

Dans tout ce chapitre, sauf précision contraire, \mathbb{K} désigne le corps \mathbb{R} ou le corps \mathbb{C} .

I : l'algèbre $\mathbb{K}[X]$

Définition

Définition : on appelle polynôme à coefficients dans \mathbb{K} toute quantité P de la forme

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + a_nX^n$$

où $n \in \mathbb{N}$ et a_0, a_1, \dots, a_n sont des éléments du corps \mathbb{K} . La quantité X s'appelle *l'indéterminée*.

L'ensemble de tous les polynômes à coefficients dans \mathbb{K} est noté $\mathbb{K}[X]$.

Notation : Si $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, on note $P = \sum_{k=0}^n a_kX^k = \sum_{0 \leq k \leq n} a_kX^k$.

Par souci de simplification, on notera également $P = \sum_{k=0}^{+\infty} a_kX^k$ voire $P = \sum_{k \in \mathbb{N}} a_kX^k$ ou encore

$P = \sum_k a_kX^k = \sum a_kX^k$, en supposant que **les termes a_k sont nuls à partir d'un certain rang** (i.e il existe $n \in \mathbb{N}$ tel que $k > n \Rightarrow a_k = 0$).

Remarque : ainsi tout polynôme à coefficients dans \mathbb{K} peut être identifié à une suite nulle à partir d'un certain rang (à valeurs dans \mathbb{K}). En effet, on peut écrire $P = (a_0, a_1, a_2, \dots)$ en supposant $a_k = 0$ dès que k dépasse un certain entier (par exemple n), d'où $P = (a_0, a_1, a_2, \dots, a_{n-1}, a_n, 0, 0, 0, \dots)$.

Avec ces notations, $P = a_0(1, 0, 0, \dots) + a_1(0, 1, 0, \dots) + a_2(0, 0, 1, 0, \dots) + \cdots + a_n(0, \dots, 0, 1, 0, \dots)$ et $\tilde{1} = X^0 = (1, 0, 0, \dots)$, $X = X^1 = (0, 1, 0, \dots)$, $X^2 = (0, 0, 1, 0, \dots)$, $X^3 = (0, 0, 0, 1, 0, \dots)$ etc...

Il est facile de prouver que l'ensemble des suites nulles à partir d'un certain rang est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$ (\mathbb{K} -espace vectoriel des suites à coefficients dans \mathbb{K}).

Donc en définissant les opérations :

pour tous $P = \sum a_iX^i$ et $Q = \sum b_iX^i$ de $\mathbb{K}[X]$, et pour tout scalaire $\lambda \in \mathbb{K}$,

$$P + Q := \sum (a_i + b_i)X^i \quad \text{et} \quad \lambda.P := \sum (\lambda.a_i)X^i,$$

on obtient

Propriété : $\mathbb{K}[X]$ est un \mathbb{K} -espace vectoriel, de vecteur nul $\tilde{0} = \sum_i 0X^i = (0, 0, 0, 0, \dots)$.

On peut également définir un produit interne sur $\mathbb{K}[X]$.

Définition-proposition : soit $(a_i)_{i \geq 0}$ et $(b_j)_{j \geq 0}$, deux suites à valeurs dans \mathbb{K} .

On définit alors la suite $(c_k)_{k \geq 0}$ par

$$c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^k a_i b_{k-i} = \sum_{j=0}^k a_{k-j} b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_i b_{k-i} + \cdots + a_{k-1} b_1 + a_k b_0.$$

Ainsi : $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$, $c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$, etc...

Premier résultat : si $(a_i)_{i \geq 0}$ et $(b_j)_{j \geq 0}$ sont nulles à partir d'un certain rang, alors $(c_k)_{k \geq 0}$ également.

Second résultat : par conséquent, si $P = \sum a_i X^i$ et $Q = \sum b_j X^j$ sont des polynômes de $\mathbb{K}[X]$, alors $R = \sum c_k X^k$ est aussi un polynôme. On le note $R = P \times Q = PQ$ (polynôme produit de P par Q).

Preuve du premier résultat : en supposant $(i > n \Rightarrow a_i = 0)$ et $(j > m \Rightarrow b_j = 0)$, on vérifie facilement que $(k > n + m \Rightarrow c_k = 0)$.

Remarque : cela correspond bien au produit usuel que l'on connaît sur le produit de fonctions.

Par exemple, si $P = a_0 + a_1X + a_2X^2$ et $Q = b_0 + b_1X$, alors

$PQ = (a_0 + a_1X + a_2X^2)(b_0 + b_1X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_1b_1 + a_2b_0)X^2 + (a_2b_1)X^3$,
ce qui peut encore s'écrire

$PQ = (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^3$
en prenant $a_3 = b_2 = b_3 = 0$.

On vérifie assez facilement les propriétés suivantes (admis ici).

Propriété : le produit de polynômes est une loi interne sur $\mathbb{K}[X]$ (on vient de le prouver) qui est commutative ($PQ = QP$), associative ($(PQ)R = P(QR)$), distributive sur l'addition à gauche et à droite ($P(Q + R) = PQ + PR$ et $(P + Q)R = PR + QR$), et $X^0 \times P = P \times X^0 = P$.

Conséquence : $\mathbb{K}[X]$ est un anneau commutatif, de neutres $\tilde{0}$ (pour $+$) et $\tilde{1} = X^0$ (pour \times).

On rappelle qu'on a déjà vu que $\mathbb{K}[X]$ est un espace vectoriel. De plus, on vérifie facilement, avec $\lambda \in \mathbb{K}$: $\lambda.(PQ) = (\lambda.P)Q = P(\lambda.Q)$. On peut alors affirmer : $(\mathbb{K}[X], +, \times, .)$ est une *algèbre*.

Degré d'un polynôme

Définition : soit $P = \sum a_k X^k \in \mathbb{K}[X]$.

- si $P \neq \tilde{0}$, on définit le degré de P par le plus grand entier i tel que $a_i \neq 0$, autrement dit

$$\deg(P) = \max \{i \in \mathbb{N} \mid a_i \neq 0\}.$$

- si $P = \tilde{0}$, on pose (convention) : $\deg(\tilde{0}) = -\infty$.

Attention : si $P = \sum a_k X^k$ est un polynôme constant (i.e $k \geq 1 \Rightarrow a_k = 0$), alors son degré $\deg(P) = -\infty$ ou 0 selon que P est constant nul ou constant non nul.

On prend les conventions, pour tout entier $n \in \mathbb{N}$:

$$(-\infty) < n, \quad (-\infty) + (-\infty) = -\infty \quad \text{et} \quad (-\infty) + n = -\infty.$$

Propriétés : pour tous P et Q dans $\mathbb{K}[X]$,

- $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$
(avec égalité dans l'inégalité si $\deg(P) \neq \deg(Q)$, mais ce n'est pas le seul cas d'égalité)
- $\deg(P \times Q) = \deg(P) + \deg(Q)$

Preuve : en cours.

Remarque : pour la composition de polynômes (avec une définition s'inspirant de la composition de fonction), les formules sont plus compliquées. En effet, pour tout $P \in \mathbb{K}[X]$, on a $\tilde{0} \circ P = \tilde{0}$ mais $P \circ \tilde{0} = P(0)$, donc $\deg(\tilde{0} \circ P) = -\infty$ et $\deg(P \circ \tilde{0}) = -\infty$ ou 0 , selon que 0 est racine de P ou non. Même problème si P est constant...

Dans le cas où P et Q ne sont pas constants, on a tout de même $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Définition : soit $P = \sum a_k X^k$, un polynôme non nul ($P \neq \tilde{0}$), de degré $d \geq 0$. On dit que P est un polynôme **unitaire** (ou *normalisé*) si son coefficient dominant vaut 1 (i.e si $a_d = 1$).

Proposition : si P est un polynôme non nul, il existe un unique polynôme unitaire colinéaire à P . Autrement dit, il existe un unique $\lambda \in \mathbb{K}$ tel que $\lambda.P$ est unitaire.

Facile à voir : il faut et il suffit de prendre $\lambda = \frac{1}{a_d}$ où $d = \deg(P)$. On a $P = a_d.P_0$ avec P_0 unitaire.

Proposition-définition : pour tout entier $n \in \mathbb{N}$, on définit l'ensemble $\mathbb{K}_n[X]$ des polynômes à coefficients dans \mathbb{K} et de degré **inférieur ou égal** à n . Ainsi $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$.

Cet ensemble $\mathbb{K}_n[X]$ est un sous-espace vectoriel du \mathbb{K} -espace vectoriel $\mathbb{K}[X]$.

Preuve : ça se vérifie facilement par caractérisation de sev (avec les propriétés connues sur les degrés).

On peut aussi remarquer que $\mathbb{K}_n[X]$ est l'ensemble des polynômes de la forme $a_0 + a_1X + \dots + a_nX^n$ (i.e) $a_0X^0 + a_1X^1 + \dots + a_nX^n$: c'est donc l'ensemble des combinaisons linéaires des vecteurs X^0, X^1, \dots, X^n .

On a :

$$\mathbb{K}_n[X] = \text{vect}(X^0, X^1, \dots, X^n).$$

On retrouve le fait que c'est un sev en tant que sev engendré par la famille (X^0, X^1, \dots, X^n) .

Attention : $\mathbb{K}_n[X]$ n'est pas stable par produit (dès que $n \geq 1$), donc n'est pas un anneau (ni algèbre par conséquent).

Divisibilité dans $\mathbb{K}[X]$

Définition : Soit deux polynômes A et B dans $\mathbb{K}[X]$.

On dit que A **divise** B s'il existe un polynôme C dans $\mathbb{K}[X]$ tel que $B = A \times C$.

On dit aussi que B est un multiple de A ou encore que A est un diviseur de B , et on notera parfois « $A \mid B$ » lorsque A divise B .

Exemples : dans $\mathbb{R}[X]$, $(X^2 + X + 1)$ divise $X^3 - 1$ car $X^3 - 1 = (X^2 + X + 1)(X - 1)$.

Dans $\mathbb{C}[X]$, $(X - i)$ divise $X^2 + 1$ car $X^2 + 1 = (X - i)(X + i)$.

Rappel : dans l'anneau $\mathbb{K}[X]$, on dit qu'un élément P est **inversible** s'il existe un polynôme Q tel que $P \times Q = X^0 = \tilde{1}$.

Proposition : les seuls éléments inversibles de $\mathbb{K}[X]$ sont les **polynômes constants non nuls**.

Preuve : facile, car si $P \times Q = 1$, alors $\deg(P) + \deg(Q) = \deg(1) = 0$, donc $\deg(P) = \deg(Q) = 0$.

Remarque : souvent on pourra identifier les constants et les polynômes constants.

Autrement dit : « $\mathbb{K} = \mathbb{K}_0[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq 0 \text{ i.e } \deg(P) = -\infty \text{ ou } 0\}$ ».

Proposition : $\mathbb{K}[X]$ est un anneau commutatif, qui est aussi un **anneau intègre**.

On rappelle que cela signifie que, pour P et Q dans $\mathbb{K}[X]$:

$$\boxed{\text{si } P \times Q = \tilde{0} \text{ alors } P = \tilde{0} \text{ ou } Q = \tilde{0}}.$$

Conséquence : tout élément non nul de $\mathbb{K}[X]$ est **régulier**. Ceci signifie :

$$\boxed{\text{si } P \neq \tilde{0} \text{ alors on a l'implication : } (P \times Q = P \times R) \Rightarrow (Q = R)}.$$

Proposition : si P et Q sont deux polynômes non-nuls qui se divisent l'un l'autre (i.e)

$P \mid Q$ et $Q \mid P$, alors P et Q sont **associés** (i.e) il existe un scalaire $\lambda \neq 0$ tel que $P = \lambda Q$ (polynômes colinéaires).

Preuve : facile, car il existe R et S dans $\mathbb{K}[X]$ tels que $P = QR$ et $Q = PS$, d'où $P = PRS$.

Si $P = \tilde{0}$ alors nécessairement $Q = \tilde{0}$ et tout $\lambda \in \mathbb{K}^*$ convient !

Si $P \neq \tilde{0}$ alors P est régulier, donc $RS = \tilde{1}$: R et S sont inversibles donc constantes non-nulles.

Division euclidienne dans $\mathbb{K}[X]$

Théorème : pour tout couple de polynômes $(A, B) \in \mathbb{K}[X]^2$ tel que $B \neq \tilde{0}$, il existe **un, et un seul couple** de polynômes $(Q, R) \in \mathbb{K}[X]^2$ vérifiant

$$\begin{cases} A = B \times Q + R \\ \text{et} \\ \deg(R) < \deg(B) \end{cases}.$$

Les polynômes Q et R s'appellent respectivement le **quotient** et le **reste** dans la **division euclidienne** du polynôme A par le polynôme $B \neq 0$.

Preuve : on prouve d'abord l'unicité (facile) puis l'existence (plus délicat).

Unicité : supposons qu'il existe deux couples (Q_1, R_1) et (Q_2, R_2) dans $\mathbb{K}[X]^2$ vérifiant

$$\begin{cases} A = B \times Q_1 + R_1 \\ A = B \times Q_2 + R_2 \end{cases} \text{ et } \begin{cases} \deg(R_1) < \deg(B) \\ \deg(R_2) < \deg(B) \end{cases}.$$

Des égalités on déduit, par soustraction : $R_1 - R_2 = B \times (Q_2 - Q_1)$. D'où en passant aux degrés :

$$\deg(R_1 - R_2) = \deg(B \times (Q_2 - Q_1)) = \deg(B) + \deg(Q_2 - Q_1).$$

Mais, d'autre part, avec les inégalités sur les degrés, on déduit :

$$\deg(R_1 - R_2) \leq \max(\deg(R_1), \deg(R_2)) < \deg(B), \text{ d'où } \deg(R_1 - R_2) < \deg(B).$$

Avec le premier résultat établi, on en déduit $\deg(R_1 - R_2) = \deg(B) + \deg(Q_2 - Q_1) < \deg(B)$, ce qui n'est possible que si $\deg(Q_2 - Q_1) < 0$, (i.e) $\deg(Q_2 - Q_1) = -\infty$, ce qui implique $Q_2 - Q_1 = 0$ donc $Q_1 = Q_2$. En reportant dans les égalités précédentes, on en déduit aussi $R_1 = R_2$, ce qui prouve l'unicité du couple (Q, R) dans la division euclidienne.

Existence :

1er cas : si $A = 0$. C'est évident, car on peut écrire $0 = B \times 0 + 0$ avec $\deg(0) = -\infty < \deg(B)$ (on rappelle que $B \neq 0$ donc $0 \leq \deg(B)$). Ainsi $(Q, R) = (0, 0)$ est une solution au problème.

2nd cas : si $A \neq 0$. On sépare selon que B est constant ou non.

- **1er sous-cas** : si B est un polynôme constant. On a donc $B = \lambda \in \mathbb{K}^*$.

On peut écrire $A = \lambda \times (\frac{1}{\lambda}.A) + 0$ (car $\lambda \neq 0$). En posant $(Q, R) = (\frac{1}{\lambda}.A, 0)$, on a l'égalité recherchée avec l'inégalité sur les degrés $\deg(R) = -\infty < \deg(B) = 0$. Là encore, l'existence du couple est prouvée.

- **2nd sous-cas** : si B n'est pas un polynôme constant. Dans ce cas, on a $p = \deg(B) \geq 1$.

Pour prouver l'existence du couple (Q, R) , on s'inspire de la méthode pratique de calcul effectif du quotient et du reste. On va travailler par **récurrence forte** sur le degré n du polynôme A , le polynôme B étant fixé et de degré $p \geq 1$.

Posons la proposition (H_n) : « pour tout polynôme A de degré n , il existe un couple (Q, R) de polynômes vérifiant $A = B \times Q + R$ et $\deg(R) < \deg(B)$ ».

♡ Initialisation : si A est de degré 0, A est une constante non nulle, on écrit $A = B \times 0 + A$, et en posant $(Q, R) = (0, A)$, on a l'égalité avec $\deg(R) = \deg(A) = 0 < p = \deg(B)$ (car désormais B n'est pas constant). D'où l'existence du couple dans ce cas, et (H_0) est vraie.

♡ Hérité : supposons $(H_0), (H_1), \dots, (H_n)$ vraies pour un certain entier $n \geq 0$. On veut prouver que, sous ces hypothèses, (H_{n+1}) est vraie? Soit A , un polynôme quelconque de

degré $n + 1$. On peut donc l'écrire $A = a_{n+1}X^{n+1} + a_nX^n + \dots + a_1X^1 + a_0$ avec $a_{n+1} \neq 0$.
 Ecrivons le polynôme B sous la forme $B = b_pX^p + \dots + b_1X^1 + b_0$ avec $b_p \neq 0$ (et $p \geq 1$).
 1ère possibilité : $n + 1 < p$.

En écrivant $A = B \times 0 + A$, avec l'hypothèse $\deg(A) = n + 1 < p = \deg(B)$, le couple $(Q, R) = (0, A)$ est une solution. Donc (H_{n+1}) est vraie dans ce cas.

2nde possibilité : $n + 1 \geq p$.

Le rapport des termes dominants de A et B est $\left(\frac{a_{n+1}}{b_p}\right) X^{n+1-p}$.

On définit le polynôme $A_1 = A - \frac{a_{n+1}}{b_p} X^{n+1-p} \times B$. On développe :

$$A_1 = a_{n+1}X^{n+1} + a_nX^n + \dots + a_0 - \frac{a_{n+1}}{b_p} X^{n+1-p} \times (b_pX^p + \dots + b_1X^1 + b_0), \text{ puis}$$

$$A_1 = a_{n+1}X^{n+1} + a_nX^n + \dots + a_0 - (a_{n+1}X^{n+1} + \dots + \frac{a_{n+1}b_0}{b_p} X^{n+1-p}).$$

On simplifie, et A_1 est donc de la forme $A_1 = \alpha_nX^n + \alpha_{n-1}X^{n-1} + \dots + \alpha_1X^1 + \alpha_0$.

Le degré de A_1 est donc inférieur ou égal à n : $\deg(A_1) \leq n$

Par hypothèse de récurrence forte, on est assuré de l'existence d'un couple de polynômes (Q_1, R_1) tels que $A_1 = B \times Q_1 + R_1$ avec $\deg(R_1) < \deg(B)$.

Mais on se souvient de : $A = A_1 + \frac{a_{n+1}}{b_p} X^{n+1-p} \times B$. On reporte l'expression de A_1 , on en tire $A = B \times Q_1 + R_1 + \frac{a_{n+1}}{b_p} X^{n+1-p} \times B = B \times (Q_1 + \frac{a_{n+1}}{b_p} X^{n+1-p}) + R_1$.

On pose $(Q, R) = (Q_1 + \frac{a_{n+1}}{b_p} X^{n+1-p}, R_1)$: ce couple vérifie bien $A = B \times Q + R$ avec $\deg(R) = \deg(R_1) < \deg(B)$! Donc (H_{n+1}) est vraie, d'où l'hérédité.

♥ Conclusion : par récurrence forte on a prouvé que (H_n) est vraie pour tout entier $n \geq 0$.

II : racines d'un polynôme de $\mathbb{K}[X]$

Fonctions polynomiales

A tout polynôme $P = \sum_{k=0}^n a_k X^k$ de $\mathbb{K}[X]$ on associe la fonction polynomiale \tilde{P} définie par :

$$\tilde{P} : \begin{cases} \mathbb{K} & \longrightarrow \mathbb{K} \\ t & \longmapsto \tilde{P}(t) := \sum_{k=0}^n a_k t^k \end{cases} .$$

On récupère ainsi les fonctions puissances $\tilde{X}^k : \begin{cases} \mathbb{K} & \longrightarrow \mathbb{K} \\ t & \longmapsto \tilde{X}^k(t) := t^k \end{cases} .$

On définit alors l'application Φ qui à tout polynôme P associe sa fonction polynomiale $\Phi(P) = \tilde{P}$:

$$\Phi : \begin{cases} \mathbb{K}[X] & \longrightarrow \mathcal{F}(\mathbb{K}, \mathbb{K}) \\ P & \longmapsto \Phi(P) := \tilde{P} \end{cases} .$$

On vérifie aisément que Φ est une application linéaire : $\Phi(\lambda.P + \mu.Q) = \lambda.\Phi(P) + \mu.\Phi(Q)$.

Avec en plus les propriétés suivantes : $\Phi(P \times Q) = \Phi(P) \times \Phi(Q)$ et $\Phi(X^0) = \tilde{1}$.

On dit que Φ est aussi un morphisme d'anneaux (donc morphisme d'algèbres).

Remarque : on verra plus tard dans ce chapitre que, avec $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} , l'application Φ est injective, donc réalise une bijection (isomorphisme) entre $\mathbb{K}[X]$ et l'espace des fonctions polynomiales.

Dans la pratique : il arrivera souvent que l'on note de la même façon un polynôme P et sa fonction

polynomiale associée \tilde{P} .

Racine d'un polynôme

Définition : si P est un polynôme de $\mathbb{K}[X]$ et a un élément du corps \mathbb{K} , on dit que a est une **racine** (ou **zéro**) de P si $\tilde{P}(a) = 0$.

Proposition : on a l'équivalence (caractérisation) :

$$(a \text{ est une racine de } P) \Leftrightarrow (X - a \text{ divise } P)$$

Preuve(s) : en cours.

Conséquence 1 : tout polynôme P de degré $n \geq 0$ possède *au plus* n racines distinctes.

Preuve : en cours.

A retenir : si un polynôme P a une infinité de racines, c'est donc nécessairement le polynôme nul.

Mieux :

si on sait que $\deg(P) \leq n$ et P possède au moins $(n + 1)$ racines, alors P est le polynôme nul.

Conséquence 2 : l'application $\Phi : \begin{array}{l} \mathbb{K}[X] \longrightarrow \mathcal{F}(\mathbb{K}, \mathbb{K}) \\ P \longmapsto \Phi(P) := \tilde{P} \end{array}$ est injective (il y a donc une bijec-

tion entre $\mathbb{K}[X]$ et l'espace des fonctions polynomiales $\text{Im}(\Phi)$: on parle d'isomorphisme d'algèbres).

Preuve : $(P \in \ker(\Phi)) \Leftrightarrow (\Phi(P) = \tilde{0}) \Leftrightarrow (\text{pour tout } a \in \mathbb{K}, \tilde{P}(a) = 0) \Rightarrow (P \text{ a une infinité de racines}).$

Ainsi $(P \in \ker(\Phi)) \Rightarrow (P \text{ est le polynôme nul})$. On a donc $\ker(\Phi) = \{0\}$, d'où l'injectivité de Φ .

C'est donc le caractère infini des corps \mathbb{C} et \mathbb{R} qui permet d'affirmer qu'il y a identification possible entre un polynôme et sa fonction polynomiale.

Ce résultat ne tient plus lorsque l'on travaille avec un corps \mathbb{K} fini (hors programme) : par exemple si $\mathbb{K} = \{0, 1\}$, corps dans lequel $1 + 1 = 0$, en posant $P = X^2 + X$ et $Q = X^5 + X^3$, on a $\tilde{P} = \tilde{Q}$! En effet, évaluer ces polynômes en 0 et en 1... Ainsi $\Phi(P) = \Phi(Q)$ mais $P \neq Q$ (degrés distincts).

Ordre de multiplicité d'une racine d'un polynôme

Définition : soit un polynôme $P \neq 0$, un élément a du corps \mathbb{K} , un entier naturel $k \geq 1$.

On dit que

a est une **racine de P d'ordre de multiplicité supérieur ou égal à k** si $(X - a)^k$ divise P .

Ainsi :

$(a \text{ est un zéro d'ordre de multiplicité } \geq k \text{ de } P) \Leftrightarrow (\text{il existe } Q \in \mathbb{K}[X] \text{ tel que } P = (X - a)^k \times Q).$

Exemple : soit $P = X^5 - 3X^4 + 5X^3 - 7X^2 + 6X - 2 = (X - 1)^2(X^3 - X^2 + 2X - 2)$.

On peut affirmer que 1 est une racine de P avec un ordre de multiplicité supérieur ou égal à 2. Voir la suite ci-dessous.

Définition : soit un polynôme $P \neq 0$, un élément a du corps \mathbb{K} , un entier naturel $m \geq 1$.

On dit que

a est une **racine de P d'ordre de multiplicité égal à m** si

$$(X - a)^m \text{ divise } P \text{ MAIS } (X - a)^{m+1} \text{ ne divise pas } P.$$

Ainsi :

$(a \text{ est un zéro d'ordre de multiplicité } m \text{ de } P) \Leftrightarrow (\exists Q \in \mathbb{K}[X], P = (X - a)^m \times Q \text{ et } Q(a) \neq 0).$

Exemple : soit $P = X^5 - 3X^4 + 5X^3 - 7X^2 + 6X - 2$. On remarque $P(1) = 0$: donc 1 est une racine du polynôme P , notons m son ordre de multiplicité. De $P(1) = 0$, on peut déjà affirmer $m \geq 1$.

On a $P = (X - 1) \times Q$ où $Q = X^4 - 2X^3 + 3X^2 - 4X + 2$. On observe $Q(1) = 0$, donc $m \geq 2$.

On a $P = (X - 1)^2 \times R$ où $R = X^3 - X^2 + 2X - 2$. On observe $R(1) = 0$, donc $m \geq 3$.

On a $P = (X - 1)^3 \times S$ où $S = X^2 + 2$. On observe $S(1) \neq 0$, donc $m = 3$: le réel 1 est donc une racine d'ordre trois du polynôme P (racine triple).

Remarque : il peut être parfois pratique de considérer les définitions ci-dessous pour des entiers k et m éventuellement nuls. Dans ce cas, il faut admettre la **convention** suivante :

« a est une racine d'ordre 0 de P » signifie « a n'est pas racine de P ».

Relations racines/coefficients d'un polynôme

Définition : un polynôme P non constant de $\mathbb{K}[X]$ est dit **scindé sur \mathbb{K}** si son degré est égal au nombre de ses racines, chacune étant comptée avec son ordre de multiplicité.

Autrement dit, si $P = \sum_{0 \leq k \leq n} a_k X^k$, avec $n \geq 1$ et $a_n \neq 0$, P est scindé (sur \mathbb{K}) s'il peut s'écrire sous la forme

$$P = a_n (X - \alpha_1)^{m_1} (X - \alpha_2)^{m_2} \dots (X - \alpha_r)^{m_r} = a_n \prod_{1 \leq i \leq r} (X - \alpha_i)^{m_i}$$

les α_i étant les racines de P dans \mathbb{K} , chacune de multiplicité m_i , et $m_1 + \dots + m_r = n = \deg(P)$.

Exemples :

- $P = X^6 - 3X^5 - 15X^4 + 87X^3 - 162X^2 + 132X - 40 = (X - 2)^3 (X + 5) (X - 1)^2$ est un polynôme scindé sur \mathbb{R} .

- $P = X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$ n'est pas scindé sur \mathbb{R} mais il l'est sur \mathbb{C} car on peut écrire $P = (X - 1)(X + 1)(X - i)(X + i)$.

Proposition : si P est un polynôme de $\mathbb{K}[X]$ qui est **scindé et unitaire**, alors il peut s'écrire

$$P = X^n + \sum_{k=0}^{n-1} a_k X^k \quad \text{et} \quad P = \prod_{i=1}^n (X - \alpha_i)$$

où les α_i représentent les racines de P , pas nécessairement deux à deux distinctes. En développant la seconde écriture et en identifiant, on obtient les deux relations racines/coefficients (entre autres)

$$\alpha_1 + \alpha_2 + \dots + \alpha_n = -a_{n-1} \quad (\text{somme} - P \text{ unitaire})$$

$$\alpha_1 \alpha_2 \dots \alpha_n = (-1)^n a_0 \quad (\text{produit} - P \text{ unitaire})$$

Cas général : si P est scindé (de degré $n \geq 1$ mais pas forcément unitaire) alors

$$P = a_n X^n + \sum_{k=0}^{n-1} a_k X^k = a_n \left(X^n + \sum_{k=0}^{n-1} \frac{a_k}{a_n} X^k \right) = a_n \prod_{i=1}^n (X - \alpha_i),$$

et on en déduit les formules générales

$$\alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n} \quad (\text{somme})$$

$$\alpha_1 \alpha_2 \dots \alpha_n = (-1)^n \frac{a_0}{a_n} \quad (\text{produit})$$

Complément on obtient d'autres relations entre les racines et coefficients, qui peuvent se résumer, pour tout entier r compris entre 1 et n , par (somme des produits de r racines parmi les n)

$$\sum_{i_1 < i_2 < \dots < i_r} (\alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_r}) = (-1)^r \frac{a_{n-r}}{a_n}.$$

Les relations données précédemment s'obtiennent respectivement pour $r = 1$ et $r = n$.

Exemple :

- $n = 2$: $P = aX^2 + bX + c = a(X - \alpha_1)(X - \alpha_2)$. On a

$$\alpha_1 + \alpha_2 = -\frac{a_1}{a_2} = -\frac{b}{a} \quad \text{et} \quad \alpha_1 \alpha_2 = (-1)^2 \frac{a_0}{a_2} = \frac{c}{a}.$$

- $n = 3$: $P = aX^3 + bX^2 + cX + d = a(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$. On a

$$\alpha_1 + \alpha_2 + \alpha_3 = -\frac{a_1}{a_3} = -\frac{b}{a} \quad \text{et} \quad \alpha_1 \alpha_2 \alpha_3 = (-1)^3 \frac{a_0}{a_3} = -\frac{d}{a}.$$

On récupère également $\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = (-1)^2 \frac{a_1}{a_3} = \frac{c}{a}$.

A retenir : $X^2 - sX + p$ est un polynôme de degré deux dont la somme des racines vaut s et le produit p .

A retenir : $(x + y = s \text{ et } xy = p) \Leftrightarrow (x \text{ et } y \text{ sont les racines du polynôme } X^2 - sX + p)$

III : factorisation des polynômes dans $\mathbb{K}[X]$

Théorème de d'Alembert-Gauss

Théorème (admis) :

tout polynôme de $\mathbb{C}[X]$ (à coefficients complexes) *non constant* (de degré ≥ 1) possède *au moins* une racine complexe (dans \mathbb{C}).

Attention : il y a des polynômes à coefficients réels qui n'ont pas de racine réelle (exemple : $X^2 + 1$, $X^4 + 7X^2 + 5$), mais ceux-ci auront, d'après le théorème, au moins une racine complexe.

Conséquence : tout polynôme de $\mathbb{C}[X]$ (à coefficients complexes) est scindé sur \mathbb{C} .

Preuve : en cours.

Ainsi, tout polynôme non constant et à coefficients réels ou complexes peut nécessairement se factoriser sous la forme $a_n \prod_{i=1}^r (X - \alpha_i)^{m_i}$, avec $a_n, \alpha_1, \alpha_2, \dots, \alpha_r$ des nombres complexes.

Par conséquent, le degré de tout polynôme est égal au nombre de ses racines complexes, chacune étant comptée avec son ordre de multiplicité.

Attention : c'est bien sûr faux en général dans $\mathbb{R}[X]$. Par exemple $X^2 + 1$, $X^4 + 1$ ne sont pas scindés sur \mathbb{R} . Mais peut-être est-il possible de les factoriser avec des polynômes, à coefficients réels et de degrés plus petits ? Le paragraphe suivant traite ce problème.

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

Définition : un polynôme non-constant P de $\mathbb{K}[X]$ est dit **irréductible dans $\mathbb{K}[X]$** s'il ne peut pas se factoriser par des polynômes de $\mathbb{K}[X]$ de degrés strictement plus petits que $\deg(P)$.

Autrement dit, P est irréductible si ses seuls diviseurs sont les polynômes constants non-nuls et les polynômes associés à P .

Autre présentation, $P \in \mathbb{K}[X]$, non constant, est irréductible dans $\mathbb{K}[X]$ si, dès que $P = A \times B$ avec A et B polynômes dans $\mathbb{K}[X]$, on a nécessairement A ou B qui est constant (non nul).

Proposition : dans $\mathbb{K}[X]$ (avec $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}), les polynômes de degré 1 sont irréductibles.

Preuve : c'est évident, car si $\deg(P) = 1$ avec $P = AB$, alors, en passant aux degrés, on tire $1 = \deg(A) + \deg(B)$, donc $\deg(A) = 0$ ou $\deg(B) = 0$ (i.e) A ou B est constant (non-nul).

Proposition :

dans $\mathbb{C}[X]$, les polynômes irréductibles sont exactement les polynômes de degré 1.

C'est équivalent à dire que dans $\mathbb{C}[X]$, tout polynôme de degré ≥ 2 peut se factoriser avec des polynômes de degré 1 (i.e n'est pas irréductible)!

Preuve : soit $P \in \mathbb{C}[X]$ avec $\deg(P) = n \geq 2$. On sait que P est scindé sur \mathbb{C} , donc peut s'écrire sous la forme $P = a_n \prod_{i=1}^n (X - \alpha_i) = a_n (X - \alpha_n) \times \prod_{i=1}^{n-1} (X - \alpha_i)$, qui est donc un produit de deux polynômes de degrés au moins égaux à 1, donc P n'est pas irréductible. CQFD!

Proposition : les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement

- les polynômes de degré un
- les polynômes de degré deux sans racine réelle (à discriminant strictement négatif).

Preuve : en cours. Au passage, on rappelle le lemme suivant (utile dans la démonstration)

Lemme : si P est un polynôme à coefficients réels et α un complexe, alors on a l'équivalence

$$(P(\alpha) = 0) \Leftrightarrow (P(\bar{\alpha}) = 0).$$

Conséquence de la proposition : tout polynôme à coefficients réels et de degré supérieur à 3 peut se factoriser en des polynômes de degrés inférieurs (dans $\mathbb{R}[X]$). En itérant le procédé, on aboutit à une factorisation de ce polynôme ne comportant que des polynômes de degré 1 ou 2 (dans $\mathbb{R}[X]$).

Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$

Théorème : tout polynôme de $\mathbb{K}[X]$ admet une, et une seule décomposition en un produit de facteurs irréductibles de $\mathbb{K}[X]$.

Preuve : l'existence est immédiate, il suffit de factoriser les facteurs un par un tant qu'ils ne sont pas irréductibles! On admet l'unicité. Au passage, il faut comprendre que l'unicité de la décomposition est définie à l'ordre des facteurs irréductibles et à des constantes multiplicatives (non nulles) près.

Exemple : $(3X + 4)(2X - 1) = (2X - 1)(3X + 4) = (X - \frac{1}{2})(6X + 8) = 6(X - \frac{1}{2})(X + \frac{4}{3})$.

Cas particulier de $\mathbb{C}[X]$: tout polynôme non constant P de $\mathbb{C}[X]$ peut se factoriser en

$$P = a_n \prod_{i=1}^r (X - \alpha_i)^{m_i}$$

où a_n et les α_i sont complexes, $m_i \in \mathbb{N}$, $a_n \neq 0$ et $m_1 + m_2 + \dots + m_r = n = \deg(P)$.

Cas particulier de $\mathbb{R}[X]$: tout polynôme non constant P de $\mathbb{R}[X]$ peut se factoriser en

$$P = a_n \prod_{i=1}^s (X - \alpha_i)^{m_i} \prod_{j=1}^t (X^2 + b_j X + c_j)^{n_j}$$

où a_n et les α_i, b_j, c_j sont des réels, $a_n \neq 0$, $b_j^2 - 4c_j < 0$ (discriminant négatif), $m_i \in \mathbb{N}$, $n_j \in \mathbb{N}$ et $m_1 + m_2 + \dots + m_r + 2n_1 + 2n_2 + \dots + 2n_s = n = \deg(P)$.

Un exemple important

Soit $n \in \mathbb{N}^*$ et $P = X^n - 1$. On sait (voir cours sur les nombres complexes) que ce polynôme P possède exactement n racines distinctes, les racines $n^{\text{ièmes}}$ de l'unité, les $\omega_0, \omega_1, \dots, \omega_{n-1}$ où $\omega_k = e^{\frac{2ik\pi}{n}}$.

La factorisation sur $\mathbb{C}[X]$ est donc $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) = (X - 1) \prod_{k=1}^{n-1} (X - e^{\frac{2ik\pi}{n}})$.

Pour obtenir la factorisation en produits de facteurs irréductibles sur $\mathbb{R}[X]$, il suffit de regrouper les facteurs «conjugués» de la forme $(X - \omega)(X - \bar{\omega}) = X^2 - sX + p$ où $s = \omega + \bar{\omega} = 2\text{Re}(\omega)$ et $p = \omega\bar{\omega} = |\omega|^2$ sont des réels!

Exemples :

- $X^2 - 1 = (X - 1)(X + 1)$ sur $\mathbb{C}[X]$ et $\mathbb{R}[X]$.
- $X^3 - 1 = (X - 1)(X - j)(X - \bar{j})$ sur $\mathbb{C}[X]$ (où $j = e^{\frac{2i\pi}{3}}$), et $X^3 - 1 = (X - 1)(X^2 + X + 1)$ sur $\mathbb{R}[X]$.
- $X^4 - 1 = (X - 1)(X + 1)(X - i)(X + i)$ sur $\mathbb{C}[X]$, et $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$ sur $\mathbb{R}[X]$.
- $X^5 - 1 = (X - 1)(X - \omega)(X - \omega^2)(X - \omega^3)(X - \omega^4) = (X - 1)(X - \omega)(X - \omega^2)(X - \bar{\omega}^2)(X - \bar{\omega})$ sur $\mathbb{C}[X]$ avec $\omega = e^{\frac{2i\pi}{5}}$, et $X^5 - 1 = (X - 1) \left(X^2 + \left(\frac{1 - \sqrt{5}}{2} \right) X + 1 \right) \left(X^2 + \left(\frac{1 + \sqrt{5}}{2} \right) X + 1 \right)$ sur $\mathbb{R}[X]$.

Forme à retenir : $X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \dots + X + 1)$, mais qui n'est pas une factorisation en produit de facteurs irréductibles sur $\mathbb{R}[X]$ (sauf si $n = 2$).

IV : caractérisation de l'ordre de multiplicité d'une racine

Notions de dérivation dans $\mathbb{K}[X]$

Définition : si P est constant, on pose $D(P) = P' := 0$.

Sinon, avec $P = \sum_{k=0}^n a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ ($n \geq 1$), on pose

$$D(P) = P' := \sum_{k=1}^n k a_k X^{k-1} = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \dots + 2 a_2 X + a_1.$$

De manière plus générale, avec $P = \sum_{k \geq 0} a_k X^k$, on a $D(P) = \sum_{k \geq 1} k a_k X^{k-1}$.

On dit que $D(P) = P'$ est le **polynôme dérivé** de P .

Il est facile de vérifier que D est un endomorphisme de l'espace vectoriel $\mathbb{K}[X]$ (i.e)

$$D(\lambda P + \mu Q) = \lambda D(P) + \mu D(Q).$$

De même, on vérifie facilement la propriété suivante, pour tout $(P, Q) \in \mathbb{K}[X]^2$:

$$D(P \times Q) = D(P) \times Q + P \times D(Q) \text{ (i.e) } \boxed{D(PQ) = D(P)Q + PD(Q)}.$$

Ce résultat permet alors de prouver, par récurrence simple sur n , la **formule de Leibniz** qui donne la dérivée $n^{\text{ième}}$ d'un produit de deux polynômes :

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

ce qui peut s'écrire, avec la notation usuelle de dérivée $n^{\text{ième}}$ d'une fonction,

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

Caractérisation de l'ordre de multiplicité d'une racine d'un polynôme

On rappelle la définition vue pour l'ordre de multiplicité d'une racine α d'un polynôme $P \in \mathbb{K}[X]$.

- α est une racine du polynôme P d'ordre de multiplicité supérieur ou égal à k
si $(X - \alpha)^k$ divise P .

Autrement dit :

$$(\alpha \text{ est une racine d'ordre } \geq k \text{ de } P) \Leftrightarrow (\exists Q \in \mathbb{K}[X], P = (X - \alpha)^k Q).$$

- α est une racine du polynôme P d'ordre de multiplicité (*exactement*) m
si $(X - \alpha)^m$ divise P et si $(X - \alpha)^{m+1}$ ne divise pas P .

Autrement dit :

$$(\alpha \text{ est une racine d'ordre } m \text{ de } P) \Leftrightarrow (\exists Q \in \mathbb{K}[X], P = (X - \alpha)^m Q \text{ et } Q(\alpha) \neq 0).$$

Vocabulaire

Une racine d'ordre 1 (2, 3, ...) d'un polynôme P est dite racine simple (double, triple,...) de P .

On rappelle qu'on a pris la convention : $\boxed{\alpha \text{ est une racine d'ordre } 0 \text{ de } P \text{ si } \alpha \text{ n'est pas racine de } P}$.

Remarque : l'ordre de multiplicité est unique. En effet, supposons que α soit racine de P d'ordre m et n avec $m < n$. Il existe donc R et S dans $\mathbb{K}[X]$ tels que $\tilde{R}(\alpha) \neq 0$, $\tilde{S}(\alpha) \neq 0$ et $P = (X - \alpha)^m R = (X - \alpha)^n S = (X - \alpha)^m (X - \alpha)^{n-m} S$. Par régularité de $(X - \alpha)^m \neq \tilde{0}$, on en déduit l'égalité $R = (X - \alpha)^{n-m} S$, puis $\tilde{R}(\alpha) = 0^{n-m} \tilde{S}(\alpha) = 0$ car $n - m > 0$, ce qui est absurde !

Exemples

- 1 est une racine d'ordre 1 de $A = X^3 - 1$ car $A = (X - 1)Q$ avec $Q = 1 + X + X^2$ et $Q(1) = 3 \neq 0$.
 - -2 est une racine d'ordre 2 de $B = X^4 - 17X^2 - 36X - 20$ car $B = (X + 2)^2 R$ avec $R = X^2 - 4X - 5$ et $R(-2) = 7 \neq 0$.
 - 2 est une racine d'ordre ≥ 2 de $C = X^5 - 6X^4 + 11X^3 - 2X^2 - 12X + 8 = (X - 2)^2 (X^3 - 2X^2 - X + 2)$.
- Mieux : 2 est une racine de C d'ordre 3 car $C = (X - 2)^3 T$ avec $T = X^2 - 1$ et $T(2) = 3 \neq 0$.

On cherche un critère plus pratique à utiliser pour caractériser l'ordre de multiplicité d'une racine. Pour commencer, on établit un premier résultat utile pour la suite.

Lemme

Soit $P \in \mathbb{K}[X]$, un polynôme, α un élément du corps \mathbb{K} et $m \geq 1$, un entier naturel non nul.

$$\boxed{(\alpha \text{ est une racine d'ordre } m \text{ de } P) \Leftrightarrow (\alpha \text{ est une racine d'ordre } m - 1 \text{ de } P' = P^{(1)} \text{ ET } P(\alpha) = 0)}$$

Preuve

Sens « \Rightarrow »

On suppose que α est une racine de P d'ordre m (avec $m \geq 1$). On a donc bien $P(\alpha) = 0$ et il existe un polynôme $S \in \mathbb{K}[X]$ tel que :

$$P = (X - \alpha)^m S \text{ et } S(\alpha) \neq 0.$$

En dérivant cette égalité, on obtient :

$$P' = m(X - \alpha)^{m-1}S + (X - \alpha)^m S' = (X - \alpha)^{m-1}(mS + (X - \alpha)S') = (X - \alpha)^{m-1}T$$

où $T = mS + (X - \alpha)S'$ vérifie $T(\alpha) = mS(\alpha) + 0S'(\alpha) = mS(\alpha) \neq 0$ car $m \geq 1$ et $S(\alpha) \neq 0$.

Ceci signifie exactement que α est une racine d'ordre $m - 1$ du polynôme P' .

Sens « \Leftrightarrow »

On utilise ici le sens direct « \Rightarrow » qui vient d'être démontré pour prouver le sens réciproque « \Leftarrow ».

Supposons que α est une racine d'ordre $m - 1$ de P' et $P(\alpha) = 0$. Puisque α est une racine de P , notons r son ordre de multiplicité ($r \geq 1$). D'après le sens direct « \Rightarrow », on peut en déduire que α est une racine de P' d'ordre $r - 1$. Or, par hypothèse cet ordre est $m - 1$, d'où, par unicité de l'ordre de multiplicité, $r = m$! Et c'est FINI !

Proposition (caractérisation de l'ordre de multiplicité à l'aide des dérivées $n^{\text{ièmes}}$)

Soit $P \in \mathbb{K}[X]$, un polynôme, α un élément du corps \mathbb{K} et $m \geq 1$, un entier naturel non nul.

$$(\alpha \text{ est une racine de } P \text{ d'ordre } m) \Leftrightarrow (P(\alpha) = P^{(1)}(\alpha) = P^{(2)}(\alpha) = \dots = P^{(m-1)}(\alpha) = 0 \text{ ET } P^{(m)}(\alpha) \neq 0)$$

Pour retenir :

l'ordre de multiplicité de α = le nombre d'annulations successives de P et de ses dérivées évaluées en α .

Preuve

On applique le lemme démontré précédemment tant que c'est possible (i.e tant que l'ordre est ≥ 1) à P , puis à $P' = P^{(1)}$, puis à $P'' = P^{(2)}$, puis à $P^{(3)}$, ..., puis à $P^{(m-2)}$, puis à $P^{(m-1)}$. On y va :

(α est une racine de P d'ordre m)

\Leftrightarrow (α est une racine de $P^{(1)}$ d'ordre $m - 1$ et $P(\alpha) = 0$)

\Leftrightarrow (α est une racine de $P^{(2)}$ d'ordre $m - 2$ et $P^{(1)}(\alpha) = 0$ et $P(\alpha) = 0$)

\Leftrightarrow (α est une racine de $P^{(3)}$ d'ordre $m - 3$ et $P^{(2)}(\alpha) = 0$ et $P^{(1)}(\alpha) = P(\alpha) = 0$)

\Leftrightarrow (α est une racine de $P^{(4)}$ d'ordre $m - 4$ et $P^{(3)}(\alpha) = 0$ et $P^{(2)}(\alpha) = P^{(1)}(\alpha) = P(\alpha) = 0$)

(...)

\Leftrightarrow (α est une racine de $P^{(m-2)}$ d'ordre 2 et $P^{(m-3)}(\alpha) = 0$ et $P^{(m-4)}(\alpha) = \dots = P^{(1)}(\alpha) = P(\alpha) = 0$)

\Leftrightarrow (α est une racine de $P^{(m-1)}$ d'ordre 1 et $P^{(m-2)}(\alpha) = 0$ et $P^{(m-3)}(\alpha) = \dots = P^{(1)}(\alpha) = P(\alpha) = 0$)

\Leftrightarrow (α est une racine de $P^{(m)}$ d'ordre 0 et $P^{(m-1)}(\alpha) = 0$ et $P^{(m-2)}(\alpha) = \dots = P^{(1)}(\alpha) = P(\alpha) = 0$)

Or cette dernière proposition signifie exactement :

α n'est pas racine de $P^{(m)}$ (i.e) $P^{(m)}(\alpha) \neq 0$ ET

$P^{(m-1)}(\alpha) = P^{(m-2)}(\alpha) = \dots = P^{(1)}(\alpha) = P(\alpha) = 0$. CQFD !

Un exemple : soit $P = 2X^4 - 5X^3 + 3X^2 + X - 1$. On remarque que $P(1) = 0$. Donc 1 est une racine de P , notons m son ordre de multiplicité. Pour l'instant, on peut juste affirmer que $m \geq 1$.

Mais $P^{(1)} = P' = 8X^3 - 15X^2 + 6X + 1$ et $P'(1) = 0$, donc $m \geq 2$.

Mais $P^{(2)} = P'' = 24X^2 - 30X + 6$ et $P^{(2)}(1) = 0$, donc $m \geq 3$.

Mais $P^{(3)} = 48X - 30$ et $P^{(3)}(1) \neq 0$, donc $m = 3$.

On a prouvé : 1 est une racine de P d'ordre de multiplicité égal à 3.

On sait alors qu'il existe $Q \in \mathbb{R}[X]$ tel que $P = (X - 1)^3 Q$, avec ici $Q = aX + b$ (examiner les degrés).

Une division euclidienne de P par $(X - 1)^3 = X^3 - 3X^2 + 3X - 1$ fournit $Q = 2X + 1$.