

EC 222. Polynômes

Partie 3: Arithmétique des polynômes

Jean-François Culus

17 février 2016

Cadrage

Ici, $(\mathbb{K}, +, \times)$ est l'un des corps $\mathbb{R}$ ou $\mathbb{C}$. Aussi, on identifie le polynôme P et fonction polynomiale $\tilde{P}$.

- Division euclidienne dans $\mathbb{K}[X]$
- Racine d'un polynôme / ordre de multiplicité
- Polynôme scindé
- Décomposition des polynômes de $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

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

Théorème : Division euclidienne

Pour tout $(A, B) \in \mathbb{K}[X]^2$ ($B \neq 0$), il existe un unique couple $(Q; R) \in \mathbb{K}[X]^2$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$. On dit que Q est le quotient et R le reste de la division euclidienne de A par B .

Une conséquence importante

Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Alors le reste de la division euclidienne de P par $(X - \lambda)$ est $R = P(\lambda)$.

$P(X) = Q(X)(X - \lambda) + R(X)$ avec $\deg(R) < \deg(X - \lambda) = 1$
donc R est une constante. $\forall x \in \mathbb{R}, \tilde{P}(x) = \tilde{Q}(x) \times (x - \lambda) + R$.
En évaluant en λ , on obtient $P(\lambda) = R$.

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

Démo :

Soit $B \neq 0$ fixé. On raisonne par récurrence forte sur le degré de A .

Initialisation : Si $\deg(A) = 0$ (ie. A est une constante non nulle), alors si $\deg(B) = 0$, $Q = AB^{-1}$ et $R = 0$, sinon $\deg(B) > 0 = \deg(A)$ alors $Q = 0$ et $R = A$.

De même, si $\deg(A) < \deg(B)$, on pose $Q = 0$ et $R = A$ et on a bien $A = BQ + R$ avec $\deg(R) < \deg(B)$.

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

Démo :

Hérédité : Supposons la propriété vraie pour tout polynôme de degré $\leq n$ et soit A de degré $n + 1$.

Notons a le coeff dominant de A et b le coeff dominant de B .

Posons : $P = A - ab^{-1}BX^{\deg(A)-\deg(B)}$.

On a $\deg(P) \leq n$ d'où $\exists (Q_P; R_P)$ tels que $P = Q_P B + R_P$ avec $\deg(R_P) < \deg(B)$. Donc $A - ab^{-1}BX^{\deg(A)-\deg(B)} = Q_P B + R_P$ d'où

$$A = \underbrace{(Q_P + ab^{-1}X^{\deg(A)-\deg(B)})}_{=Q} B + \underbrace{R_P}_{=R}$$

Racine & double nature des polynômes

Définition : Racine d'un polynôme

Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On dit que λ est une racine de P si P est un multiple de $(X - \lambda)$.

Caractérisation algébrique

λ racine de P ssi le reste de la division euclidienne de P par $(X - \lambda)$ est nul.

Caractérisation analytique

$\lambda \in \mathbb{K}$ est racine de P ssi $\tilde{P}(\lambda) = 0$.

Polynômes premiers entre eux

Définition : Premiers entre eux

Soient A, B deux polynômes de $\mathbb{K}[X]$. On dit que A et B sont premiers entre eux s'ils n'ont pas de racine commune.

Théorème de Bezout

Les polynômes A et B sont premiers entre eux si et seulement si il existe $(U, V) \in \mathbb{K}[X]^2$ tels que $UA + VB = 1$.

Théorème de Gauss

Soient A, B, C trois polynômes tels que A et B sont premiers entre eux. Si $A|BC$, alors $A|C$.

Un exemple Algorithme d'Euclide & Bezout

cf : <http://homeomath2.immingo.net/polyeuc.htm>

$A(X) = 2X^4 - 3X^3 - 3X - 2$ et $B(X) = X^2 - 1$.

- **Algorithme d'Euclide**

$$A(X) = (2X^2 - 3X + 2)B(X) - 6X$$

$$B(X) = \left(-\frac{1}{6}X\right)(-6X) - 1.$$

- **Coefficients de Bezout**

$$-1 = B(X) + \frac{1}{6}X(-6X).$$

$$-1 = B(X) + \frac{1}{6}X[A(X) - (2X^2 - 3X + 2)B(X)]$$

$$-1 = \frac{X}{6}A(X) + \left[1 - \frac{X}{6}(2X^2 - 3X + 2)\right] B(X)$$

$$1 = \frac{-X}{6}A(X) + \left(\frac{X^3}{3} - \frac{X^2}{2} + \frac{1}{3}X - 1\right) B(X)$$

Racines (simples) & polynôme

$$(X - \lambda_1) = 1 \times (X - \lambda_2) + (\lambda_1 - \lambda_2).$$

Proposition (conséquence du théorème de Gauss)

Soit $P \in \mathbb{K}[X]$ et $\lambda_1, \lambda_2, \dots, \lambda_k$ des éléments de $\mathbb{K}$ tous différents. Alors $(X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_k) \mid P$ si et seulement si $\tilde{P}(\lambda_1) = \tilde{P}(\lambda_2) = \dots = \tilde{P}(\lambda_k) = 0$.

Théorème

$P \in \mathbb{K}[X]$ possède au plus $\deg(P)$ racines différentes.

Corollaire

Si $\deg(P) \leq k - 1$ et P admet k racines, alors $P = 0$.

Ordre de multiplicité d'une racine

Définition : Ordre de multiplicité d'une racine

Soit $P \in \mathbb{K}[X]$. On dit que $\lambda \in \mathbb{K}$ est racine d'ordre de multiplicité k si $(X - \lambda)^k \mid P$ et $(X - \lambda)^{k+1} \nmid P$.

Caractérisation analytique

$\lambda \in \mathbb{K}$ est une racine d'ordre de multiplicité k de P si $\tilde{P}(\lambda) = \tilde{P}'(\lambda) = \tilde{P}''(\lambda) = \dots = \tilde{P}^{(k)}(\lambda) = 0$ et $\tilde{P}^{(k+1)}(\lambda) \neq 0$.

Exemple $P(X) = (X - 1)^3 = X^3 - 3X^2 + 3X - 1$ alors $\tilde{P}'(x) = 3x^2 - 6x + 3$, $\tilde{P}''(x) = 6x - 6$ et $\tilde{P}^{(3)}(x) = 6$.

Racines (multiples) & polynôme

Théorème

Soient $\lambda_1, \dots, \lambda_k$ des racines de P , deux à deux différentes, d'ordre de multiplicité respective $d_1, d_2, \dots, d_k$.

Alors $(X - \lambda_1)^{d_1} (X - \lambda_2)^{d_2} \dots (X - \lambda_k)^{d_k} \mid P$.

Proposition

On a forcément $\sum_{i=1}^k d_i \leq \deg(P)$.

Corollaire

Si $\deg(P) \leq k - 1$ et P admet k racines comptées avec leur ordre de multiplicité, alors $P = 0$.

Polynôme scindé

Résumé :

Si P admet $\lambda_1, \lambda_2, \dots, \lambda_m$ pour racines d'ordre de multiplicité respectives $d_1, d_2, \dots, d_m$, alors $\prod_{i=1}^m (X - \lambda_i)^{d_i} | P$ et $\sum_{i=1}^m d_i \leq \deg(P)$.

Si de plus $\sum_{i=1}^m d_i = \deg(P) = d$, alors $P(X) = \alpha \prod_{i=1}^m (X - \lambda_i)^{d_i}$

Quelle est encore la question ?

Si $\lambda_1, \dots, \lambda_m$ sont toutes les racines de P , est-ce que P s'écrit $P(X) = \alpha \prod_{i=1}^m (X - \lambda_i)^{d_i}$?

Définition : Polynôme scindé

Le polynôme $P \in \mathbb{K}[X]$ est scindé si et seulement si $P = \alpha \prod_{i=1}^d (X - \lambda_i) = \alpha \prod_{i=1}^m (X - \lambda_i)^{d_i}$.

Exemples : Le polynôme $P(X) = X^2 - 1$ est scindé sur $\mathbb{R}$ et $\mathbb{C}$.
Le polynôme $Q(X) = X^2 + 1$ est scindé sur $\mathbb{C}$ mais non dans $\mathbb{R}$.

Définition : Polynôme irréductible

Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible s'il n'est pas constant et s'il ne peut s'écrire comme produit de polynômes non constants.

La question est donc : est-ce que les polynômes irréductibles de $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont uniquement les polynômes de degré 1 ?

Décomposition d'un polynôme dans $\mathbb{C}$

Théorème de d'Alembert-Gauss

Le corps des complexes $\mathbb{C}$ est algébriquement clos (ie. tout polynôme P non constant admet une racine dans $\mathbb{C}$).

Corollaires

Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Tout polynôme est scindé dans $\mathbb{C}$.

Décomposition dans $\mathbb{C}$

Si $P \in \mathbb{C}[X]$ et $\deg(P) = d$, alors

$$P = \alpha \prod_{i=1}^m (X - \lambda_i)^{d_i} \quad \text{avec} \quad \sum_{i=1}^m d_i = d$$

Décomposition d'un polynôme dans $\mathbb{R}$

Irréductibles de $\mathbb{R}$

Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

Décomposition dans $\mathbb{R}$

Si $P \in \mathbb{R}[X]$ et $\deg(P) = d$, alors

$$P = \alpha \prod_{i=1}^m (X - \lambda_i)^{d_i} \times Q_1(X) \times Q_2(X) \times \dots \times Q_\ell(X)$$

avec $\deg(Q_i) = 2$, $\Delta(Q_i) < 0$ et $\sum_{i=1}^m d_i + 2\ell = d$.

Irréductibles vs. avoir une racine

Faire attention

- $(X - 1)$ est irréductible (dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$) mais admet (évidemment) une racine.
- $(X^2 + 1)(X^2 + 2)$ n'admet pas de racines réelles mais est réductible dans $\mathbb{R}[X]$.

Qu'est-ce qui est vrai alors ?

- Si P admet au moins 2 racines différentes, alors il est réductible.