MathComp - Algèbre
Arithmétique sur $K[X]$

Pierre-Alain Fouque

Université de Rennes 1

Septembre 2020

Agenda

1. Degré
2. Idéaux de $K[X]$ - pgcd - ppcm
3. Polynômes irréductibles
4. Théorème fondamental de l'arithmétique de $K[X]$
5. Racines d'un polynôme

Degré

Definition (Application degré)

Soit $F = (a_i)_{i \geq 0}$ un polynôme à coefficients dans K

1. $\deg : K[X] \to \mathbb{N} \cup \{-\infty\}$
2. Si $F = 0$ i.e. si tous les a_i sont nuls, on pose $\deg(F) = -\infty$.
3. Si $F \neq 0$, $\deg(F)$ est le plus grand entier $n \geq 0$ tq $a_n \neq 0$

On dit que $\deg(F)$ est le degré de F

Lemme

Soient P et Q deux éléments de $K[X]$

1. $\deg(P+Q) \leq \max(\deg(P), deg(Q))$ *; égalité si* $\deg(P) \neq \deg(Q)$
2. $\deg(PQ) = \deg(P) + \deg(Q)$
3. *L'anneau $K[X]$ est intègre et le groupe de ses éléments inversibles est K (éléments non nuls de K)*

Division euclidienne dans $K[X]$

Theorem

Soient A et B deux polynômes de $K[X]$ tq $B \neq 0$. Il existe un unique couple $(Q, R) \in (K[X])^2$ tq $A = BQ + R$, $\deg R < \deg B$
Q, R est le quotient, reste de la division euclidienne de A par B

Lemme

U et V polynômes de $K[X]$ tq $V \neq 0$ et $\deg(U) \geq \deg(V)$ Alors, il existe $Q \in K[X]$ tq $\deg(U - VQ) < \deg(U)$

Definition (A et B deux polynômes)

B divise A, A est multiple de B, s'il existe $Q \in K[X]$ tq $A = BQ$.
Si $B \neq 0$, le reste de la division euclidienne de A par B est nul

Lemme (A et B deux polynômes non nuls)

Si A divise B et que B divise A, il existe $\lambda \in K$ non nul tq $A = \lambda B$
On dit alors que A et B sont associés.

Idéaux de $K[X]$

Definition

P est un polynôme de $K[X]$. L'ensemble $(P) = \{PR | R \in K[X]\}$ est un idéal de $K[X]$. C'est l'idéal de $K[X]$ engendré par P

Theorem

I un idéal non nul de $K[X]$. Il existe un unique polynôme unitaire $P \in K[X]$ tq $I = (P)$

Theorem

Deux polynômes A et B de $K[X]$ non tous les deux nuls, et $I = \{AU + BV | U, V \in K[X]\}$. Il existe un unique polynôme unitaire $D \in K[X]$ tq $I = (D)$, appelé le pgcd de A et B.
Il existe U et V dans $K[X]$ tq $D = AU + BV$

pgcd

Theorem

F un polynôme unitaire de $K[X]$. F est le pgcd de A et B ssi les deux conditions suivantes sont satisfaites :

1. *le polynôme F divise A et B.*
2. *Tout diviseur de A et B dans $K[X]$ divise F.*

Definition

A et B premiers entre eux, ou que A est premier avec B, si $D = 1$

Corollary

A et B premiers entre eux ssi $\exists (U, V) \in (K[X])^2$ tq $AU + BV = 1$

Theorem (Gauss)

Soient F, G et H des polynômes de $K[X]$ tq F divise GH et F premier avec G. Alors, F divise H

ppcm

Definition

Deux polynômes non nuls A et B de $K[X]$. L'ensemble $(A) \cap (B)$ est un idéal de $K[X]$. Il existe donc un unique polynôme unitaire $M \in K[X]$ tq $(A) \cap (B) = (M)$, M est le plus petit commun multiple de A et B, ppcm de A et B

Theorem

F un polynôme unitaire de $K[X]$. Alors, F est le ppcm de A et B ssi les deux conditions suivantes sont vérifiées :

1. *le polynôme F est un multiple de A et B*
2. *Tout multiple de A et B dans $K[X]$ est un multiple de F*

Proposition

Soit D le pgcd de A et B. On a $(AB) = (DM)$.

Polynômes irréductibles

Definition

Un polynôme de $K[X]$ est dit irréductible (dans $K[X]$) si son degré est supérieur ou égal à 1 et si l'ensemble de ses diviseurs est formé des éléments non nuls de K et des polynômes qui lui sont associés.

Definition

Un polynôme $P \in K[X]$ de degré ≥ 1 est irréductible s'il ne possède pas de diviseur $Q \in K[X]$ tq $1 \leq \deg(Q) \leq \deg(P) - 1$. C'est le cas des polynômes de degré 1. Ce sont les seuls si K est le corps $\mathbb{C}$ des nombres complexes. Deux polynômes irréductibles de $K[X]$ sont premiers entre eux ou sont associés. Un polynôme qui n'est pas irréductible est dit réductible.

Théorème fondamental de l'arithmétique de $K[X]$

Theorem

Soit $\mathbb{P}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. P polynôme non nul de $K[X]$ s'écrit de manière unique sous la forme $P = \lambda \prod_{F \in \mathbb{P}} F^{n_F}$, où $\lambda \in K$, et où les n_F sont des entiers naturels nuls sauf un nombre fini d'entre eux

Lemme

Soit A un polynôme irréductible divisant un produit de polynômes $A_1 \cdots A_r$ dans $K[X]$. Alors, A divise l'un des A_i.

Corollary

Soient $P = \lambda \prod_{F \in \mathbb{P}} F^{n_F}$ et $Q = \mu \prod_{F \in \mathbb{P}} F^{m_F}$, D et M, le pgcd et le ppcm de P et Q.

$$D = \lambda \prod_{F \in \mathbb{P}} F^{Min(n_F, m_F)} \text{ et } M = \mu \prod_{F \in \mathbb{P}} F^{Max(n_F, m_F)}$$

Racines d'un polynôme

Definition

Soit $P = a_0 + \ldots + a_n X^n$ un polynôme de $K[X]$. On appelle fonction polynôme associée à P l'application $\tilde{P} : K \to K$ définie par

$$\tilde{P}(x) = \sum_{i=0}^{n} a_i x^i \text{ quel que soit } x \in K$$

Definition

$P \in K[X]$ et a un élément de K. a est une racine de P si $P(a) = 0$

Lemme

Soient $P \in K[X]$ et a un élément de K. $P(a) = 0$ ssi $X - a$ divise P

Racine Multiple

Definition (Ordre de multiplicité d'une racine)

Soient P un polynôme non nul de $K[X]$ et $a \in K$ une racine de P. L'ordre de multiplicité de a (dans P) est le plus grand entier naturel r tq P soit divisible par $(X-a)^r$.
Si $r = 1$, a est racine simple de P, et si $r \geq 2$, a est une racine multiple de P.

Definition

(Polynôme dérivé). Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme de $K[X]$. Le polynôme dérivé de P, noté $P' = \sum_{i=1}^{n} ia_iX^{i-1}$

Proposition

Soit P un polynôme de $K[X]$. Pour qu'un élément $a \in K$ soit racine simple de P, il faut et il suffit que $P(a) = 0$ et $P'(a) \neq 0$

Racine Multiple (suite)

Theorem

Soient P un polynôme de $K[X]$ et $a_1, \ldots, a_k$ des éléments de K, distincts deux à deux, qui sont racines de P d'ordre de multiplicité $n_1, \ldots, n_k$ respectivement. Il existe un polynôme $Q \in K[X]$, tq

$$P = Q \prod_{i=1}^{k} (X - a_i)^{n_i},$$

et que $Q(a_i)$ soit non nul pour tout $i = 1, \ldots, k$.

Corollary

Soit P un polynôme non nul de degré n dans $K[X]$. Alors, P possède au plus n racines distinctes dans K.