val(P) \leq \deg(P)$ pout tout $P \neq 0_{\mathbb{K}[X]}$.

Exemples

$P =$

Addition

Proposition-Définition
Soient $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.
Alors $P + Q = (a_n + bn)_{n\in\mathbb{N}} \in \mathbb{K}[X]$, appelé somme des polynômes P et Q.
Démonstration
Il faut montrer que $(a_n + bn)_{n\in\mathbb{N}}$ est une suite nulle à partir d'un certain rang. Mais

$$P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \Longleftrightarrow (\exists N_1 \in \mathbb{N}, \forall n \in \mathbb{N}, (n > N_1 \Longrightarrow a_n = 0))$$

et

$$Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X] \Longleftrightarrow (\exists N_2 \in \mathbb{N}, \forall n \in \mathbb{N}, (n > N_2 \Longrightarrow b_n = 0)).$$

Posons $N = \max(N_1, N_2) \in \mathbb{N}$ on a alors

$$\forall n \in \mathbb{N}, \quad (n > N \Longrightarrow n > N_1 \text{ et } n > N_2 \Longrightarrow a_n = 0 \text{ et } b_n = 0 \Longrightarrow a_n + b_n = 0).$$

Ce qui prouve que $P + Q = (a_n + bn)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.

Proposition
Soient P et Q deux polynômes. Alors :

$$deg(P + Q) \leq \max\{deg(P), deg(Q)\}\text{avec égalité si } deg(P) \neq deg(Q)$$

et

$$val(P + Q) \geq \min\{val(P), val(Q)\}\text{avec égalité si } val(P) \neq val(Q)$$

Démonstration

Les propriétés sont évidentes si $P = 0$ ou $Q = 0$.
Supposons $P \neq 0$ et $Q \neq 0$, et notons

$$P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}, N_1 = \deg(P), N_2 = \deg(Q), \nu_1 = val(P), \nu_2 = val(Q).$$

Posons

$$N = \max(N_1, N_2) \text{ et } \nu = \max(\nu_1, \nu_2).$$

Alors $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$, et pour tout $n \in \mathbb{N}$ on a

$$n > N \Longrightarrow \left\{ \begin{array}{ccc} n & > & N_1 \\ n & > & N_2 \end{array} \right. \Longrightarrow \left\{ \begin{array}{ccc} a_n & = & 0 \\ b_n & = & 0 \end{array} \right. \Longrightarrow a_n + b_n = 0,$$

donc $\deg(P+Q) \leq N$.
D'autre part, pour tout $n \in \mathbb{N}$ on a

$$n < \nu \Longrightarrow \left\{ \begin{array}{ccc} n & < & \nu_1 \\ n & < & \nu_2 \end{array} \right. \Longrightarrow \left\{ \begin{array}{ccc} a_n & = & 0 \\ b_n & = & 0 \end{array} \right. \Longrightarrow a_n + b_n = 0,$$

donc $val(P+Q) \geq \nu$.

Supposons que $\deg(P) \neq \deg(Q)$, par exemple : $N_1 < N_2$, alors

$$a_N + b_N = a_{N_2} + b_{N_2} = b_{N_2} \neq 0 \text{ donc } \deg(P+Q) = N_2 = N.$$

De même, si par exemple, $\nu_1 = val(P) > \nu_2 = val(Q)$, alors

$$a_\nu + b_\nu = a_{\nu_2} + b_{\nu_2} = b_{\nu_2} \neq 0 \text{ donc } val(P+Q) = \nu_2 = \nu.$$

Exemples
1. $P = X^{2016} - 3X^5 + 2$. On $\deg(P) = 2016$ et $val(P) = 0$
2. $P = X^5 - 6X^4 + X$. On On $\deg(P) = 5$ et $val(P) = 1$.

Multiplication

Proposition-Définition
Soient $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$.

On appelle produit de P par Q et on note $P \times Q$ ou PQ, la suite $(c_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$ définie par

$$\forall n \in \mathbb{N}, \qquad c_n = \sum_{i+j=n} a_i b_j = \sum_{k=0}^{n} a_k b_{n-k}.$$

Proposition
Soient P et Q deux polynômes. Alors :

$$deg(PQ) = deg(P) + deg(Q) \text{ et } val(PQ) = val(P) + val(Q)$$

- **Démonstration :**
  Les propriétés sont évidentes si $P = 0$ ou $Q = 0$.
  Supposons $P \neq 0$ et $Q \neq 0$, et notons

  $$P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}, N_1 = \deg(P), N_2 = \deg(Q), \nu_1 = val(P), \nu_2 = val(Q).$$

  Posons

  $$PQ = (c_n)\, n \in \mathbb{N},\ N = \max(N_1, N_2) \text{ et } \nu = \max(\nu_1, \nu_2).$$

D'après la proposition précédente pour tout $n \in \mathbb{N}$ on a

$$n > N_1 + N_2 \Longrightarrow c_n = 0,$$

En outre

$$c_{N_1+N_2} = \sum_{k=0}^{N_1+N_2} a_k b_{N_1+N_2-k} = a_{N_1} b_{N_2} = 0,$$

car, pour tout $k \in \mathbb{N}$,

$$\begin{cases} k < N_1 & \Longrightarrow & N_1 + N_2 - k > N_2 & \Longrightarrow & b_{N_1+N_2-k} = 0 \\ k > N_1 & \Longrightarrow & a_k = 0 \end{cases}$$

Ceci prouve que $\deg(PQ) = \deg(P)\deg(Q)$.

Remarque :
On convient que pour tout $n \in \mathbb{N}$

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

Proposition
$(\mathbb{K}[X], +, \times)$ est un anneau commtatif intègre. L'élément neutre de la loi $(+)$ est $0_{\mathbb{K}[X]}$ et l'élément unité est $1_{\mathbb{K}[X]}$.
Démonstration
$(\mathbb{K}[X], +)$ est un groupe commutatif.
La multiplication est une loi interne dans $\mathbb{K}[X]$. Montrons que la multiplication est associative. Soient

$$P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}, P = (a_n)_{n\in\mathbb{N}}, R = (c_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$$

Alors

$$PQ = P = (d_n)_{n\in\mathbb{N}}, \text{ où } \forall n \in \mathbb{N}, \quad d_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

puis

$$(PQ)R = (e_n)_{n\in\mathbb{N}}, \text{ où } \forall n \in \mathbb{N}, \quad e_n = \sum_{k=0}^{n} d_k c_{n-k}.$$

D'autre part,

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

puis

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

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

$$\begin{aligned} g_n &= \sum_{i+p=n} a_i f_p = \sum_{i+p=n} a_i \left(\sum_{j+k=p} b_j c_k\right) = \sum_{i+(j+k)=n} a_i\,(b_j c_k) = \sum_{i+(j+k)=n} (a_i b_j)\, c_k \\ &= \sum_{q+k=n}\left(\sum_{j+i=q} a_i b_j\right) c_k = \sum_{s+r=n} d_s c_r. = \sum_{k=0}^{n} d_k c_{n-k} = e_n. \end{aligned}$$

Ceci prouve que $P\,(QR) = (PQ)\,R$.
Proposition
Les seuls éléments inversibles de l'anneau $(\mathbb{K}\,[X]\,,+,\times)$ sont les polynômes constants.
Démonstration

Montrons que les seuls éléments inversibles de l'anneau $(\mathbb{K}\,[X]\,,+,\times)$ sont les polynômes constants autre que le polynôme nul.
Il est clair que tout élément de $\mathbb{K}^*$ est inversible car $\mathbb{K}$ est un corps.
Réciproquement, soit $P\in\mathbb{K}\,[X]$ inversible. Montrons que P est un polynôme constant.
Dire que P est inversible revient à dire qu'il existe $Q\in\mathbb{K}\,[X]$ tel que $PQ=1$. Alors

$$\deg(PQ)=0 \Longrightarrow \deg(P)+\deg(Q)=0 \Longrightarrow \deg(P)=0 \text{ et} \deg(Q)=0,$$

c'est-à-dire P est un polynôme constant non nul.
Il en résulte que seuls les polynômes constants autres que $0_{\mathbb{K}[X]}$ sont inversibles. Par conséquent, $(\mathbb{K}\,[X]\,,+,\times)$ n'est pas un corps.

Lois externe

On considère l'application

$$\begin{array}{rccc} \cdot\ : & \mathbb{K}\times\mathbb{K}\,[X] & \longrightarrow & \mathbb{K}\,[X] \\ & (\lambda,P) & \longmapsto & \lambda\cdot P \end{array}$$

telle que pour tout $P=(a_n)_{n\in\mathbb{N}}\in\mathbb{K}\,[X]$ on a $\lambda\cdot P = \lambda\cdot(a_n)_{n\in\mathbb{N}} = (\lambda a_n)_{n\in\mathbb{N}}\in\mathbb{K}\,[X]\,.$ On définit ainsi une loi de composition externe sur $\mathbb{K}\,[X]$ vérifiant les propriétés suivantes :

1. $\forall P\in\mathbb{K}\,[X]\,,$ on a $1_{\mathbb{K}}\cdot P = P$
2. $\forall\alpha,\beta\in\mathbb{K},\forall P\in\mathbb{K}\,[X]$ on a $\alpha\cdot(\beta\cdot P) = (\alpha\beta)\cdot P$
3. $\forall\alpha,\beta\in\mathbb{K},\forall P\in\mathbb{K}\,[X]$ on a $(\alpha+\beta)\cdot P = \alpha\cdot P+\beta\cdot P.$

4. $\forall\alpha \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$ on a $\alpha \cdot (P+Q) = \alpha \cdot P + \alpha \cdot Q$.

Proposition
$(\mathbb{K}[X], +, \times, \cdot)$ est une $K-$algèbre associative, commutative, unitaire.

La proposition suivante est immédiate.
Proposition
$\forall\alpha \in \mathbb{K}-\{0\}, \forall P \in \mathbb{K}[X]$ on a :

$$\left\{ \begin{array}{rcl} \deg(\alpha P) & = & \deg(P) \\ val(\alpha P) & = & val(P) \end{array} \right.$$

Nouvelle écriture des polynômes

Définition

Soit X une lettre non utilisée par ailleurs. On note

$$X = (0, 1, \cdots, 0, 0 \cdots).$$

La lettre X est donc utilisée pour désigner le polynôme particulier $(0, 1, \cdots, 0, 0 \cdots)$. On dit que X est l'indétérminée. L'indéterminée est donc la lettre servant à désigner ce polynôme particulier. Le nom donnée à cette lettre dépend des circonstances, du moment qu'elle n'est pas utilisée par une autre chose dans le même texte. X est donc un polynôme particulier. X n'est pas une variable.
Calculons X^2 . On obtient alors

$$X^2 = XX = (0, 1, \cdots, 0, 0 \cdots, 0)(0, 1, \cdots, 0, 0 \cdots, 0) = (0, 0, 1, 0 \cdots, 0 \cdots).$$

Une récurrence immédiate donne

$$X^n = (0, \cdots, 0, 1, 0 \cdots, 0 \cdots)$$

où 1 est à la $(n+1)^0$ place. On convient que $1 = X^0$
Par ailleurs, soit $P = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}[X]$ et $N \in \mathbb{N}$ tel que $N \geq \deg(P)$; on a :

$$\begin{array}{rcl} P & = & (a_0, a_1, \cdots, a_N, 0 \cdots, 0) \\ & = & a_0(1, 0, \cdots, 0, 0 \cdots) + a_1(0, 1, \cdots, 0, 0 \cdots) + \ldots + a_N(0, 0, \cdots, 1, 0 \cdots, 0) \\ & = & a_0 + a_1X + \ldots + a_NX^N \\ & = & \sum\limits_{k=0}^{N} a_kX^k. \end{array}$$

Avec cette notation un monôme s'écrit donc a_kX^k, le polynôme constant est a_0 et $\forall n, m \in \mathbb{N}$ on a $X^{m+n} = X^mX^n$.

Composition des polynômes

Définition :

Soient $P = \sum\limits_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$. On définit le polynôme **composé** $P \circ Q$ (ou $P(Q)$) par

$$P \circ Q = P(Q) = \sum_{k=0}^{N} a_k Q^k.$$

Autrement dit, on a remplacé l'indéterminée X par Q.

Proposition

Soient P et Q deux polynômes non nuls. Alors :

$$deg(P \circ Q) = deg(P).deg(Q)$$

Démonstration

Proposition

Soient $\alpha \in \mathbb{K}$ et $(P, Q, R) \in (\mathbb{K}[X])^3$ on a alors

1. $(P + \alpha Q) \circ R = P \circ R + \alpha Q \circ R.$ (la loi $\circ$ est distributive à droite sur $+$ dans $\mathbb{K}[X]$)
2. $(PQ) \circ R = (P \circ R)(Q \circ R)$.
3. $(P \circ Q) \circ R = P \circ (Q \circ R)$ (la loi $\circ$ est associative dans $\mathbb{K}[X]$)
4. $X \circ P = P \circ X = P.$

Remarques :

1. La loi $\circ$ n'est pas commutative dans $\mathbb{K}[X]$. En effet, pour $P = X + 2$ et $Q = X^2 + 1$ on a
$$P \circ Q = P(Q) = Q + 2 = X^2 + 3$$
cependant,
$$Q \circ P = Q(P) = P^2 + 1 = (X + 2)^2 + 1 = X^2 + 4X + 5$$
ce qui prouve que $P \circ Q \neq Q \circ P$.

2. La loi $\circ$ n'est pas distributive à gauche sur $+$ dans $\mathbb{K}[X]$.En effet, pour $P = X^2$ et $Q = R = 1$ on a
$$P \circ (Q + R) = X^2(2) = 4$$
cependant,
$$P \circ Q + P \circ R = X^2 \circ 1 + = X^2 \circ 1 = 1 + 1 = 2.$$
ce qui prouve que $P \circ (Q + R) \neq P \circ Q + P \circ R$.

Remarque :
On notera P ou $P(X)$ un polynôme de $\mathbb{K}[X]$.

Dérivation

Définition : Soient $P = \sum\limits_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$. On appelle **polynôme dérivé de** qu'on note P' le polynôme défini par
$$P' = \sum_{k=1}^{N} k a_k X^{k-1} = \sum_{k=0}^{N-1} (k+1)\, a_{k+1} X^k$$
On note $P^{(0)} = P,\ \ P^{(1)} = P', P^{(2)} = P''$ et pour tout n de $\mathbb{N}^*$, $\quad P^{(n)} = \left(P^{(n-1)}\right)'$.

Exemples
1. $P = X^{2016} - 3X^5 + 2$. Donc $P' = 2016X^{2015} - 15X^4$
2. $P = X^5 - 6X^4 + X$. Donc $P' = 5X^4 - 24X^3 + 1$.

La proposition suivante est immédiate.

Proposition
$\forall P \in \mathbb{K}[X]$ on a :
$$\deg(P') = \begin{cases} \deg(P) - 1 & \text{si} \quad \deg(P) \geq 1 \\ -\infty & \text{si} \quad \deg(P) \leq 0 \end{cases}$$

Proposition
$\forall n \in \mathbb{N}, \forall P \in \mathbb{K}[X]$ on a :
$$\left(\deg(P) \leq n \iff P^{(n+1)} = 0 \right)$$

Proposition
$\forall \alpha \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$ on a :

1. $(P + Q)' = P' + Q'$
2. $(\alpha P)' = \alpha P'$
3. $(PQ)' = P'Q + PQ'$
4. $(P \circ Q)' = P'(Q)\, Q'$

5. $\forall n \in \mathbb{N}$

$$(PQ)^{(n)} = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}.$$

Fonctions polynômiales

Soit $P = \sum\limits_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$. On considère l'application

$$\begin{array}{rccl} \widetilde{P} & : \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & \widetilde{P}(x) = \sum\limits_{k=0}^{N} a_k x^k \end{array}$$

appelée **fonction polynômiale associée à** P.
Commentaire :
Dans $P = \sum\limits_{k=0}^{N} a_k X^k$ le X est une indéterminée, ce qui nous permet d'écirire $P(Q) = \sum\limits_{k=0}^{N} a_k Q^k$ ou $P(f) = \sum\limits_{k=0}^{N} a_k f^k$ ou bien $P(\nabla) = \sum\limits_{k=0}^{N} a_k \nabla^k$. En revanche, dans $\widetilde{P}(x)$ le x est un scalaire (réel ou complexe).

Proposition
$\forall \alpha \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$ on a :

1. $\widetilde{P + \alpha Q} = \widetilde{P} + \alpha \widetilde{Q}$
2. $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$
3. $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$
4. $\left(\widetilde{P}\right)' = \widetilde{P'}$

Remarque :
On pourra selon la commodité confondre P et $\widetilde{P}$.

Algorithme de Hörner

Soit $P = \sum\limits_{k=0}^{N} a_k X^k \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On veut calculer

$$\widetilde{P}(\alpha) = \sum_{k=0}^{N} a_k \alpha^k = a_0 + a_1 \alpha^1 + a_2 \alpha^2 \ldots + a_N \alpha^N.$$

On doit donc calculer

$$\left\{ \begin{array}{ccc} \alpha^N & \text{puis multiplier par} & a_N \\ & + & \\ \alpha^N & \text{puis multiplier par} & a_{N-1} \\ & + & \\ \vdots & \vdots & \vdots \\ \alpha^2 & \text{puis multiplier par} & a_2 \\ & + & \\ \alpha & \text{puis multiplier par} & a_1 \\ & + & \\ & a_0 & \end{array} \right.$$

Cela nécessite $\frac{n(n+1)}{2}$ multiplications et n additions. C'est fastidieux ! Au secours Hörner!
La méthode de Hörner consiste à calculer

$$\begin{array}{rcl} \widetilde{P}\left(\alpha\right) & = & a_N\alpha^N + a_{N-1}\alpha^{N-1} + \cdots + a_2\alpha^2 + a_1\alpha + a_0 \\ & = & \left(\left(\cdots\left(\left(\left(a_N\alpha + a_{N-1}\right)\alpha + a_{N-2}\right)\alpha + a_{N-3}\right)\alpha + \cdots + a_2\right)\alpha + a_1\right)\alpha + a_0 \end{array}$$

Cela nécessite n multiplications et n additions. C'est plus économique!

Exemples :

Théorème : (Théorème de Taylor pour les polynômes)
Soient $P \in \mathbb{C}\left[X\right]$, et $N \in \mathbb{N}$. tel que $\deg(P) \leq N$, $a \in \mathbb{C}$, on a

$$P(a+X) = \sum_{k=0}^{N} \frac{\widetilde{P^{(n)}}(a)}{n!} X^k$$

Démonstration :

En remplaçant X par $(X-a)$ dans la formule précédente on obtient

Corollaire :
Soient $P \in \mathbb{C}\left[X\right]$, et $N \in \mathbb{N}$. tel que $\deg(P) \leq N$, $a \in \mathbb{C}$, on a

$$P(X) = \sum_{k=0}^{N} \frac{\widetilde{P^{(n)}}(a)}{n!} \left(X-a\right)^k$$

Division suivant les puissances croissantes

Théorème Soient A et B deux polynômes tel que $val\left(B\right) = 0$. Il existe un unique couple (Q,R) de polynômes tel que :

$$\left\{\begin{array}{ccc} A & = & BQ + X^{n+1}R \\ \text{avec} & & \\ \deg(Q) & \leq & n \end{array}\right.$$

Les polynômes Q et R s'appellent respectivement **quotient** et **reste** dans la division de A par B.
suivant les puissances croissantes jusqu'à l'ordre n.

Démonstration : On a deux choses à démontrer : l'existence et l'unicité.

<u>Existence :</u> Par récurrence sur $\deg(P)$, Q étant fixé. On écrit

$$P = \sum_{k=0}^{n} a_k X^k \text{ et } Q = \sum_{k=0}^{q} b_k X^k.$$

Si $n < q$, alors on peut prendre $A = 0$ et $B = P$.
Si $n \geq q$, on construit le polynôme $P_1 = P - \frac{a_n}{b_q} Q X^{n-q}$; le terme de plus haut degré de ce nouveau polynôme est strictement inférieur à n car son terme de degré n est nul (on a ch oisi le coefficient devant Q volontairement pour cela). On applique l'hypothèse de récurrence au polynôme P_1 ainsi obtenu; il existe donc A_1 et B_1 deux polynômes de $\mathbb{K}[X]$ tels que

$$\left\{\begin{array}{ccc} P_1 & = & A_1 Q + B_1 \\ \deg(B_1) & < & \deg(Q) \end{array}\right. .$$

Ceci donne alors

$$\left\{\begin{array}{ccc} P & = & \left(\frac{a_n}{b_q} Q X^{n-q} + A_1\right) Q + B_1 \\ \deg(B_1) & < & \deg(Q) \end{array}\right. .$$

En posant $A = \left(\frac{a_n}{b_q} Q X^{n-q} + A_1\right)$ et $B = B_1$, on obtient alors

$$\left\{\begin{array}{ccc} P & = & AQ + B \\ \deg(R) & < & \deg(B) \end{array}\right. .$$

ce qui prouve l'existence.
<u>Unicité :</u> Supposons qu'il existe deux couples (A, B) et (A', B') de $(\mathbb{K}[X])^2$ tels que

$$\left\{\begin{array}{ccc} P & = & AQ + B \\ \deg(B) & < & \deg(Q) \end{array}\right. \text{ et } \left\{\begin{array}{ccc} P & = & A'Q + B' \\ \deg(B') & < & \deg(Q) \end{array}\right.$$

Ainsi $(A - A')Q = B' - B$. Or,

$$\deg\left((A - A')Q\right) = \deg(Q) + \deg(A - A') = \deg(B - B')$$

et

$$\deg(B - B') \leq \max(\deg(B), \deg(B')) < \deg(Q)$$

ce qui implique que $\deg(A-A') \leq 0$; la seule possibilité c'est que $A - A' = 0$; donc $A = A'$ et par conséquent $B = B'$.
Exemples :

Divisibilité dans $\mathbb{K}[X]$

Soient $A, P \in \mathbb{K}[X]$. On dit que A divise P ou P est divisible par A et on note A/P s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = AQ$. Dans ce cas A est un diviseur de P et P est un multiple de A

Proposition.

1) $\forall A \in \mathbb{K}[X]$, on a $A \mid A$.
2) $\forall A, P \in \mathbb{K}[X]$, on a $(A \mid P \text{ et } P \mid A \Longleftrightarrow \exists \alpha \in \mathbb{K} \text{ tel que } P = \alpha A)$: On dit que A et P sont **associés**.
3) $\forall A, B, C \in \mathbb{K}[X]$, on a $(A \mid B \text{ et } B \mid C \Longleftrightarrow A \mid C)$.

Démonstration : Facile
Proposition.

1) $\forall A, B, C \in \mathbb{K}[X]$, on a $(A \mid B \Longleftrightarrow A / BC)$
2) $\forall A, B, C \in \mathbb{K}[X]$, on a $(A \mid B \text{ et } B \mid C \Longleftrightarrow A \mid B + C)$.
3) $\forall A, B, C, D \in \mathbb{K}[X]$, on a $(A \mid B \text{ et } C / D \Longleftrightarrow AC \mid BD)$.
4) $\forall A, B \in \mathbb{K}[X]$, $\forall n \in \mathbb{N}$ on a $(A \mid B \Longleftrightarrow A^n \mid B^n)$.

Démonstration : Immédiate
Division euclidienne.

Théorème-Définition 1. Soient $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0_{\mathbb{K}[X]}$. Il existe un unique couple $(A, B) \in \mathbb{K}[X]^2$ tels que

$$\begin{cases} P & = & AQ + B \\ \deg(B) & < & \deg(Q) \end{cases}.$$

Le polynôme A est appelé le quotient de la division euclidienne de P par Q; et le polynôme B est appelé le reste de la division euclidienne de P par Q.
Remarque :
On notera l'analogie dans l'énoncé avec la division euclidienne dans $\mathbb{Z}$. Les démonstrations, en ce qui conçerne l'unicité sont aussi analogues.
Démonstration.

On a deux choses à démontrer : l'existence et l'unicité.

<u>Existence :</u> Par récurrence sur $\deg(P)$, Q étant fixé. On écrit

$$P = \sum_{k=0}^{n} a_k X^k \text{ et } Q = \sum_{k=0}^{q} b_k X^k.$$

Si $n < q$, alors on peut prendre $A = 0$ et $B = P$.

Si $n \geq q$, on construit le polynôme $P_1 = P - \frac{a_n}{b_q} Q X^{n-q}$; le terme de plus haut degré de ce nouveau polynôme est strictement inférieur à n car son terme de degré n est nul (on a ch oisi le coefficient devant Q volontairement pour cela). On applique l'hypothèse de récurrence au polynôme P_1 ainsi obtenu; il existe donc A_1 et B_1 deux polynômes de $\mathbb{K}[X]$ tels que

$$\left\{ \begin{array}{ccc} P_1 & = & A_1 Q + B_1 \\ \deg(B_1) & < & \deg(Q) \end{array} \right. .$$

Ceci donne alors

$$\left\{ \begin{array}{ccc} P & = & \left(\frac{a_n}{b_q} Q X^{n-q} + A_1 \right) Q + B_1 \\ \deg(B_1) & < & \deg(Q) \end{array} \right. .$$

En posant $A = \left(\frac{a_n}{b_q} Q X^{n-q} + A_1 \right)$ et $B = B_1$, on obtient alors

$$\left\{ \begin{array}{ccc} P & = & AQ + B \\ \deg(R) & < & \deg(B) \end{array} \right. .$$

ce qui prouve l'existence.
Unicité : Supposons qu'il existe deux couples (A, B) et (A', B') de $(\mathbb{K}[X])^2$ tels que

$$\left\{ \begin{array}{ccc} P & = & AQ + B \\ \deg(B) & < & \deg(Q) \end{array} \right. \text{ et } \left\{ \begin{array}{ccc} P & = & A'Q + B' \\ \deg(B') & < & \deg(Q) \end{array} \right.$$

Ainsi $(A - A')Q = B' - B$. Or,

$$\deg\left((A - A')Q\right) = \deg(Q) + \deg(A - A') = \deg(B - B')$$

et

$$\deg(B - B') \leq \max(\deg(B), \deg(B')) < \deg(Q)$$

ce qui implique que $\deg(A - A') \leq 0$; la seule possibilité c'est que $A - A' = 0$; donc $A = A'$ et par conséquent $B = B'$.

Remarques.

1) Cette division est applé aussi division suivant les puissances décroissantes.

2) $\forall A, B \in \mathbb{K}[X]$, B divise A si, et seulement si, le reste de la division euclidienne de A par B est nul. .

3) $\forall A, B \in \mathbb{K}[X]$ on a

$$\deg(Q) = \left\{ \begin{array}{cc} -\infty & \text{si} \quad \deg(A) < \deg(B) \\ \deg(A) - \deg(B) & \text{sinon} \end{array} \right. .$$

4) Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 1$ et soit $a \in \mathbb{K}$. Effectuons la division euclidienne de P par $(X - a)$.Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$\left\{ \begin{array}{ccc} P & = & (X - a)Q + R \\ \deg(R) & < & 1 \end{array} \right. .$$

Ainsi le polynôme R est constant (éventuellement nul).
D'autre part, $\widetilde{P}(a) = (a-a)\widetilde{Q}(a) + \widetilde{R}(a)$, donc $\widetilde{P}(a) = \widetilde{R}(a) = R$. D'où $P = (X-a)Q + \widetilde{P}(a)$.

Exercice 1

Soient $n \in \mathbb{N} - \{0,1\}$, H et S les deux polynômes définis par :

$$H = (X-1)^{2n} - X^{n+1} + 1 \text{ et } S = X^2 - X.$$

Déterminer le reste de la division euclidienne de H par S.

Exercice 1(solution)

Soient $n \in \mathbb{N} - \{0,1\}$, H et S les deux polynômes définis par :

$$H(X) = (X-1)^{2n} - X^{n+1} + 1 \text{ et } S(X) = X^2 - X.$$

Le théorème de la division euclidienne de $H(X)$ par $S(X)$ nous dit qu'il existe $Q, R \in \mathbb{R}[X]$ tels que

$$\begin{cases} H(X) & = & S(X)Q + R \\ \deg(R) & < & 2 \end{cases}$$

Soit $R = aX + b$. Cherchons a, b.

On a $(X-1)^{2n} - X^{n+1} + 1 = (X^2 - X)Q + aX + b$.
<u>Pour $X = 0$</u> on obtient $2 = b$.
<u>Pour $X = 1$</u> on obtient $0 = a + b$.
Ainsi $R = -2X + 2$.

Polynômes irréductibles.

Définition. Soit $P \in \mathbb{K}[X]$.
1) On dit que P est irréductible (ou premier) si et seulement si $\deg(P) \geq 1$ et P n'admet comme diviseur dans $\mathbb{K}[X]$ que les constantes non nulles et ses polynômes associés.
2) On dit que P est réductible (ou non premier) si et seulement si P n'est pas irréductible. En d'autres termes

$$\exists P_1, P_2 \in \mathbb{K}[X], \text{ non constants tel que } P = P_1 P_2$$

Remarques.
1) Tout polynôme associé à un polynôme irréductible est irréductible.
2) Tout polynôme de degré 1 est irréductible.
3) Il découle de l'inclusion $\mathbb{R}[X] \subset \mathbb{C}[X]$, que tout polynôme à coefficients réels, premier dans $\mathbb{C}[X]$ est premier dans $\mathbb{R}[X]$.

Proposition. Soient $P \in \mathbb{K}[X]$ irréductible, $n \in \mathbb{N}^*$, $A_1, A_2, \cdots, A_n \in \mathbb{K}[X] - \{0\}$, alors

$$P \text{ divise } \prod_{i=1}^{n} A_i = 1 \Longleftrightarrow (\exists i \in \{1, 2, \cdots, n\}, P \text{ divise } A_i).$$

Théorème (de factorisation).

Soit $P \in \mathbb{K}[X]$ de degré ≥ 1. Alors P admet une décomposition en produits de polynômes irréductibles, unique à l'ordre près des facteurs et à constants de $\in \mathbb{K} - \{0\}$ multiplicatives près.i.e.

$$P = a \prod_{i=1}^{N} P_i^{\alpha_i}$$

où $\forall i \in \{1, 2, \cdots, N\}$, P_i est un polynôme unitaire et irréductible dans $\mathbb{K}[X]$, $\alpha_i \in \mathbb{N}$ et $a \in \mathbb{K}$.

Remarque L'écriture $P = a \prod_{i=1}^{N} P_i^{\alpha_i}$ s'appelle la décompositiuon primaire (ou décomposition de Gauss) de A dans $\mathbb{K}[X]$.

Racines.

1. Racines simples

Définition. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une racine de P (on zéro de P) si et seulement $P(\alpha) = 0$. (en réalité $\widetilde{P(\alpha)} = 0$)

Exemples.
1. $P = X^2 - 3X + 2$. On $P(1) = 0$
2. $P = X^2 + X + 1$. On $P(j) = 0$.

Proposition. Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Le scalaire α est une racine de P si et seulement $X - \alpha$ divise P.

Proposition. Soient $P \in \mathbb{K}[X]$ $n \in \mathbb{N}^*$ et $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{K}$ tels que $\alpha_i \neq \alpha_j$ si $i \neq j$. Alors

$$\alpha_1, \alpha_2, \cdots, \alpha_n \text{ racines de } P \Longleftrightarrow \prod_{i=1}^{N} (X - \alpha_i) \text{ divise } P.$$

Proposition. Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$. Alors P admet au plus n racines.

Proposition. Soient $P \in \mathbb{K}[X]$. Si P admet une infinité re racines alors $P = 0_{\mathbb{K}[X]}$.

Racines multiples

Définition. Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$.
1. On dit que α est une racine de P d'ordre au moins k si et seulement $(X - \alpha)^k$ divise P.
2. On dit que α est une racine de P d'ordre exactement k si et seulement $(X - \alpha)^k$ divise P et $(X - \alpha)^{k+1}$ ne divise pas$P$.

Vocabulaire.
L'entier k est appelé l'ordre de multiplicité de la racine α dans le polynôme P.
Si $k = 1$, on dit que la racine α est simple.

Si $k=2$, on dit que la racine α est double.
Si $k=3$, on dit que la racine α est triple.

Théorème (Caractérisation des racines d'ordre k).

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$.

αest une racine de P d'ordre exactement $k \Longleftrightarrow P(\alpha) = P'(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0$ et $P^{(k)}(\alpha) \neq 0$.

Exercice

Donner le reste de la division euclidienne de $P = (\cos\alpha + X\sin\alpha)^n$ par $\left(X^2+1\right)^2$ où $n \geq 4$, $n \in \mathbb{N}$.

Exercice (co)

En effectuant la division euclidienne de $P = (\cos\alpha + X\sin\alpha)^n$ par $\left(X^2+1\right)^2$ on obtient l'existence de deux polynômes Q et R tels que

$$\left\{\begin{array}{ccc} P & = & (X^2+1)^2 Q + R \\ \text{avec} & & \\ \deg(R) & < & 4 \end{array}\right.$$

ou encore $\deg(R) \leq 3$, soit $R = aX^3 + bX^2 + cX + d$. Cherchons a, b, c et $d \in \mathbb{C}$.
Remarqouns que

$$P' = 4X\left(X^2+1\right)Q + \left(X^2+1\right)^2 Q' + R' = \left(X^2+1\right)\left[4XQ + \left(X^2+1\right)Q'\right] + R'$$

Comme i et $-i$ sont les racines doubles de $\left(X^2+1\right)^2$ alors on obtient

$$\left\{\begin{array}{ccc} P(i) & = & R(i) \\ P(-i) & = & R(-i) \\ P'(i) & = & R'(i) \\ P'(-i) & = & R'(-i) \end{array}\right. \Longleftrightarrow \left\{\begin{array}{ccc} e^{in\alpha} & = & -ai - b + ci + d \\ e^{-in\alpha} & = & ai - b - ci + d \\ n\sin\alpha e^{i(n-1)\alpha} & = & -3a + 2bi + c \\ n\sin\alpha e^{-i(n-1)\alpha} & = & -3a - 2bi + c \end{array}\right.$$

$$\Longleftrightarrow \left\{\begin{array}{ccc} a & = & -\frac{1}{2}\sin n\alpha + \frac{n}{2}\sin\alpha\cos(n-1)\alpha \\ b & = & \frac{n}{2}\sin\alpha\sin(n-1)\alpha \\ c & = & \frac{1}{2}\sin n\alpha + \frac{n}{2}\sin\alpha\cos(n-1)\alpha \\ d & = & \frac{n}{2}\sin\alpha\sin(n-1)\alpha + \cos n\alpha \end{array}\right.$$

Par suite

$$\begin{aligned} R \;=\; & \left(-\frac{1}{2}\sin n\alpha + \frac{n}{2}\sin\alpha\cos(n-1)\alpha\right)X^3 + \left(\frac{n}{2}\sin\alpha\sin(n-1)\alpha\right)X^2 + \\ & \left(\frac{1}{2}\sin n\alpha + \frac{n}{2}\sin\alpha\cos(n-1)\alpha\right)X + \frac{n}{2}\sin\alpha\sin(n-1)\alpha + \cos n\alpha \end{aligned}$$

est le reste de de la division euclidienne de $P = (\cos\alpha + X\sin\alpha)^n$ par $\left(X^2+1\right)^2$.

Etude de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$

Théorème. Le corps $\mathbb{C}$ des nombres complexes est algébriquenment clos. En d'autres termes, tout polynôme de $\mathbb{C}[X]$.

Conséquences.
1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
2. Tout polynôme de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.
3. Un polynôme de degré n admet exactement n racines dans comptées autant de fois que la multiplicité des racines.
4. Soit $P \in \mathbb{C}[X]$, alors

$$P = \lambda(X-\alpha_1)^{s_1}(X-\alpha_2)^{s_2}\cdots(X-\alpha_k)^{s_k}$$

où $\lambda \in \mathbb{C}$, $\alpha_1, \alpha_2, \cdots \alpha_k \in \mathbb{C}$ et $k, s_1, s_2, \cdots s_k \in \mathbb{N}$.
Lemme

Soit $P \in \mathbb{C}[X]$, $\alpha \in \mathbb{C}-\mathbb{R}$ et $k \in \mathbb{N}^*$. Alors

$$\alpha \text{ est une racine d'ordre } k \text{ de } P \Longleftrightarrow \overline{\alpha} \text{ est une racine d'ordre } k \text{ de } \overline{P}.$$

Etude de $\mathbb{R}[X]$
Proposition. soit $P \in \mathbb{C}[X]$.

$$P \in \mathbb{R}[X] \Longleftrightarrow \left[\forall z \in \mathbb{C},\ P(\overline{z}) = \overline{P(z)}\right]$$

Proposition. soit $P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C}-\mathbb{R}$ et $k \in \mathbb{N}^*$. Pour que α soit un zéro de P d'ordre k (exactement k) il faut et il suffit que $\overline{\alpha}$ soit un zéro de P d'ordre k (exactement k).

Conséquences.
1. Un polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle.
2. Soit $P \in \mathbb{R}[X]$. Alors le nombre de racine non réelles est un nombre pair (car si α soit un zéro de P d'ordre k alors $\overline{\alpha}$ est aussi un zéro de P d'ordre k.

Théorème.Soit P un polynôme réel non constant. P est le produit de polynômes de degré

1 et de polynômes de degré 2 à discriminant strictement négatif. Donc il existe des réels $a_1, a_2, \cdots, a_r, b_1, b_2, \cdots, b_s, c_1, c_2, \cdots, c_s, \lambda$ et des entiers naturels $\alpha_1, \alpha_2, \cdots, \alpha_r, \beta_1, \beta_2, \cdots, \beta_s$ tels que pour tout $1 \leq j \leq s, b_j^2 - 4c_j < 0$ et

$$P = \lambda \prod_{i=1}^{r}(X-a_i)^{\alpha_i} \prod_{j=1}^{s}\left(X^2+b_jX+c_j\right)^{\beta_j}$$

On en déduit que $\deg(P) = \sum\limits_{i=1}^{r}\alpha_i + 2\sum\limits_{j=1}^{s}\beta_j$
Corollaire. Les polynômes irréductibles de $\mathbb{R}[X]$, sont :

1. Les polynômes du premier degré,

2. Les polynômes du second degré à discriminant strictement négatif.

Remarques.

1. Factoriser un polynôme c'est l'écrire comme produit de facteurs irréductibles.
2. Pour factoriser dans $\mathbb{R}[X]$ on peut "passer" par $\mathbb{R}[X]$ puis "marier" les conjuguées.

PGCD-PPCM

Définition : Soient $P, Q \in \mathbb{K}[X]$. Le plus grand commun diviseur unitaire à P et Q est un polynôme D de degré *le* plus grand possible qui divise à la fois P et Q. On note

$$D = PGCD(P, Q) = P \wedge Q.$$

Définition : Soient $P, Q \in \mathbb{K}[X]$. Le plus grand commun Multiple unitaire à P et Q est un polynôme M de degré *le* plus petit possible qui est multiple à la fois P et Q. On note

$$M = PPCM(P, Q) = P \vee Q.$$

Définition : Soient $P, Q \in \mathbb{K}[X]$. On dit que P et Q sont premiers entre eux lorsque

$$P \wedge Q = 1.$$

Théorème: (Identité de Bezout pour les polynômes) Soient $P, Q \in \mathbb{K}[X]$.

$$P \wedge Q = D \Longleftrightarrow \exists U, V \in \mathbb{K}[X] \text{ tels que } PU + QV = D.$$

En particulier

$$P \wedge Q = 1 \Longleftrightarrow \exists U, V \in \mathbb{K}[X] \text{ tels que } PU + QV = 1.$$

Théorème: Soient $P, Q \in \mathbb{K}[X]$.

$$\Delta \text{ diviseur commun à } P \text{ et } Q \Longleftrightarrow \Delta \text{ divise } D = PGCD(P, Q).$$

et

$$H \text{ diviseur commun à } P \text{ et } Q \Longleftrightarrow H \text{ est un multiple de } M = PPCM(P, Q).$$

Proposition : Soient $A, B, C \in \mathbb{K}[X]$.

1. Si $(A \wedge C = 1$ et $B \wedge C = 1)$ alors $(AB \wedge C = 1)$.
2. Si $(A \wedge B = 1)$ alors $(A^n \wedge B^n = 1)$.

3. Si $(B \wedge C = 1$ et C divise $AB)$ alors $(C$ divise $A)$.

Calcul du PGCD : Algorithme d'euclide

Proposition: Soient $P, Q \in \mathbb{K}[X]$ et R le reste de la division euclidienne de P par Q.Alors

$$P \wedge Q = Q \wedge R.$$

En d'autres termes l'ensemble des diviseurs communs à P et Q est égal à 'ensemble des diviseurs communs à Q et R.

Algotithme d'euclide : Soient $P, Q \in \mathbb{K}[X]$.

$$\begin{aligned}
P &= AQ + R_0 \text{ avec } \deg R_0 < \deg Q \\
Q &= A_1 R_0 + R_1 \text{ avec } \deg R_1 < \deg R_0 \\
R_0 &= A_2 R_1 + R_2 \text{ avec } \deg R_2 < \deg R_1 \\
R_1 &= A_3 R_2 + R_{{}_2} \text{ avec } \deg R_3 < \deg R_2 \\
&\vdots \\
R_{n-2} &= A_n R_{n-1} + R_n \text{ avec } \deg R_n < \deg R_{n-1} \\
&\vdots \\
R_{n+1} &= 0
\end{aligned}$$

Il en résulte que

$$P \wedge Q = Q \wedge R_0 = \cdots = R_n$$

En d'autres termes le dernier reste non nul dans l'algorithme d'Euclide fournit le $PGCD$ de P et Q.

Exercice

Soient

$$A = 4X^3 + 6X^2 - 22X - 12 \text{ et } B = X^6 - 8X^4 - 8X^2 - 9$$

Déterminer $A \wedge B$ et $A \vee B$.

Exercice (Solution)

Quand on veut calculer le $PGCD$ de deux polynômes, on se refère généralement à l'algorithme d'Euclide. L'ennui, c'est que les calculs sont ici fastidieux... Donc, soit le prof est cruel, ... etc.. soit il s'est trompe. Absurde donc (si, si!). Conclusion, il y a forcement une autre methode. La seule chance est qu'un de ces polynomes soit factorisable. On peut aller donc en toute confiance vers la recherche de racines evidentes. On voit que 2 est racine de A donc $(X-2)$ divise A et il en résulte après la division euclidienne de A par $(X-2)$ que

$$A = (X-2)(4X^2+14X+6) = 2(X-2)(X+3)(2X+1)$$

l s'agit de la decomposition de A en facteurs irreductibles.
Par ailleurs, puisque B est paire alors si α est une racine alors $-\alpha$ est aussi une racine; et on vérifie facilement que

$$B(-3)=0; B(-\frac{1}{2}) \neq 0 \text{ et } B(2) \neq 0$$

On verifie ainsi que -3 est la seule racine commune de B et par suite le $PGCD$ de A et B est donc $(X+3)$. Il en résulte que en effectuant la division euclidienne du produit AB par $(X+3)$ que

$$A \vee B = 4X^7 - 26X^6 + 62X^5 - 78X^4 + 58X^3 - 10X^2 - 10X + 12$$

Fractions rationnelles

I) Le corps $\mathbb{K}(X)$
1) L'ensemble $\mathbb{K}(X)$

Dans la pratique, une fraction rationnelle s'écrit,

$$\frac{A}{B}$$

où A et B sont des polynômes avec $B \neq 0$.
Cependant les régles de simplification des fractions imposent de ne pas distinguer les fractions

$$\frac{A}{B} \text{ et } \frac{PA}{PB}$$

où P est un polynôme quelconque non nul.
a) **Définition 1.** Une fraction rationnelle s'écrit sous la forme

$$F = \frac{A}{B}$$

où A et B sont des polynômes avec $B \neq 0$.
On définit sur l'ensemble $E = \mathbb{K}[X] \times \mathbb{K}[X]^*$ une relation $\mathcal{R}$ par

$$\forall (A_1, B_1) \in E \text{ et } \forall (A_2, B_2) \in E, \quad (A_1, B_1)\, \mathcal{R}\, (A_2, B_2) \Longleftrightarrow A_1B_2 = A_2B_1.$$

Proposition. La relation $\mathcal{R}$ est une relation d'équivalence sur E. On note $F = classe(A,B) = \{(C,D) \in E, (A,B)\mathcal{R}\,(C,D)\}$.

Notation. On note $\mathbb{K}(X)$ l'ensemble des fractions à une indéterminée et à coefficients dans $\mathbb{K}$.

Remarques. Soit $P \in \mathbb{K}[X]$, alors $P = \dfrac{P}{1} \in \mathbb{K}(X)$. Ainsi $\mathbb{K}[X] \subset \mathbb{K}(X)$.

On définit sur $\mathbb{K}(X)$ une addition par

$$\frac{A}{B}+\frac{C}{D}=\frac{AD+BC}{BD}\in\mathbb{K}(X).$$

Proposition. $(\mathbb{K}(X),+)$ est un groupe commutatif.

Démonstration.
De même on définit sur $\mathbb{K}(X)$ une multiplication par

$$\frac{A}{B}\times\frac{C}{D}=\frac{AC}{BD}\in\mathbb{K}(X).$$

Proposition. $(\mathbb{K}(X),+,\times)$ est un corps commutatif.

Démonstration. en exercice.

On définit sur $\mathbb{K}(X)$ une loi de composition externe par $\forall\lambda\in\mathbb{K}$

$$\lambda\cdot\left(\frac{A}{B}\right)=\frac{\lambda A}{B}\in\mathbb{K}(X).$$

2. Fractions irréductibles.

Définition. Soit $F=\dfrac{A}{B}\in\mathbb{K}(X)$. On dit que F est une fraction irréductible si et seulement si $A\wedge B=1$. On dit alors que $\dfrac{A}{B}$ est la forme réduite de F.

Exemples
-) $F=\dfrac{X^2+X-2}{X^2+4X+4}$
-) $F=\dfrac{X^7(X+1)}{X^3+2X}$

Proposition. Toute fraction rationnelle admet une forme réduite c'est-à-dire une écriture irréductible.
3.Degré d'une fraction rationnelle.
Définition. Soit $F=\dfrac{A}{B}\in\mathbb{K}(X)$. On appelle degré de F qu'on note $\deg(F)$ l'entier relatif $\deg(F)=\deg(A)-\deg(B)$.

Soient $F,G\in\mathbb{K}(X)$.
1.$\deg(F)\in\in\mathbb{Z}\cup\{-\infty\}$.
2. $\deg(F+G)\leq Max(\deg(F),\deg(G))$
3.$\deg(FG)=\deg(F)+\deg(F)$.
4. Par convention $\deg(0_{\mathbb{K}(X)})=-\infty$.

4. Dérivée formelle d'une fration rationnelle.

Définition. Soit $F = \dfrac{A}{B} \in \mathbb{K}(X)$. On appelle dérivée de F qu'on note F' la fraction rationnelle

$$F' = \left(\frac{A}{B}\right)' = \frac{A'B - AB'}{B^2}.$$

Proposition. Soient $F = \dfrac{A}{B} \in \mathbb{K}(X)$ et $G = \dfrac{C}{D} \in \mathbb{K}(X)$. Alors

i) $\left(\dfrac{A}{1}\right)' = A'$.

ii) $\left(\dfrac{A}{B} + \dfrac{C}{D}\right)' = \left(\dfrac{A}{B}\right)' + \left(\dfrac{C}{D}\right)'$.

iii) $\left(\dfrac{A}{B}\dfrac{C}{D}\right)' = \left(\dfrac{A}{B}\right)'\left(\dfrac{C}{D}\right) + \left(\dfrac{A}{B}\right)\left(\dfrac{C}{D}\right)'$.

Partie entière d'une fraction rationnelle.

Proposition-Définition. Soit $F = \dfrac{A}{B} \in \mathbb{K}(X)$. Il existe un unique polynôme et une unique fraction rationnelle G telle que

$$F = E + G \qquad \text{avec } \deg(G) < 0$$

Le polynôme E est appélé la partie entière (ou encore polynôme asymptote) de la fraction F.

Pôles et zéros d'une fraction rationnelle.

Définitions. Soit $F = \dfrac{A}{B} \in \mathbb{K}(X)$ tel que $A \wedge B = 1$.
On appelle zéro de F les racine de A.
On appelle pôle de F les racine de B.
L'ordre de multiplicité d'un zéro (respectivement d'un pôle) est l'ordre de multiplicité de ce zéro (respectivement de ce pôle) comme étant un zéro de A (respectivement d'un zéro de B).

Exemples :

1. $F = \dfrac{X^2 + 2X + 1}{X^2 + 1}$: les zéros : $1(double)$ et les pôles i et $-i(simples)$
2. $F = \dfrac{X^7(X + 1)}{X^3 - 1}$: les zéros : $0(d\prime ordre 7)$ et $-1(simple)$ et les pôles $j, \overline{j}$ et $1(simples)$

Décomposition en éléments simples d'une fraction rationnelle

Eléments simples.

Définition. Les fractions rationnelle de la forme $\dfrac{P}{Q^k}$ avec $\deg(P) < \deg(Q)$ et Q irréductible dans $\mathbb{K}[X]$ sont appelés les éléments simples de$\mathbb{K}(X)$.
Si Q est de degé l, on dit que la fration rationnelle est du $l^{ième}$ espèce

Les éléments simples de $\mathbb{C}(X)$

$\dfrac{\alpha}{(X-a)^k}$ avec $\alpha \in \mathbb{C}, a \in \mathbb{C}$ et $k \in \mathbb{N}^*$

Les éléments simples de $\mathbb{R}(X)$

$i)\dfrac{\alpha}{(X-a)^k}$ avec $\alpha \in \mathbb{R}, a \in \mathbb{R}$ et $k \in \mathbb{N}^*$

$ii)\dfrac{aX+b}{(X^2+cX+d)^k}$ avec $a, b \in \mathbb{R}, c, d \in \mathbb{R}$ tels que $c^2 - 4d < 0,$

Exemples.

Théorème. Toute fraction rationnelle irréductible se décompose de façon unique comme somme d'éléments simples et de sa partie entière, i.i. si $F = \dfrac{A}{B}$ avec $B = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_q^{\alpha_q}$ où $\forall 1 \leq i \leq q$, P_i est irréducible dans $\mathbb{K}[X]$ et $\alpha_i \in \mathbb{N}$ alors

$$F = E + \left(\sum_{i=1}^{q} \left(\sum_{j=1}^{\alpha_q} \frac{A_{ij}}{P_i^j} \right) \right) \text{ avec } \forall 1 \leq i \leq q \text{ et } \forall 1 \leq j \leq \alpha_q \text{ on a } \deg(A_{ij}) < \deg(P_i^j).$$

Si $\mathbb{K} = \mathbb{C}$ alors $B = (X-a_1)^{\alpha_1}(X-a_2)^{\alpha_2} \cdots (X-a_q)^{\alpha_q}$ et par suite

$$\begin{aligned} F &= E + \left[\frac{A_{11}}{X-a_1} + \frac{A_{12}}{(X-a_1)^2} + \cdots + \frac{A_{1\alpha_1}}{(X-a_1)^{\alpha_1}} \right] + \\ & \left[\frac{A_{21}}{X-a_2} + \frac{A_{22}}{(X-a_2)^2} + \cdots + \frac{A_{2\alpha_2}}{(X-a_2)^{\alpha_2}} \right] + \cdots \left[\frac{A_{q1}}{X-a_q} + \frac{A_{q2}}{(X-a_q)^2} + \cdots + \frac{A_{q\alpha_q}}{(X-a_q)^{\alpha_{q1}}} \right] \end{aligned}$$

Si $\mathbb{K} = \mathbb{R}$ alors $B = \prod_{i=1}^{N} (X-a_i)^{\alpha_i} \prod_{j=1}^{N'} (X^2 + b_j X + c_j)^{\beta_j}$ avec $1 \leq j \leq N', b_j^2 - 4c_j < 0$ alors

$$F = E + \left(\sum_{i=1}^{N} \left(\sum_{k=1}^{\alpha_i} \frac{A_{ik}}{(X-a_i)^k} \right) \right) + \left(\sum_{j=1}^{N'} \left(\sum_{k=1}^{\beta_j} \frac{\delta_{jk} X + \lambda_{jk}}{(X^2 + b_j X + c_j)^k} \right) \right).$$

Problème: comment calculer les coefficients ?

Méthodes pratiques de le décomposition en éléments simples d'une fraction rationnelle

Calculs des coefficients par dérivation.
a) le cas d'un pôle simple.

Soit $F = \dfrac{A}{B}$ une fraction rationnelle admettant a comme pôle simple. Alors il existe un polynôme Q tel que $B = (X-a)Q$ avec $Q(a) \neq 0$. D'après le théorème fondamental de la décomposition en éléments simples il existe $\lambda \in \mathbb{K}$ et $A_1 \in \mathbb{K}[X]$ tels que

$$F = \frac{\lambda}{X-a} + \frac{A_1}{Q}.$$

Cherchons λ.
On a $F = \dfrac{\lambda}{X-a} + \dfrac{A_1}{Q}$ donc $(X-a)\dfrac{A}{B} = \lambda + (X-a)\dfrac{A_1}{Q}$ ou encore $(X-a)\dfrac{A}{(X-a)Q} = \lambda + (X-a)\dfrac{A_1}{Q}$.
D'où $\dfrac{A}{Q} = \lambda + (X-a)\dfrac{A_1}{Q}$. Ainsi pour $X = a$, on obtient $\dfrac{A(a)}{Q(a)} = \lambda$.
Or $B = (X-a)Q$ donc $B' = (X-a)Q' + Q$. Finalement

$$\lambda = \frac{A(a)}{B'(a)}.$$

b) Le cas d'un pôle multiple

Soit $F = \dfrac{A}{B}$ une fraction rationnelle admettant a comme pôle d'ordre α. Alors il existe un polynôme Q tel que $B = (X-a)^\alpha Q$ avec $Q(a) \neq 0$. D'après le théorème fondamental de la décomposition en éléments simples il existe $\lambda_1, \lambda_2, \cdots, \lambda_\alpha \in \mathbb{K}$ et $A_1, E \in \mathbb{K}[X]$ tels que

$$F = E + \frac{\lambda_1}{(X-a)} + \frac{\lambda_2}{(X-a)^2} + \cdots + \frac{\lambda_\alpha}{(X-a)^\alpha} + \frac{A_1}{Q}.$$

Cherchons λ_α.
On a $F = \dfrac{\lambda_1}{(X-a)} + \dfrac{\lambda_2}{(X-a)^2} + \cdots + \dfrac{\lambda_\alpha}{(X-a)^\alpha} + \dfrac{A_1}{Q}$ donc $(X-a)^\alpha \dfrac{A}{B} = (X-a)^\alpha \left[\dfrac{\lambda_1}{(X-a)} + \dfrac{\lambda_2}{(X-a)^2} + \cdots \right.$
ou encore $\dfrac{A}{Q} = \lambda_1 (X-a)^{\alpha-1} + \lambda_2 (X-a)^{\alpha-2} + \cdots + \lambda_\alpha + (X-a)^\alpha \dfrac{A_1}{Q}$.
Ainsi pour $X = a$, on obtient $\dfrac{A(a)}{Q(a)} = \lambda_\alpha$.
Or $B = (X-a)^\alpha Q$ donc $B' = \alpha(X-a)^{\alpha-1}Q + (X-a)^\alpha Q'$. Finalement $B^{(\alpha)}(a) = \alpha! Q(a)$ et par suite

$$\lambda_\alpha = \frac{\alpha! A(a)}{B^{(\alpha)}(a)}.$$

Calculs des coefficients par division.
a)cas particulier.

Soit $F = \dfrac{A}{B}$ une fraction rationnelle admettant 0 comme pôle d'ordre α. Alors il existe un polynôme Q tel que $B = X^\alpha Q$ avec $Q(0) \neq 0$. D'après le théorème fondamental de la décomposition en éléments simples il existe $a_1, a_2, \cdots, a_\alpha \in \mathbb{K}$ et $A_1, E \in \mathbb{K}[X]$ tels que

$$F = E + \frac{a_1}{X} + \frac{a_2}{X^2} + \cdots + \frac{a_\alpha}{X^\alpha} + \frac{A_1}{Q}.$$

<u>Cherchons $a_1, a_2, \cdots, a_\alpha$.</u>

Effectuons la division suivant les puissances croissantes de A par Q à l'ordre $(\alpha - 1)$. Alors

$$A = \left(a_\alpha + a_{\alpha-1}X + a_{\alpha-2}X^2 + \cdots + a_1 X^{\alpha-1}\right) Q + X^\alpha R$$

donc

$$F = \frac{A}{B} = \frac{\left(a_\alpha + a_{\alpha-1}X + a_{\alpha-2}X^2 + \cdots + a_1 X^{\alpha-1}\right) Q + X^\alpha R}{X^\alpha Q} = \frac{a_\alpha}{X^\alpha} + \frac{a_{\alpha-1}}{X^{\alpha-1}} + \cdots + \frac{a_1}{X} + \frac{R}{Q}.$$

En vertu de l'unicité de la décomposition on obtient d'un seul coup $a_1, a_2, \cdots, a_\alpha$.

Exemple
$F = \dfrac{1}{X^3(X^2+X+1)}$
b) Le cas général.

Soit $F = \dfrac{A}{B}$ une fraction rationnelle admettant a comme pôle d'ordre α. Alors il existe un polynôme Q tel que $B = (X-a)^\alpha Q$ avec $Q(a) \neq 0$. D'après le théorème fondamental de la décomposition en éléments simples il existe $a_1, a_2, \cdots, a_\alpha \in \mathbb{K}$ et $A_1 \in \mathbb{K}[X]$ tels que

$$F = E + \frac{a_1}{(X-a)} + \frac{a_2}{(X-a)^2} + \cdots + \frac{a_\alpha}{(X-a)^\alpha} + \frac{A_1}{Q}.$$

<u>Cherchons $a_1, a_2, \cdots, a_\alpha$.</u>
Considèrons la fraction rationnelle $G(X) = F(X+a) = \dfrac{A(X+a)}{X^\alpha Q(X+a)}$.
On se ramène ainsi au cas précédent.

Exemple
$F = \dfrac{1}{X^3(1-X)^7}$.

3. Réduction du nombre des coefficients.
Soit $F = \dfrac{A}{B}$ une fraction rationnelle irréductible admettant a comme pôle d'ordre α. La partie polaire relative au pôle a s'écrit

$$\frac{\lambda_1}{(X-a)} + \frac{\lambda_2}{(X-a)^2} + \cdots + \frac{\lambda_\alpha}{(X-a)^\alpha} \text{ avec } \lambda_1, \lambda_2, \cdots, \lambda_\alpha \in \mathbb{K}.$$

a) Utilisation de la parité :

Si de plus F est paire ou impaire alors $(-a)$ est également un pôle de F, de même multiplicité que a.La partie relative à $(-a)$ s'écrit

$$\frac{\lambda'_1}{(X+a)} + \frac{\lambda'_2}{(X+a)^2} + \cdots + \frac{\lambda'_\alpha}{(X+a)^\alpha} \text{ avec } \lambda'_1, \lambda'_2, \cdots, \lambda'_\alpha \in \mathbb{K}.$$

On a alors, en vertu de l'unicité de la décomposition en éléments simples, les résultats suivants :

.) Si F est **paire** alors

$$\forall k \in \{1, 2, \cdots, \alpha\} \qquad \lambda'_k = (-1)^k \lambda_k$$

.) Si F est **impaire** alors

$$\forall k \in \{1, 2, \cdots, \alpha\} \qquad \lambda'_k = (-1)^{k-1} \lambda_k$$

a) Utilisation de la conjugaison :

On suppose que $F = \dfrac{A}{B}$ est une fraction à coefficients réels et $a \in \mathbb{C}/\mathbb{R}$. Alors la partie polaire relative au pôle (a) s'écrit

$$\frac{\lambda_1}{(X-a)} + \frac{\lambda_2}{(X-a)^2} + \cdots + \frac{\lambda_\alpha}{(X-a)^\alpha} \text{ avec } \lambda_1, \lambda_2, \cdots, \lambda_\alpha \in \mathbb{C}.$$

La partie polaire relative au pôle conjugué $(\overline{a})$ s'écrit

$$\frac{\beta_1}{(X-\overline{a})} + \frac{\beta_2}{(X-\overline{a})^2} + \cdots + \frac{\beta_\alpha}{(X-\overline{a})^\alpha} \text{ avec } \beta_1, \beta_2, \cdots, \beta_\alpha \in \mathbb{C}.$$

Puisque F est à coefficients réels, On a alors, en vertu de l'unicité de la décomposition en éléments simples,

$$\forall k \in \{1, 2, \cdots, \alpha\} \qquad \beta_k = \overline{\lambda_k}$$

Résumons-nous :

Pour décomposer sur $\mathbb{R}$ une fraction rationnelle irréductible F.

- On commence par chercher la partie entière E de F
  Ensuite on peut
- Si a est un pôle d'ordre k de la fraction, multiplier par $(X-a)^k$ puis remplacer X par a.
- Si a est un pôle d'ordre k de la fraction, c'est-à-dire $F = \frac{A}{(X-a)^k Q}$on effectue le changement de variable $Y = X - a$ puis effectuer la division suivant les puissances croissantes à l'ordre $(k-1)$ de A par Q.
- Multiplier par $(X^2 + pX + q)^\alpha$ puis remplacer X par une racine complexedu trinôme $X^2 + pX + q$.

- Des connaissances de parité permettent d'avoir des relations entre certains coefficients.
- Méthode des divisions euclidiennes successives.
- Remplacer X par un réel ou un complexe fixé distinct des pôles.
- Faire tendre X vers $+\infty$, après avoir multiplié par un facteur approprié.
- Faire la décomposition dans $\mathbb{C}$ puis regrouper les termes conjugés.