Les polynômes à coefficients réels ou complexes

Dans ce fichier, $\mathbb{K}$ **désignera le corps** $\mathbb{R}$ ou $\mathbb{C}$

I <u>Notion de</u> <u>polynôme à coefficients réels ou complexes</u>

Rappelons le résultat sur les fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$, J étant un intervalle quelconque de $\mathbb{R}$ non réduit à un point

$$\forall\, (\boldsymbol{a_0}, \boldsymbol{a_1}, \dots, \boldsymbol{a_n}) \in \mathbb{K}^{\boldsymbol{n+1}} :$$

$$\forall\, \boldsymbol{x} \in \boldsymbol{J} : \ \boldsymbol{a_0} + \boldsymbol{a_1}\, \boldsymbol{x} + \ \dots + \ \boldsymbol{a_n}\, \boldsymbol{x^n} = \boldsymbol{0} \ \Rightarrow \ \boldsymbol{a_0} = \boldsymbol{a_1} = \cdots = \boldsymbol{a_n} = \boldsymbol{0}$$

Autrement dit, si une fonction polynomiale à coefficients dans $\mathbb{K}$ s'annule sur un intervalle de $\mathbb{R}$ non réduit à un point alors tous ses coefficients sont nuls.

Un corollaire est que **si deux fonctions polynomiales coïncident sur un même intervalle réel non réduit à un point, alors elles ont le même degré et les mêmes coefficients.**

On est alors amené à définir une notion de polynôme qui se distingue de celle de fonction polynomiale, comme suit :

A toute fonction polynomiale f_P définie par $f_P(x) = a_0 + a_1\, x + \ \dots + \ a_n\, x^n$, on fait correspondre la suite de ses coefficients que l'on qualifie de polynôme : $P = (a_0, a_1, \dots, a_n, 0,0, \dots)$. On peut ainsi créer une correspondance bijective entre l'ensemble $\mathcal{F}_P(\mathbb{K}, \mathbb{K})$ des fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ et l'ensemble $\mathcal{F}_0(\mathbb{N}, \mathbb{K})$ des suites d'éléments de $\mathbb{K}$ nulles à partir d'un certain rang, telle que :

$$\Phi : \ \mathcal{F}_P(\mathbb{K}, \mathbb{K}) \to \mathcal{F}_0(\mathbb{N}, \mathbb{K})$$
$$f_P : \ x \to a_0 + a_1\, x + \ \dots + \ a_n\, x^n \to P = (a_0, a_1, \dots, a_n, 0,0, \dots)$$

Φ est en fait bien plus qu'une bijection car, d'une part $\mathcal{F}_P(\mathbb{K}, \mathbb{K})$ et $\mathcal{F}_0(\mathbb{N}, \mathbb{K})$ sont des espaces vectoriels sur le corps $\mathbb{K}$ et Φ vérifie :

$$\Phi\big(f_P + f_Q\big) = \Phi(f_P) + \Phi\big(f_Q\big)$$

$$\Phi(\lambda\, f_P) = \lambda\, \Phi(f_P)$$

Ce qui fait de Φ un isomorphisme d'espaces vectoriels.

D'autre part $(\mathcal{F}_P(\mathbb{K}, \mathbb{K}), +, \times)$ est un anneau commutatif. On définit alors le produit de deux polynômes P et Q par

$$\mathrm{P} \times \mathrm{Q} = \Phi\big(f_P \times f_Q\big)$$

On obtient ainsi, d'une part une structure d'anneau commutatif pour $(\mathcal{F}_0(\mathbb{N}, \mathbb{K}), +, \times)$, d'autre part :

$$\Phi\left(f_P \times f_Q\right) = \Phi(f_P) \times \Phi\left(f_Q\right)$$

Φ devient ainsi un isomorphisme d'anneaux.

Ajoutons une dernière propriété : La composée de deux polynôme définie par

$$\mathrm{P} \circ \mathrm{Q} = \Phi\left(f_P \circ f_Q\right)$$

Ainsi :

$$\Phi\left(f_P \circ f_Q\right) = \Phi(f_P) \circ \Phi\left(f_Q\right)$$

<u>Notations simplifiées</u> :

Pour plus de commodités, on convient de noter :

$$0 = \Phi(f_P : x \to 0) = (0,0,0 \dots)$$

$$1 = \Phi(f_P : x \to 1) = (1,0,0 \dots)$$

$$\mathrm{X} = \Phi(f_P : x \to x) = (0,1,0 \dots)$$

$$\mathrm{X}^2 = \Phi(f_P : x \to x^2) = (0,0,1,0 \dots)$$

$$\mathrm{X}^{\mathrm{n}} = \Phi(f_P : x \to x^n) = (0,0, \dots 0,1,0 \dots)$$

<u>Degré d'un polynôme</u> :

Le degré d'un polynôme est le rang à partir duquel tous les termes de la suite de coefficients sont nuls et auquel on enlève 1. Exemples :

$$d(0) = -1$$

$$d(1) = 0$$

$$d(\mathrm{X}) = 1$$

$$d(\mathrm{X}^2) = 2$$

$$d(1 + \mathrm{X} - \mathrm{X}^4) = 4$$

<u>Notation usuelle de l'ensemble des polynômes</u> :

$\mathcal{F}_0(\mathbb{N}, \mathbb{K})$ est noté plus simplement $\mathbb{K}[X]$ qu'il ne faut pas confondre avec $\mathbb{K}(X)$ qui est l'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$

On note, pour $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n. C'est un sous espace vectoriel de $\mathbb{K}[X]$ de dimension $n + 1$ et on a :

$$\boldsymbol{\mathbb{K}_n[X] = Vect[1, X, \dots X^n]}$$

La famille $(1, X, \dots X^n)$ qui est une base de $\mathbb{K}_n[X]$ est appelée **base canonique**.

Pour plus de commodité, on fera généralement apparaitre le symbole X dans la désignation d'un polynôme, ainsi :

$$P(X) = X + X^2$$

Cette notation est commode quand il s'agit de déterminer un polynôme composé par exemple $P(X)$ composé avec $Q(X) = 1 - X$.

$P(X) \circ Q(X)$ sera alors noté : $P\big(Q(X)\big)$ et défini par :

$$P(X) \circ Q(X) = P\big(Q(X)\big) = Q(X) + Q(X)^2 = 1 - X + (1 - X)^2$$

$$= 1 - X + 1 - 2\,X + X^2 = 2 - 3\,X + X^2$$

<u>Propriété de la composée</u> :

Une propriété de la composition des polynômes (fausse en général pour la composée des fonctions) :

$$\boxed{\begin{cases} \boldsymbol{P(X) \circ Q(X) = 0} \\ \boldsymbol{Q(X)\ non\ constant} \end{cases} \Rightarrow \boldsymbol{P(X) = 0}}$$

<u>Preuve</u>

Si $P(X) \circ Q(X) = 0$ alors :

$$\forall\, x \in \mathbb{K} : \ f_P \circ f_Q\,(x) = 0$$

$$\forall\, x \in \mathbb{K} : f_P\left(f_Q\,(x)\right) = 0$$

Or, f_Q n'étant pas une fonction polynomiale constante, $f_Q(\mathbb{K})$ contient au moins un intervalle J non réduit à un point (si $\mathbb{K} = \mathbb{C}$ tout réel y est en effet image d'au moins un complexe x par f_Q car la fonction polynômiale complexe $f_Q\,(x) - y$ admet au moins une racine complexe) et ainsi f_P s'annule sur un tel intervalle J donc est identiquement nulle d'où $P(X) = 0$

<u>Exemple d'usage de cette propriété</u> :

$$\boxed{\forall\, \boldsymbol{a} \in \mathbb{K} : \ \boldsymbol{P(X - a) = 0} \Leftrightarrow \boldsymbol{P(X) = 0}}$$

<u>Propriété du produit</u> :

Une propriété du produit des polynômes (fausse également pour le produit des fonctions) :

$$\boxed{\boldsymbol{P(X)\,Q(X) = 0} \Leftrightarrow \boldsymbol{P(X) = 0\ \ ou\ Q(X) = 0}}$$

<u>Preuve</u>

Seul le sens direct n'est pas trivial :

Si $P(X)\,Q(X) = 0$ et si $Q(X) \neq 0$ alors :

$$\forall x \in \mathbb{K} : \; f_P(x)\, f_Q\,(x) = 0$$

Or f_Q qui n'est pas identiquement nulle possède au moins un intervalle non réduit à un point sur lequel elle ne s'annule pas et ainsi f_P s'annule sur un tel intervalle donc est identiquement nulle d'où $P(X) = 0$

III Polynôme dérivé

1) Définitions

Soit un polynôme non nul de $\mathbb{K}[X]$:

$$P(X) = a_0 + a_1\,X + \; \dots + \; a_n\,X^n = (a_0, a_1, \dots, a_n, 0,0, \dots)$$

On définit le polynôme dérivé par :

$$P^{(1)}(X) = a_1 + 2\,a_2\,X \; + \; \dots + \; n\,a_n\,X^{n-1} = (a_1, 2\,a_2, \dots n\,a_n, 0,0,0, \dots)$$

On définit le polynôme dérivé du polynôme nul comme étant le polynôme nul

On note également :

$$P^{(0)}(X) = P(X)$$

$$P^{(2)}(X) = \left(P^{(1)}\right)^{(1)}(X)$$

$$P^{(3)}(X) = \left(P^{(2)}\right)^{(1)}(X)$$

Etc…

2) Théorème

Si deux polynômes ont même polynôme dérivé alors ils diffèrent d'une constante arbitraire.
Autrement dit :

$$\forall\, (\boldsymbol{P(X)}, \boldsymbol{Q(X)}) \in \mathbb{K}[\boldsymbol{X}]^{\mathbf{2}} : \; \boldsymbol{P^{(1)}(X)} = \boldsymbol{Q^{(1)}(X)} \Leftrightarrow \; \exists\, \boldsymbol{c} \in \mathbb{K} : \; \boldsymbol{P(X)} = \boldsymbol{Q(X)} + \boldsymbol{c}$$

Preuve :

Posons :

$$P(X) = a_0 + a_1\,X + \; \dots + \; a_n\,X^n$$

$$Q(X) = b_0 + b_1\,X + \; \dots + \; b_m\,X^m$$

Alors :

$$P^{(1)}(X) = a_1 + 2\,a_2\,X \; + \; \dots + \; n\,a_n\,X^{n-1}$$

$$Q^{(1)}(X) = b_1 + 2\,b_2\,X \; + \; \dots + \; m\,b_m\,X^{m-1}$$

Ainsi :

$$P^{(1)}(X) = Q^{(1)}(X) \Leftrightarrow \begin{cases} m-1 = n-1 \\ a_1 = b_1 \\ 2\,a_2 = 2\,b_2 \\ \vdots \\ n\,a_n = n\,b_n \end{cases} \Leftrightarrow P(X) - Q(X) = a_0 - b_0$$

Ce qui prouve le théorème

3) **Propriétés vis-à-vis des opérations** :

$$\forall\,(\boldsymbol{P(X)}, \boldsymbol{Q(X)}) \in \mathbb{K}[X]^2 : \begin{cases} (\boldsymbol{P}+\boldsymbol{Q})^{(1)}(\boldsymbol{X}) = \boldsymbol{P}^{(1)}(\boldsymbol{X}) + \boldsymbol{Q}^{(1)}(\boldsymbol{X}) \\ (\boldsymbol{P}\times\boldsymbol{Q})^{(1)}(\boldsymbol{X}) = \boldsymbol{P}^{(1)}(\boldsymbol{X})\,\boldsymbol{Q}(\boldsymbol{X}) + \boldsymbol{P}(\boldsymbol{X})\,\boldsymbol{Q}^{(1)}(\boldsymbol{X}) \end{cases}$$

Ces propriétés se vérifient aisément

4) Développement de Taylor

$$\forall\,\boldsymbol{P}(\boldsymbol{X}) \in \mathbb{K}_{\boldsymbol{n}}[\boldsymbol{X}]\,, \forall\,\boldsymbol{a} \in \mathbb{K} : \qquad \boldsymbol{P}(\boldsymbol{X}) = \sum_{\boldsymbol{k}=\boldsymbol{0}}^{\boldsymbol{n}} \frac{\boldsymbol{P}^{(\boldsymbol{k})}(\boldsymbol{a})}{\boldsymbol{k}!}\,(\boldsymbol{X}-\boldsymbol{a})^{\boldsymbol{k}} =$$

$$\boldsymbol{P}(\boldsymbol{a}) + \boldsymbol{P}^{(1)}(\boldsymbol{a})\,(\boldsymbol{X}-\boldsymbol{a}) + \frac{\boldsymbol{P}^{(2)}(\boldsymbol{a})}{\boldsymbol{2}!}\,(\boldsymbol{X}-\boldsymbol{a})^2 + \cdots + \frac{\boldsymbol{P}^{(\boldsymbol{n})}(\boldsymbol{a})}{\boldsymbol{n}!}\,(\boldsymbol{X}-\boldsymbol{a})^{\boldsymbol{n}}$$

Preuve :

Par récurrence sur n

Initialisation : pour $n = -1$ et $n = 0$

Si $n = -1$ ou $n = 0$, $P(X)$ est un polynôme constant éventuellement nul et on a :

$$\forall\, a \in \mathbb{K} :\ P(X) = P(a)$$

Hérédité : Soit $n \in \mathbb{N}$ tel que la propriété soit vraie et soit $P(X) \in \mathbb{K}_{n+1}[X]$ alors $P^{(1)}(X) \in \mathbb{K}_n[X]$ donc :

$$P^{(1)}(X) = \sum_{k=0}^{n} \frac{\left(P^{(1)}\right)^{(k)}(a)}{k!}\,(X-a)^k$$

Donc

$$P^{(1)}(X) = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} \ (X-a)^k$$

$$P^{(1)}(X) = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} \left(\frac{(X-a)^{k+1}}{k+1}\right)^{(1)}$$

$$P^{(1)}(X) = \left(\sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} \ \frac{(X-a)^{k+1}}{k+1}\right)^{(1)}$$

$$P^{(1)}(X) = \left(\sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{(k+1)!} \ (X-a)^{k+1}\right)^{(1)}$$

D’où , en vertu du théorème précédent :

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{(k+1)!} \ (X-a)^{k+1} + c$$

Et en évaluant les deux membres en a :

$$c = P(a)$$

Finalement, en changeant l’indice k en $k-1$:

$$P(X) = P(a) + \sum_{k=1}^{n+1} \frac{P^{(k)}(a)}{k!} \ (X-a)^k = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!} \ (X-a)^k$$

Ce qui prouve la propriété au rang $n+1$ et achève la récurrence.

II <u>Division euclidienne des polynomes</u>

En notant $\mathbb{K}^*[X]$ l’ensemble des polynômes non nuls de $\mathbb{K}[X]$

$$\boxed{\forall \left(\boldsymbol{A(X)}, \boldsymbol{B(X)}\right) \in \ \mathbb{K}[\boldsymbol{X}] \times \mathbb{K}^*[\boldsymbol{X}] : \ \exists \ ! \ \left(\boldsymbol{Q(X)}, \boldsymbol{R(X)}\right) \in \ (\mathbb{R}[\boldsymbol{X}])^2 : \begin{cases} \boldsymbol{0} \leq \boldsymbol{d}\left(\boldsymbol{R(X)}\right) < d\left(\boldsymbol{B(X)}\right) \\ \boldsymbol{A(X)} = \boldsymbol{B(X)} \ \boldsymbol{Q(X)} + \boldsymbol{R(X)} \end{cases}}$$

<u>Preuve</u> :

Commençons par prouver l’existence par récurrence sur le degré n de $A(X)$

<u>Initialisation</u> : pour $n = -1$ et $n = 0$

On a alors : $A(X) = \ a_0$

Distinguons deux cas ;

<u>1er cas : $a_0 = 0$</u> :

Posons alors

$$Q(X) = 0, \qquad R(X) = 0$$

Alors :

$$A(X) = B(X)\,Q(X) + R(X)$$

Et, puisque $B(X) \neq 0$:

$$d\big(R(X)\big) = -1 < d\big(B(X)\big)$$

<u>2ème cas : $a_0 \neq 0$</u>

Distinguons encore deux sous-cas :

1er sous-cas : $d\big(B(X)\big) = 0$ soit $B(X) = b_0 \neq 0$

Posons alors :

$$Q(X) = \frac{a_0}{b_0}, \qquad R(X) = 0$$

Il vient :

$$A(X) = B(X)\,Q(X) + R(X)$$

$$d\big(R(X)\big) = -1 < d\big(B(X)\big)$$

2ème sous-cas : $d\big(B(X)\big) > 0$

Posons alors :

$$Q(X) = 0, \qquad R(X) = a_0$$

Il vient :

$$A(X) = B(X)\,Q(X) + R(X)$$

$$d\big(R(X)\big) = 0 < d\big(B(X)\big)$$

<u>Hérédité</u> Soit $n \in \mathbb{N}$ tel que la propriété énoncée soit vraie pour tous les polynômes $A(X)$ de degré inférieur ou égal à n. Soit alors un polynôme non nul $A(X)$ de degré $n+1$ et un polynôme non nul quelconque $B(X)$ de degré m. Posons :

$$A(X) = a_0 + a_1\,X + \cdots + a_{n+1}\,X^{n+1}$$

$$B(X) = b_0 + b_1 X + \cdots + b_m X^m$$

On alors $a_{n+1} \neq 0$ et $b_m \neq 0$ et :

Distinguons deux cas :

1^er cas : $n+1 < m$

Posons alors :

$$Q(X) = 0, \qquad R(X) = A(X)$$

Il vient :

$$A(X) = B(X)\,Q(X) + R(X)$$

$$d\big(R(X)\big) = n+1 < m = d\big(B(X)\big)$$

2^ème cas : $n+1 \geq m$

Posons alors :

$$A_1(X) = A(X) - \frac{a_{n+1}}{b_m} B(X)$$

On a :

$$d\big(A_1(X)\big) \leq n$$

On peut alors appliquer l'hypothèse de récurrence à ce nouveau polynôme :

$$\exists\,!\ \big(Q_1(X), R_1(X)\big) \in \ (\mathbb{K}[X])^2 : \begin{cases} \ 0 \leq d\big(R_1(X)\big) < d\big(B(X)\big) \\ A_1(X) = B(X)\,Q_1(X) + R_1(X) \end{cases}$$

Or :

$$A(X) = \frac{a_{n+1}}{b_m} B(X) + A_1(X)$$

Donc :

$$A(X) = \frac{a_{n+1}}{b_m} B(X) + B(X)\,Q_1(X) + R_1(X)$$

$$A(X) = B(X)\left(\frac{a_{n+1}}{b_m} + Q_1(X)\right) + R_1(X)$$

En posant finalement:

$$Q(X) = \frac{a_{n+1}}{b_m} + Q_1(X), \ \ R(X) = R_1(X)$$

on voit que la propriété est vérifiée au rang $n+1$, ce qui achève la preuve de l'existence. Voyons maintenant l'unicité :

Supposons que l'on ait :

$$A(X) = B(X)\,Q(X) + R(X) = B(X)\,Q_1(X) + R_1(X)$$

Avec :

$$\begin{cases} 0 \leq d\big(R(X)\big) < d\big(B(X)\big) \\ 0 \leq d\big(R_1(X)\big) < d\big(B(X)\big) \end{cases}$$

Alors :

$$B(X)\,\big(Q(X) - Q_1(X)\big) = R_1(X) - R(X)$$

Or :

$$d\big(R_1(X) - R(X)\big) \leq max\left(d\big(R(X)\big), d\big(R_1(X)\big)\right) < d\big(B(X)\big)$$

Supposons par l'absurde : $Q(X) - Q_1(X) \neq 0$ alors :

$$d\left(B(X)\,\big(Q(X) - Q_1(X)\big)\right) = d\big(B(X)\big) + d\left(\big(Q(X) - Q_1(X)\big)\right)$$

et :

$$d\big(B(X)\big) + d\left(\big(Q(X) - Q_1(X)\big)\right) = d\big(R_1(X) - R(X)\big) < d\big(B(X)\big)$$

Ce qui est absurde donc :

$$Q(X) - Q_1(X) = 0$$

Et

$$R_1(X) - R(X) = 0$$

Ce qui prouve l'unicité.

III <u>Diviseur d'un polynôme, racine, ordre de multiplicité</u>

1) <u>Diviseur d'un polynôme</u>

Soit $\big(A(X), B(X)\big) \in \mathbb{K}[X] \times \mathbb{K}^*[X]$ on dit que $B(X)$ est un diviseur de $A(X)$ s'il existe un polynôme $Q(X)$ tel que : $A(X) = B(X)\,Q(X)$, autrement dit si le reste $R(X)$ dans la division euclidienne de $A(X)$ par $B(X)$ est nul.

Nous écrirons la définition sous le code mathématique suivant :

$$\boxed{\forall \big(\boldsymbol{A(X)}, \boldsymbol{B(X)}\big) \in \mathbb{K}[\boldsymbol{X}] \times \mathbb{K}^*[\boldsymbol{X}] : \boldsymbol{A(X)}/\boldsymbol{B(X)} \Leftrightarrow \exists\, \boldsymbol{Q(X)} \in \mathbb{K}[\boldsymbol{X}] : \boldsymbol{A(X)} = \boldsymbol{B(X)}\,\boldsymbol{Q(X)}}$$

Exemples :

a) Un polynôme constant non nul divise tout polynôme car :

$$\forall\, \boldsymbol{c} \in \mathbb{K}, \forall\, \boldsymbol{A(X)} \in \mathbb{K}[\boldsymbol{X}] :\ \boldsymbol{A(X)} = \boldsymbol{c}\left(\frac{\mathbf{1}}{\boldsymbol{c}}\, \boldsymbol{A(X)}\right)$$

b) Tout polynôme non nul divise le polynôme nul

c) $X - 1$ divise $X^2 - 1$ car : $X^2 - 1 = (X - 1)\,(X + 1)$

2) **Racine d'un polynôme** :

Définition

Soit $\boldsymbol{a} \in \mathbb{R}$ et $\boldsymbol{A(X)} \in \mathbb{K}[\boldsymbol{X}]$ on dit que $\boldsymbol{a}$ est racine de $\boldsymbol{A(X)}$ si $\boldsymbol{A(a)} = \mathbf{0}$

Théorème :

$$\forall\, \boldsymbol{A(X)} \in \mathbb{K}^*[\boldsymbol{X}] :\ \boldsymbol{A(a)} = \mathbf{0} \Leftrightarrow \boldsymbol{X} - \boldsymbol{a} \,/\, \boldsymbol{A(X)}$$

Autrement dit, pour qu'un nombre $\boldsymbol{a}$ réel ou complexe soit racine d'un polynôme il faut et il suffit que ce polynôme soit divisible par le polynôme $\boldsymbol{X} - \boldsymbol{a}$

Preuve :

Commençons par établir un résultat préliminaire :

La division euclidienne de $A(X)$ par $X - a$ s'écrit :

$$A(X) = (X - a)\, Q(X) + R(X)$$

Avec :

$$d\big(R(X)\big) < d(X - a) = 1$$

Donc $R(X)$ est un polynôme constant. Or :

$$A(a) = (a - a)\, Q(a) + R(a)$$

Soit :

$$A(a) = R(a)$$

Il vient alors :

$$\boldsymbol{A(X)} = (\boldsymbol{X} - \boldsymbol{a})\, \boldsymbol{Q(X)} + \boldsymbol{A(a)}$$

La preuve du théorème en découle :

Si $A(a) = 0$ il est clair que $X - a$ divise $A(X)$

Réciproquement, si $X-a$ divise $A(X)$ alors il existe un polynôme $Q_1(X)$ tel que :

$$A(X)=(X-a)\,Q_1(X)$$

Donc :

$$(X-a)\,Q_1(X)=(X-a)\,Q(X)+A(a)$$

En particulier :

$$(a-a)\,Q_1(a)=(a-a)\,Q(a)+A(a)$$

Donc $A(a)=0$

3) <u>Ordre de multiplicité d'une racine</u>

<u>Définition</u>

Soit $\boldsymbol{a}\in\mathbb{R}$ et $\boldsymbol{P(X)}\in\mathbb{K}^*[\boldsymbol{X}]$ alors l'ordre de multiplicité de $\boldsymbol{a}$ dans $\boldsymbol{P(X)}$ est le plus grand entier naturel $\boldsymbol{m}$ tel que $(\boldsymbol{X}-\boldsymbol{a})^{\boldsymbol{m}}$ divise $\boldsymbol{P(X)}$. Nous le noterons : $\boldsymbol{Ord(a,P(X))}$

<u>Théorème</u> :

si $\boldsymbol{m}\neq\boldsymbol{0}$:

$$\boldsymbol{Ord\big(a,P(X)\big)=m}\iff\begin{cases}\boldsymbol{P(a)=0}\\ \boldsymbol{P^{(1)}(a)=0}\\ \vdots\\ \boldsymbol{P^{(m-1)}(a)=0}\\ \boldsymbol{P^{(m)}(a)\neq 0}\end{cases}$$

<u>Preuve</u> **:**

Notons en préliminaire que :

$$Ord\big(a,P(X)\big)=m\iff\exists\, Q(X)\in\ \mathbb{R}[X]:\ \begin{cases}P(X)=(X-a)^m\,Q(X)\\ Q(a)\neq 0\end{cases}$$

$(\Rightarrow)$ Si $Ord\big(a,P(X)\big)=m$ alors d'une part :

$$\begin{cases}P(X)=(X-a)^m\,Q(X)\\ Q(a)\neq 0\end{cases}$$

D'autre part, en utilisant le développement de Taylor :

$$P(X)=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}\,(X-a)^k$$

Ainsi :

$$(X-a)^m\,Q(X)=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}\,(X-a)^k$$

Donc :

$$(X-a)^m\,Q(X)=\sum_{k=0}^{m-1}\frac{P^{(k)}(a)}{k!}\,(X-a)^k+\sum_{k=m}^{n}\frac{P^{(k)}(a)}{k!}\,(X-a)^k$$

Or :

$$\sum_{k=m}^{n}\frac{P^{(k)}(a)}{k!}\,(X-a)^k=(X-a)^m\sum_{k=m}^{n}\frac{P^{(k)}(a)}{k!}\,(X-a)^{k-m}=(X-a)^m\,Q_1(X)$$

Donc :

$$(X-a)^m\,Q(X)=\sum_{k=0}^{m-1}\frac{P^{(k)}(a)}{k!}\,(X-a)^k+(X-a)^m\,Q_1(X)$$

Soit encore :

$$(X-a)^m\,(Q(X)-Q_1(X))=\sum_{k=0}^{m-1}\frac{P^{(k)}(a)}{k!}\,(X-a)^k$$

Or si $Q(X)-Q_1(X)\neq 0$ le polynôme du membre de gauche est de degré supérieur ou égal à m et celui du membre de droite de degré strictement inférieur à m, ce qui est absurde, donc

$$Q(X)-Q_1(X)=0$$

Et :

$$\sum_{k=0}^{m-1}\frac{P^{(k)}(a)}{k!}\,(X-a)^k=0$$

On en déduit, par propriété de la composition :

$$\sum_{k=0}^{m-1}\frac{P^{(k)}(a)}{k!}\,X^k=0$$

Puis :

$$\forall\,k\in[\![0;m-1]\!]\quad P^{(k)}(a)=0$$

$(\Leftarrow)$

En utilisant le développement de Taylor on a :

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}\,(X-a)^k = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}\,(X-a)^k$$

$$= (X-a)^m \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}\,(X-a)^{k-m}$$

Donc :

$$P(X) = (X-a)^m\, Q(X)$$

Avec :

$$Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$$

4) <u>Nombre de racines</u>

Tout polynôme non nul $P(X)$ de $\mathbb{K}[X]$ de degré n admet au plus n racines distinctes. S'il admet exactement n racines distinctes $a_1, a_2, \dots, a_n$ alors :

$$\exists\, c \in \mathbb{K} : P(X) = c\,(X-a_1)\,(X-a_2)\dots(X-a_n)$$

<u>Preuve</u>

Soit un polynôme $P(X)$ de $\mathbb{K}[X]$ ayant exactement n racines distinctes $a_1, a_2, \dots, a_n$ alors :

$$\exists\, Q_1(X) \in \mathbb{K}[X] : P(X) = (X-a_1)\,Q_1(X)$$

a_2 étant racine, on en déduit :

$$(a_2 - a_1)\,Q_1(a_2) = 0$$

Donc :

$$Q_1(a_2) = 0$$

Et :

$$\exists\, Q_2(X) \in \mathbb{K}[X] : Q_1(X) = (X-a_2)\,Q_2(X)$$

Soit :

$$P(X) = (X-a_1)\,(X-a_2)\,Q_2(X)$$

Par une récurrence évidente, on aboutit à l'existence d'une suite de polynômes
$Q_1(X), Q_2(X), \dots, Q_n(X)$ telle que :

$$Q_{k+1}(X) = (X - a_k)\, Q_k(X)$$

Ainsi :

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

En prenant les degrés des deux membres, on en déduit :

$$n = n + d\big(Q_n(X)\big)$$

Soit :

$$d\big(Q_n(X)\big) = 0$$

Ainsi :

$$\exists\, c \in \mathbb{R} :\ Q_n(X) = c$$

Cette démonstration prouve également qu'un polynôme de degré n ne peut avoir plus de n racines distinctes

IV <u>Théorème de bezout</u> :

<u>Définition</u> : **polynômes premiers entre eux**

Deux polynômes $\boldsymbol{A(X)}$ et $\boldsymbol{B(X)}$ sont dits premiers entre eux s'il n'existe aucun polynôme de degré supérieur ou égal à 1 qui divise à la fois $\boldsymbol{A(X)}$ et $\boldsymbol{B(X)}$. En utilisant la définition du PGCD de deux polynômes donnée plus loin, cela revient à dire que le PGCD de $\boldsymbol{A(X)}$ et $\boldsymbol{B(X)}$ noté $\boldsymbol{A(X) \wedge B(X)}$ est égal à 1.

<u>Théorème</u> 1:

$$\forall\, \big(\boldsymbol{A(X)}, \boldsymbol{B(X)}\big) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{2}} :$$

$$\boldsymbol{A(X) \wedge B(X) = 1} \Leftrightarrow\ \exists\, \big(\boldsymbol{U(X)}, \boldsymbol{V(X)}\big) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{2}} :\ \boldsymbol{A(X)\, U(X) + B(X)\, V(X) = 1}$$

<u>Corollaire 1</u> :

$$\forall\, (\boldsymbol{A(X)}, \boldsymbol{B(X)}, \boldsymbol{D(X)}) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{3}} :$$

$$\exists\, \big(\boldsymbol{A_1(X)}, \boldsymbol{B_1(X)}\big) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{2}} :\ \begin{cases} \boldsymbol{A(X) = D(X)\, A_1(X)} \\ \boldsymbol{B(X) = D(X)\, B_1(X)} \\ \boldsymbol{A_1(X)\ et\ B_1(X)\ premiers\ entre\ eux} \end{cases}$$

$$\Rightarrow\ \exists\, \big(\boldsymbol{U(X)}, \boldsymbol{V(X)}\big) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{2}} :\ \boldsymbol{A(X)\, U(X) + B(X)\, V(X) = D(X)}$$

<u>Corollaire 1bis</u> :

$$\forall\, (\boldsymbol{A(X)}, \boldsymbol{B(X)}, \boldsymbol{C(X)}) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{3}} :$$

$$\begin{cases} \boldsymbol{A(X) \wedge B(X) = 1} \\ \boldsymbol{A(X) / B(X)\, C(X)} \end{cases} \Rightarrow\ \boldsymbol{A(X) /\, C(X)}$$

Et en version plus générale :

<u>Définition</u> : **polynômes premiers dans leur ensemble**

$\boldsymbol{n}$ polynômes $\boldsymbol{A_1(X), A_2(X), \dots A_n(X)}$ sont dits premiers dans leur ensemble s'il n'existe aucun polynôme de degré supérieur ou égal à 1 qui divise chacun d'eux. En utilisant la définition du PGCD de $\boldsymbol{n}$ polynômes donnée plus loin, cela revient à dire que le PGCD des $\boldsymbol{n}$ polynômes noté $\boldsymbol{A_1(X) \wedge A_2(X) \wedge \dots A_n(X)}$ est égal à 1.

<u>Théorème</u> 2:

$$\forall \left(\boldsymbol{A_1(X), A_2(X), \dots A_n(X)}\right) \in (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n}} :$$

$$\boldsymbol{A_1(X) \wedge A_2(X) \wedge \dots A_n(X) = 1}$$

$$\Leftrightarrow \exists \left(\boldsymbol{U_1(X), U_2(X), \dots U_n(X)}\right) \in (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n}} : \boldsymbol{A_1(X)\, U_1(X) + A_2(X)\, U_2(X) + \cdots A_n(X)\, U_n(X) = 1}$$

<u>Corollaire</u> 2 :

$$\forall \left(\boldsymbol{A_1(X), A_2(X), \dots A_n(X), D(X)}\right) \in (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n+1}} :$$

$$\exists \left(\boldsymbol{Q_1(X), Q_2(X), \dots Q_n(X)}\right) \in (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n}} \begin{cases} \boldsymbol{A_1(X) = D(X)\, Q_1(X)} \\ \boldsymbol{A_2(X) = D(X)\, Q_2(X)} \\ \vdots \\ \boldsymbol{A_n(X) = D(X)\, Q_n(X)} \\ \boldsymbol{Q_1(X) \wedge Q_2(X) \wedge \dots Q_n(X) = 1} \end{cases} \Rightarrow$$

$$\exists \left(\boldsymbol{U_1(X), U_2(X), \dots U_n(X)}\right) \in (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n}} : \boldsymbol{A_1(X)\, U_1(X) + A_2(X)\, U_2(X) \dots A_n(X)\, U_n(X) = D(X)}$$

<u>Preuve du théorème 1</u>

$(\Leftarrow)$ Supposons :

$$\exists \left(U(X), V(X)\right) \in (\mathbb{K}[X])^2 : A(X)\, U(X) + B(X)\, V(X) = 1$$

Soit alors $P(X)$ un diviseur commun de $A(X)$ et $B(X)$ alors :

$$\exists \left(R(X), S(X)\right) \in (\mathbb{K}[X])^2 : \begin{cases} A(X) = P(X)\, R(X) \\ B(X) = P(X)\, S(X) \end{cases}$$

Donc :

$$P(X)\, R(X)\, U(X) + P(X)\, S(X)\, V(X) = 1$$

Soit :

$$P(X)\left(R(X)\, U(X) + S(X)\, V(X)\right) = 1$$

Donc $P(X)$ est un diviseur de 1 d'où $P(X)$ est un polynôme de degré 0 donc une constante non nulle.

$(\Rightarrow)$ Supposons $A(X)$ et $B(X)$ premiers entre eux. Considérons l'ensemble suivant, où $c(P(X))$ désigne le coefficient de plus haut rang de $P(X)$ ou encore coefficient du terme de plus haut degré :

$$\mathbb{E} = \left\{ P(X) \in \mathbb{K}[X] : \left\{ \begin{array}{c} \exists \left(U(X), V(X)\right) \in (\mathbb{K}[X])^2 : P(X) = A(X)\, U(X) + B(X)\, V(X) \\ P(X) \neq 0 \\ c(P(X)) = 1 \end{array} \right. \right\}$$

Les polynômes ayant un coefficient de plus haut rang égal à 1, comme ceux de $\mathbb{E}$, seront qualifiés d'**unitaires** par la suite

Nous pouvons alors définir :

$$n = \min_{\mathbb{E}} \{ d\left(P(X)\right) \}$$

Soit alors $P_0(X) = A(X)\, U_0(X) + B(X)\, V_0(X) \in \mathbb{E}$ tel que : $d\left(P_0(X)\right) = n$

Nous allons montrer que $P_0(X)$ est égal à 1 en prouvant qu'il divise à la fois $A(X)$ et $B(X)$

La division euclidienne de $A(X)$ par $P_0(X)$ s'écrit :

$$A(X) = P_0(X)\, Q(X) + R(X), \quad d\left(R(X)\right) < d\left(P_0(X)\right)$$

Supposons par l'absurde que $R(X) \neq 0$, alors :

$$R(X) = A(X) - P(X)\, Q(X) = A(X) - \left(A(X)\, U_0(X) + B(X)\, V_0(X)\right) Q(X)$$

$$= \left(1 - U_0(X)\, Q(X)\right) A(X) + \left(-V_0(X)\, Q(X)\right) B(X)$$

Donc $R(X) \in \mathbb{E}$ mais $d\left(R(X)\right) < n$ ce qui est absurde d'où $R(X) = 0 \ et \ P_0(X)$ divise $A(X)$

Un même raisonnement montre que $P_0(X)$ divise $B(X)$, ce qui prouve que $P_0(X) = 1$

<u>Preuve du corollaire 1</u>

D'après le théorème 1 :

$$\exists \left(U(X), V(X)\right) \in (\mathbb{K}[X])^2 : A_1(X)\, U(X) + B_1(X)\, V(X) = 1$$

D'où , en multipliant les deux membres par $D(X)$:

$$D(X)\, A_1(X)\, U(X) + D(X)\, B_1(X)\, V(X) = D(X)$$

Soit :

$$A(X)\, U(X) + B(X)\, V(X) = D(X)$$

Preuve du corollaire 1bis

D'après le théorème 1

$$\exists \left(U(X), V(X)\right) \in (\mathbb{K}[X])^2 : A(X)\,U(X) + B(X)\,V(X) = 1$$

Multiplions les deux membres par $C(X)$:

$$A(X)\,C(X)\,U(X) + B(X)\,C(X)\,V(X) = C(X)$$

Et écrivons que $A(X)$ divise $B(X)\,C(X)$:

$$A(X)\,Q(X) = B(X)\,C(X)$$

D'où :

$$A(X)\,C(X)\,U(X) + A(X)\,Q(X)\,V(X) = C(X)$$

$$A(X)\left(C(X)U(X) + Q(X)\,V(X)\right) = C(X)$$

Donc $A(X)$ divise $C(X)$

Preuve du théorème 2

$(\Leftarrow)$ Analogue à celle du théorème 1

$(\Rightarrow)$ Par récurrence sur n

L'initialisation a été faite pour $n = 2$

Voyons l'hérédité. Soit $n \geq 2$ tel que la propriété soit vraie alors :

Soit $\left(A_1(X), A_2(X), \dots A_{n+1}(X)\right) \in (\mathbb{K}[X])^n : A_1(X) \wedge A_2(X) \wedge \dots A_{n+1}(X) = 1$

Soit $D(X)$ un **diviseur maximal commun** à $A_1(X), A_2(X), \dots A_n(X)$ c'est-à-dire tel que :

$$\exists \left(Q_1(X), Q_2(X), \dots Q_n(X)\right) \in (\mathbb{K}[X])^n \begin{cases} A_1(X) = D(X)\,Q_1(X) \\ A_2(X) = D(X)\,Q_2(X) \\ \vdots \\ A_n(X) = D(X)\,Q_n(X) \\ Q_1(X) \wedge Q_2(X) \wedge \dots Q_n(X) = 1 \end{cases}$$

Alors :

$$D(X) \wedge A_{n+1}(X) = 1$$

On en déduit d'après le théorème 1 :

$$\exists \left(U(X), V(X)\right) \in (\mathbb{K}[X])^2 : D(X)\,U(X) + A_{n+1}(X)\,V(X) = 1$$

L'hypothèse de récurrence donne alors :

$$\exists\ \big(U_1(X), U_2(X), \dots, U_n(X)\big) \in\ (\mathbb{K}[X])^n :$$

$$Q_1(X)\ U_1(X) + Q_2(X)\ U_2(X) + \cdots + Q_n(X)\ U_n(X) = 1$$

Soit :

$$D(X)\ Q_1(X)\ U_1(X) + D(X)\ Q_2(X)\ U_2(X) + \cdots + D(X)\ Q_n(X)\ U_n(X) = D(X)$$

Ou encore :

$$A_1(X)\ U_1(X) + A_2(X)\ U_2(X)\ + \cdots + A_n(X)\ U_n(X)\ = D(X)$$

On en déduit :

$$A_1(X)\ U_1(X)\ U(X) + A_2(X)\ U_2(X)\ U(X) + \cdots + A_n(X)\ U_n(X)\ U(X) +\ A_{n+1}(X)\ V(X) = 1$$

Ce qui prouve la propriété au rang $n+1$

<u>Preuve du corollaire 2</u>

Déjà faite dans celle du théorème 2 :

V <u>PGCD et PPCM de deux polynômes</u>

Pour deux polynômes non nuls $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ considérons les ensembles suivants :

$$\mathfrak{D} = \left\{ P(X) \in \mathbb{K}[X] : \begin{cases} P(X)/\ A(X) \\ P(X)/\ B(X)\ ) \\ c\big(P(X)\big) = 1 \end{cases} \right\}$$

$$\mathcal{M} = \left\{ P(X) \in \mathbb{K}[X] : \begin{cases} A(X)/\ P(X) \\ B(X)/\ P(X)\ ) \\ c\big(P(X)\big) = 1 \end{cases} \right\}$$

Où $c\big(P(X)\big)$ désigne le coefficient du terme de plus haut degré de $P(X)$

Notons que $\mathfrak{D}$ est l'ensemble des diviseurs communs à $A(X)$ et $B(X)$ de coefficient de plus haut degré égal à 1 et $\mathcal{M}$ est l'ensemble des multiples communs à $A(X)$ et $B(X)$ de coefficient de plus haut degré égal à 1.

Nous pouvons alors définir :

$$\boldsymbol{n = max_{\mathfrak{D}}\{d\big(P(X)\big)\}}$$

$$\boldsymbol{m = min_{\mathcal{M}}\{d\big(P(X)\big)\}}$$

Il existe alors un unique polynôme $\boldsymbol{D(X)}$ de $\mathfrak{D}$ de degré $\boldsymbol{n}$ et un unique polynôme $\boldsymbol{M(X)}$ de $\boldsymbol{\mathcal{M}}$ de degré $\boldsymbol{m}$

$\boldsymbol{D(X)}$ est appelé PGCD de $\boldsymbol{A(X)}$ et $\boldsymbol{B(X)}$ et nous le noterons $\boldsymbol{A(X) \wedge B(X)}$

$\boldsymbol{M(X)}$ est appelé PPCM de $\boldsymbol{A(X)}$ et $\boldsymbol{B(X)}$ et nous le noterons $\boldsymbol{A(X) \vee B(X)}$

De plus si :

$$\begin{cases} \boldsymbol{A(X) = D(X)\,A_1(X)} \\ \boldsymbol{B(X) = D(X)\,B_1(X)} \\ \boldsymbol{A_1(X)\ \wedge\ B_1(X) = 1} \end{cases}$$

Alors :

$$\exists\, \boldsymbol{c} \in \mathbb{R} :\ \boldsymbol{M(X) = c\, D(X)\, A_1(X)\ \ B_1(X)}$$

En particulier :

$$\boldsymbol{D(X)\, M(X) = c\, A(X)\, B(X)}$$

<u>Preuves</u> :

L'existence de $D(X)$ et $M(X)$ est assurée, reste à voir l'unicité.

Soit donc deux polynômes $D(X)$ et $D_1(X)$ de $\mathfrak{D}$ de degré n alors :

$D(X)$ étant un diviseur commun maximal de $A(X)$ et $B(X)$ nous avons :

$$\exists\, \big(U(X), V(X)\big) \in\ (\mathbb{K}[X])^2 :\ A(X)\,U(X) + B(X)\,V(X) = D(X)$$

Donc $D_1(X)$ qui divise $A(X)$ et $B(X)$ divise également $A(X)\,U(X) + B(X)\,V(X)$ donc $D(X)$.

Le même raisonnement montre que $D(X)$ divise $D_1(X)$. Les deux polynômes diffèrent donc d'une constante multiplicative non nulle et comme ils sont unitaires, ils sont égaux.

Soit maintenant deux polynômes $M(X)$ et $M_1(X)$ de $\mathcal{M}$ de degré m. Effectuons la division euclidienne de $M_1(X)$ par $M(X)$:

$$M_1(X) = M(X)\,Q(X) + R(X), \qquad d\big(R(X)\big) < d\big(M(X)\big) = m$$

Supposons pas l'absurde : $R(X) \neq 0$ alors :

$$R(X) = M_1(X) - M(X)\,Q(X)$$

D'autre part $M(X)$ et $M_1(X)$ étant des multiples de $A(X)$ et $B(X)$ le polynôme $R(X)$ est également un multiple de $A(X)$ et $B(X)$ et comme il est non nul il est donc dans l'ensemble $\mathcal{M}$ mais de degré strictement inférieur à m, ce qui est absurde, donc $R(X) = 0$

Il en résulte que $M(X)$ divise $M_1(X)$ et par raisonnement analogue $M_1(X)$ divise $M(X)$. Comme les deux polynômes sont unitaires, ils sont donc égaux.

Notons alors que le polynôme $D(X)A_1(X)\,B_1(X)$ est un multiple commun non nul de $A(X)$ et $B(X)$. Donc, d'après ce qui précède, $M(X)$ divise ce polynôme, soit :

$$D(X)A_1(X)\,B_1(X) = M(X)\,Q(X)$$

Ce qui s'écrit encore de deux façons :

$$\begin{cases} A(X)\,B_1(X) = M(X)\,Q(X) \\ B(X)\,A_1(X) = M(X)\,Q(X) \end{cases}$$

Ainsi, en notant que : $M(X) = A(X)\,Q_1(X) = B(X)\,Q_2(X)$:

$$\begin{cases} A(X)\,B_1(X) = A(X)\,Q_1(X)\,Q(X) \\ B(X)\,A_1(X) = B(X)\,Q_2(X)\,Q(X) \end{cases}$$

Soit en simplifiant :

$$\begin{cases} B_1(X) = Q_1(X)\,Q(X) \\ A_1(X) = Q_2(X)\,Q(X) \end{cases}$$

$Q(X)$ est donc un diviseur commun à $A_1(X)$ et $B_1(X)$, c'est donc une constante non nulle d. Il en résulte :

$$D(X)A_1(X)\,B_1(X) = d\,M(X)$$

D'où :

$$M(X) = \frac{1}{d}D(X)A_1(X)\,B_1(X)$$

IV <u>Décomposition en éléments simples des fractions rationnelles</u> :

1) <u>Approche</u>

Considérons deux polynômes premiers entre eux $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ et un polynôme $C(X)$ quelconque de $\mathbb{K}[X]$. Formons la fraction rationnelle :

$$Q(X) = \frac{C(X)}{A(X)\,B(X)}$$

Le théorème de Bezout donne alors :

$$\exists\,\big(U(X), V(X)\big) \in (\mathbb{K}[X])^2 :\ A(X)\,U(X) + B(X)\,V(X) = 1$$

Ainsi :

$$Q(X) = \frac{C(X)\left(A(X)\,U(X) + \;B(X)\,V(X)\right)}{A(X)\,B(X)}$$

$$Q(X) = \frac{C(X)\,A(X)\,U(X)}{A(X)\,B(X)} + \frac{C(X)\,B(X)\,V(X)}{A(X)\,B(X)}$$

$$Q(X) = \frac{C(X)\;\,U(X)}{B(X)} + \frac{C(X)\,V(X)}{A(X)}$$

Donc $Q(X)$ se met sous la forme :

$$Q(X) = \frac{E(X)}{A(X)} + \frac{F(X)}{B(X)}$$

Effectuons alors la division euclidienne de $E(X)$ par $A(X)$ et celle de $F(X)$ par $B(X)$

$$\begin{cases} E(X) = A(X)\,P(X) + R(X), & d\big(R(X)\big) < d\big(A(X)\big) \\ F(X) = B(X)\,T(X) + S(X), & d\big(S(X)\big) < d\big(B(X)\big) \end{cases}$$

Ainsi :

$$Q(X) = \frac{A(X)\,P(X) + R(X)}{A(X)} + \frac{B(X)\,T(X) + S(X)}{B(X)}$$

$$Q(X) = \;P(X) + \frac{R(X)}{A(X)} + T(X) + \frac{S(X)}{B(X)}$$

Finalement, $Q(X)$ se met sous la forme

$$Q(X) = \;W(X) + \frac{R(X)}{A(X)} + \frac{S(X)}{B(X)}$$

<u>**Théorème**</u> :

$$\forall\;(\boldsymbol{A(X)}, \boldsymbol{B(X)}, \boldsymbol{C(X)}) \in \;(\mathbb{K}^*[\boldsymbol{X}])^{\mathbf{3}} :$$

$$\boldsymbol{A(X)} \wedge \boldsymbol{B(X)} = \mathbf{1} \Rightarrow$$

$$\exists\,!\;\big(\boldsymbol{R(X)}, \boldsymbol{S(X)}, \boldsymbol{W(X)}\big) \in \;(\mathbb{K}[\boldsymbol{X}])^{\mathbf{3}} : \begin{cases} \dfrac{\boldsymbol{C(X)}}{\boldsymbol{A(X)\,B(X)}} = \;\boldsymbol{W(X)} + \dfrac{\boldsymbol{R(X)}}{\boldsymbol{A(X)}} + \dfrac{\boldsymbol{S(X)}}{\boldsymbol{B(X)}} \\ \boldsymbol{d}\big(\boldsymbol{R(X)}\big) < d\big(\boldsymbol{A(X)}\big) \\ \boldsymbol{d}\big(\boldsymbol{S(X)}\big) < d\big(\boldsymbol{B(X)}\big) \end{cases}$$

Preuve :

L'existence a été démontrée dans l'approche. Reste à prouver l'unicité

Notons en premier :

$$\frac{C(X)}{A(X)\,B(X)} = W(X) + \frac{R(X)}{A(X)} + \frac{S(X)}{B(X)}$$

$$\Rightarrow \frac{C(X)}{A(X)\,B(X)} = \frac{A(X)\,B(X)\,W(X) + R(X)\,B(X) + S(X)\,A(X)}{A(X)\,B(X)}$$

$$\Rightarrow C(X) = A(X)\,B(X)\,W(X) + R(X)\,B(X) + S(X)\,A(X)$$

Or :

$$d(R(X)\,B(X) + S(X)\,A(X)) \leq Max\left(d\big(R(X)\,B(X)\big), d(S(X)\,A(X))\right)$$

$$= Max\left(d\big(R(X)\big) + d\big(B(X)\big), d\big(S(X)\big) + d\big(A(X)\big)\right)$$

$$< d\big(A(X)\big) + d\big(B(X)\big) = d(A(X)\,B(X))$$

Donc $W(X)$ est le quotient de la division euclidienne de $C(X)$ par $A(X)\,B(X)$. Il est donc unique.

De même $R(X)\,B(X) + S(X)\,A(X)$ est le reste de la division euclidienne de $C(X)$ par $A(X)\,B(X)$ et est donc unique. Voyons ce qu'il en est de $R(X)$ et $S(X)$.

Supposons :

$$R(X)\,B(X) + S(X)\,A(X) = R_1(X)\,B(X) + S_1(X)\,A(X)$$

Alors :

$$\big(R(X) - R_1(X)\big)\,B(X) = \big(S_1(X) - S(X)\big)\,A(X)$$

Et comme $A(X) \wedge B(X) = 1$, $A(X)$ divise $R(X) - R_1(X)$ et $B(X)$ divise $S_1(X) - S(X)$ mais comme

$d\big(R(X) - R_1(X)\big) < d(A(X)$ et $d\big(S_1(X) - S(X)\big) < d(B(X)$:

$$\begin{cases} R(X) - R_1(X) = 0 \\ S_1(X) - S(X) = 0 \end{cases}$$

D'où l'unicité

2) **Généralisation du théorème** :

$$\forall\ (\boldsymbol{A_1(X), A_2(X), \dots, A_n(X), C(X)}) \in\ (\mathbb{K}^*[\boldsymbol{X}])^{\boldsymbol{n+1}} :$$

$$\left(\forall\ (\boldsymbol{i,j}) \in [\![\boldsymbol{1;n}]\!]^{\boldsymbol{2}}\ \boldsymbol{i \neq j \Rightarrow\ A_i(X) \wedge A_j(X) = 1}\right) \Rightarrow$$

$$\exists\ !\ \left(\boldsymbol{R_1(X), R_2(X), \dots, R_n(X), W(X)}\right) \in\ (\mathbb{K}[\boldsymbol{X}])^{\boldsymbol{n+1}} :$$

$$\begin{cases} \dfrac{\boldsymbol{C(X)}}{\boldsymbol{A_1(X), A_2(X), \dots, A_n(X)}} = \boldsymbol{W(X) + \dfrac{R_1(X)}{A_1(X)} + \dfrac{R_2(X)}{A_2(X)} + \cdots + \dfrac{R_n(X)}{A_n(X)}} \\ \forall\ \boldsymbol{k} \in [\![\boldsymbol{1;n}]\!] :\ \boldsymbol{d\left(R_k(X)\right)} < d\left(\boldsymbol{A_k(X)}\right) \end{cases}$$

Preuve :

Commençons par prouver l'existence par récurrence sur n.

L'initialisation a déjà été faite dans l'approche pour $n = 2$. Voyons l'hérédité.

Soit $n \geq 2$ tel que la propriété soit vraie.

Soit alors $(A_1(X), A_2(X), \dots, A_{n+1}(X), C(X)) \in\ (\mathbb{K}^*[X])^{n+2}$ tels que :

$$\forall\ (i,j) \in [\![1; n+1]\!]^2\ i \neq j \Rightarrow\ A_i(X) \wedge A_j(X) = 1$$

Alors :

$$A_1(X)\ A_2(X) \dots A_n(X) \wedge\ A_{n+1}(X) = 1$$

On en déduit selon le théorème de l'approche :

$$\exists\ !\ \left(R(X), S(X), W_1(X)\right) \in\ (\mathbb{K}[X])^3 :$$

$$\begin{cases} \dfrac{C(X)}{A_1(X)\ A_2(X) \dots A_n(X)\ A_{n+1}(X)} = W_1(X) + \dfrac{R(X)}{A_1(X)\ A_2(X) \dots A_n(X)} + \dfrac{S(X)}{A_{n+1}(X)} \\ d\left(R(X)\right) < d\left(A_1(X)\ A_2(X) \dots A_n(X)\right) \\ d\left(S(X)\right) < d\left(A_n(X)\right) \end{cases}$$

On applique alors l'hypothèse de récurrence :

$$\exists\ !\ \left(R_1(X), R_2(X), \dots, R_n(X), W(X)\right) \in\ (\mathbb{K}[X])^{n+1} :$$

$$\begin{cases} \dfrac{R(X)}{A_1(X), A_2(X), \dots, A_n(X)} = W(X) + \dfrac{R_1(X)}{A_1(X)} + \dfrac{R_2(X)}{A_2(X)} + \cdots + \dfrac{R_n(X)}{A_n(X)} \\ \forall\ k \in [\![1;n]\!] :\ d\left(R_k(X)\right) < d\left(A_k(X)\right) \end{cases}$$

Ainsi :

$$\frac{C(X)}{A_1(X)\,A_2(X)\dots A_n(X)\,A_{n+1}(X)} = W_1(X) + \frac{R_1(X)}{A_1(X)} + \frac{R_2(X)}{A_2(X)} + \dots + \frac{R_n(X)}{A_n(X)} + \frac{S(X)}{A_{n+1}(X)}$$

Ce qui prouve l'existence au rang $n+1$

Voyons maintenant l'unicité :

Notons que $W(X)$ est le quotient de la division euclidienne de $C(X)$ par $A_1(X)\,A_2(X)\dots A_n(X)$ et que le reste de cette division est

$$R_1(X)\prod_{k\neq 1} A_k(X) + R_2(X)\prod_{k\neq 2} A_k(X) + \dots + R_n(X)\prod_{k\neq n} A_k(X)$$

ce quotient et ce reste étant unique.

Supposons alors :

$$R_1(X)\prod_{k\neq 1} A_k(X) + R_2(X)\prod_{k\neq 2} A_k(X) + \dots + R_n(X)\prod_{k\neq n} A_k(X)$$

$$= S_1(X)\prod_{k\neq 1} A_k(X) + S_2(X)\prod_{k\neq 2} A_k(X) + \dots + S_n(X)\prod_{k\neq n} A_k(X)$$

Alors

$$\big(R_1(X) - S_1(X)\big)\prod_{k\neq 1} A_k(X) = \big(S_2(X) - R_2(X)\big)\prod_{k\neq 2} A_k(X) + \dots + \big(S_n(X) - R_n(X)\big)\prod_{k\neq n} A_k(X)$$

Donc $A_1(X)$ qui est diviseur du second membre et premier avec $\prod_{k\neq 1} A_k(X)$ diviserait $R_1(X) - S_1(X)$ qui est un polynôme de degré strictement inférieur à celui de $A_1(X)$. On en déduit :

$$R_1(X) - S_1(X) = 0$$

Et par un raisonnement analogue :

$$R_2(X) - S_2(X) = 0, \dots R_n(X) - S_n(X) = 0$$

D'où l'unicité.

3) **Décomposition en éléments simples dans $\mathbb{C}(X)$**

$$\forall \left(\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \dots, \boldsymbol{\lambda_n}, \boldsymbol{C(X)}\right) \in \mathbb{C}^{\boldsymbol{n}} \times \mathbb{C}^*[\boldsymbol{X}], \forall (\boldsymbol{k_1}, \boldsymbol{k_2}, \dots, \boldsymbol{k_n}) \in (\mathbb{N}^*)^{\boldsymbol{n}}:$$

$$\left(\forall (\boldsymbol{i}, \boldsymbol{j}) \in [\![\boldsymbol{1}; \boldsymbol{n}]\!]^2\ \boldsymbol{i} \neq \boldsymbol{j} \Rightarrow \boldsymbol{\lambda_i} \neq \boldsymbol{\lambda_j}\right) \Rightarrow$$

$$\exists !\ \left(\boldsymbol{a_{11}}, \dots \boldsymbol{a_{1k_1}}, \dots, \boldsymbol{a_{n1}}, \dots, \boldsymbol{a_{nk_n}}, \boldsymbol{Q(X)}\right) \in \mathbb{C}^{\boldsymbol{k_1}+\dots+\boldsymbol{k_n}} \times \mathbb{C}[\boldsymbol{X}] :$$

$$\frac{\boldsymbol{C(X)}}{(\boldsymbol{X}-\boldsymbol{\lambda_1})^{\boldsymbol{k_1}}\ (\boldsymbol{X}-\boldsymbol{\lambda_2})^{\boldsymbol{k_2}} \dots\ (\boldsymbol{X}-\boldsymbol{\lambda_n})^{\boldsymbol{k_n}}}$$

$$= \boldsymbol{Q(X)} + \frac{\boldsymbol{a_{11}}}{\boldsymbol{X}-\boldsymbol{\lambda_1}} + \cdots \frac{\boldsymbol{a_{1k_1}}}{(\boldsymbol{X}-\boldsymbol{\lambda_1})^{\boldsymbol{k_1}}} + \cdots + \frac{\boldsymbol{a_{n1}}}{\boldsymbol{X}-\boldsymbol{\lambda_n}} + \cdots \frac{\boldsymbol{a_{nk_n}}}{(\boldsymbol{X}-\boldsymbol{\lambda_n})^{\boldsymbol{k_n}}}$$

Preuve :

Il suffit d'appliquer dans un premier temps le théorème précédent avec pour $i \in \|1; n\|$:

$$A_i(X) = (X - \lambda_i)^{k_i}$$

Cela donne :

$$\frac{C(X)}{(X-\lambda_1)^{k_1}\ (X-\lambda_2)^{k_2} \dots\ (X-\lambda_n)^{k_n}}$$

$$= Q(X) + \frac{R_1(X)}{(X-\lambda_1)^{k_1}} + \cdots + \frac{R_n(X)}{(X-\lambda_n)^{k_n}}$$

Avec pour $i \in \|1; n\|$: $d\big(R_i(X)\big) < k_i$

Ainsi :

$$R_i(X) \in Vect[1, X, \dots, X^{k_i-1}] = Vect[1, (X-\lambda_i), \dots, (X-\lambda_i)^{k_i-1}]$$

Donc :

$$\exists !\ \left(a_{i1}, \dots a_{ik_i}\right) \in \mathbb{C}^{k_i} : R_i(X) = a_{i1}(X-\lambda_i)^{k_i-1} + a_{i2}\ (X-\lambda_i)^{k_i-2} + \cdots + a_{ik_i}$$

Ainsi :

$$\frac{R_i(X)}{(X-\lambda_i)^{k_i}} = \frac{a_{i1}}{X-\lambda_i} + \cdots \frac{a_{ik_i}}{(X-\lambda_i)^{k_i}}$$

Cela prouve l'existence et l'unicité de la décomposition.

4) **Décomposition en éléments simples dans $\mathbb{R}(X)$**

$$\forall \left(\boldsymbol{\lambda_1}, \boldsymbol{\lambda_2}, \dots, \boldsymbol{\lambda_n}, \boldsymbol{C}(\boldsymbol{X})\right) \in \mathbb{R}^{\boldsymbol{n}} \times \mathbb{R}^*[\boldsymbol{X}], \forall (\boldsymbol{k_1}, \boldsymbol{k_2}, \dots, \boldsymbol{k_n}) \in (\mathbb{N}^*)^{\boldsymbol{n}},$$

$$\forall (\boldsymbol{b_1}, \dots \boldsymbol{b_m}, \boldsymbol{c_1}, \dots \boldsymbol{c_m}) \in \mathbb{R}^{\boldsymbol{2m}}, \forall (\boldsymbol{s_1}, \boldsymbol{s_2}, \dots, \boldsymbol{s_m}) \in (\mathbb{N}^*)^{\boldsymbol{m}} :$$

$$\begin{cases} \forall (\boldsymbol{i}, \boldsymbol{j}) \in [\![\boldsymbol{1}; \boldsymbol{n}]\!]^2 \ \boldsymbol{i} \neq \boldsymbol{j} \Rightarrow \boldsymbol{\lambda_i} \neq \boldsymbol{\lambda_j} \\ \forall (\boldsymbol{i}, \boldsymbol{j}) \in [\![\boldsymbol{1}; \boldsymbol{m}]\!]^2 \ \boldsymbol{i} \neq \boldsymbol{j} \Rightarrow (\boldsymbol{b_i}, \boldsymbol{c_i}) \neq \left(\boldsymbol{b_j}, \boldsymbol{c_j}\right) \end{cases} \Rightarrow$$

$$\begin{cases} \exists ! \left(\boldsymbol{c_{11}}, \dots \boldsymbol{c_{1k_1}}, \dots, \boldsymbol{c_{n1}}, \dots, \boldsymbol{c_{nk_n}}, \boldsymbol{Q}(\boldsymbol{X})\right) \in \mathbb{R}^{\boldsymbol{k_1}+\dots+\boldsymbol{k_n}} \times \mathbb{R}[\boldsymbol{X}] \\ \exists ! \left(\boldsymbol{a_{11}}, \boldsymbol{b_{11}}, \dots, \boldsymbol{a_{1s_1}}, \dots, \boldsymbol{b_{1s_1}}, \dots, \boldsymbol{a_{m1}}, \boldsymbol{b_{m1}}, \dots, \boldsymbol{a_{1s_m}}, \boldsymbol{b_{1s_m}}\right) \in \mathbb{R}^{2(s_1+\dots+s_m)} \end{cases} :$$

$$\frac{\boldsymbol{C}(\boldsymbol{X})}{(\boldsymbol{X}-\boldsymbol{\lambda_1})^{k_1} \ \dots \ (\boldsymbol{X}-\boldsymbol{\lambda_n})^{k_n} \ (\boldsymbol{X}^2+\boldsymbol{b_1}\boldsymbol{X}+\boldsymbol{c_1})^{s_1} \dots (\boldsymbol{X}^2+\boldsymbol{b_m}\boldsymbol{X}+\boldsymbol{c_m})^{s_m}}$$

$$= \boldsymbol{Q}(\boldsymbol{X}) + \frac{\boldsymbol{c_{11}}}{\boldsymbol{X}-\boldsymbol{\lambda_1}} + \cdots \frac{\boldsymbol{c_{1k_1}}}{(\boldsymbol{X}-\boldsymbol{\lambda_1})^{k_1}} + \cdots + \frac{\boldsymbol{c_{n1}}}{\boldsymbol{X}-\boldsymbol{\lambda_n}} + \cdots \frac{\boldsymbol{c_{nk_n}}}{(\boldsymbol{X}-\boldsymbol{\lambda_n})^{k_n}}$$

$$+ \frac{\boldsymbol{a_{11}}\ \boldsymbol{X}+\boldsymbol{b_{11}}}{\boldsymbol{X}^2+\boldsymbol{b_1}\boldsymbol{X}+\boldsymbol{c_1}} + \cdots + \frac{\boldsymbol{a_{1s_1}}\ \boldsymbol{X}+\boldsymbol{b_{1s_1}}}{(\boldsymbol{X}^2+\boldsymbol{b_1}\boldsymbol{X}+\boldsymbol{c_1})^{s_1}} + \cdots + \frac{\boldsymbol{a_{m1}}\ \boldsymbol{X}+\boldsymbol{b_{m1}}}{\boldsymbol{X}^2+\boldsymbol{b_m}\boldsymbol{X}+\boldsymbol{c_m}} + \cdots + \frac{\boldsymbol{a_{1s_m}}\ \boldsymbol{X}+\boldsymbol{b_{1s_m}}}{(\boldsymbol{X}^2+\boldsymbol{b_m}\boldsymbol{X}+\boldsymbol{c_m})^{s_m}}$$

Preuve :

Il suffit d'appliquer dans un premier temps le théorème précédent avec les polynômes premiers entre eux deux à deux

$$(X-\lambda_i)^{k_i}, i \in [\![1; n]\!]$$

$$\left(X^2+b_jX+c_j\right)^{s_j}, j \in [\![1; m]\!]$$

Cela donne :

$$\frac{C(X)}{(X-\lambda_1)^{k_1} \ \dots \ (X-\lambda_n)^{k_n} \ (X^2+b_1X+c_1)^{s_1} \dots (X^2+b_mX+c_m)^{s_m}}$$

$$= Q(X) + \frac{R_1(X)}{(X-\lambda_1)^{k_1}} + \cdots + \frac{R_n(X)}{(X-\lambda_n)^{k_n}} + \frac{S_1(X)}{(X^2+b_1X+c_1)^{s_1}} + \cdots + \frac{S_m(X)}{(X^2+b_mX+c_m)^{s_m}}$$

Avec pour $i \in \|1; n\|$: $d\left(R_i(X)\right) < k_i$ et pour $j \in [\![1; m]\!]$: $d\left(S_j(X)\right) < 2\ s_j$ et cette décomposition est unique. Intéressons nous aux différents éléments fractionnaires qui sont chacun de la forme :

$$\frac{T(X)}{A(X)^k}$$

Avec : $d\left(T(X)\right) < d\left(A(X)^k\right)$

Effectuons une division euclidienne de $T(X)$ par $A(X)$:

$$T(X) = A(X)\ T_1(X) + N_1(X), \qquad d\big(N_1(X)\big) < d\big(A(X)\big)$$

On a alors :

$$\frac{T(X)}{A(X)^k} = \frac{A(X)\ T_1(X) + N_1(X)}{A(X)^k} = \frac{T_1(X)}{A(X)^{k-1}} + \frac{N_1(X)}{A(X)^k}$$

En réitérant l'opération :

$$\frac{T(X)}{A(X)^k} = \frac{T_2(X)}{A(X)^{k-2}} + \frac{N_2(X)}{A(X)^{k-1}} + \frac{N_1(X)}{A(X)^k}$$

Et ainsi de suite jusqu'à aboutir à :

$$\frac{T(X)}{A(X)^k} = \frac{T_{k-1}(X)}{A(X)} + \frac{N_{k-1}(X)}{A(X)^2} + \cdots + \frac{N_2(X)}{A(X)^{k-1}} + \frac{N_1(X)}{A(X)^k}$$

Comme $d\big(T_{k-1}(X)\big) < d(A(X))$ et $d\left(N_j(X)\right) < d(A(X)), j \in [\![1, k-1]\!]$ on obtient l'existence de la décomposition souhaitée. Pour l'unicité, il suffit de noter que les $T_j(X)$ et $N_j(X)$ sont définis de façon unique à chaque étape de division euclidienne.