Polynômes

Dans ce chapitre la lettre $\mathbb{K}$ désignera indifféremment $\mathbb{R}$ ou $\mathbb{C}$. Les lettres n et p désignent des entiers naturels.

Définition Soient A et B deux polynômes de $\mathbb{K}[X]$. On dit que A divise B (ou que A est un diviseur de B) et on note $A|B$ lorsque $\exists P \in \mathbb{K}[X]$ tel que $B = AP$. A divise B se note $A|B$.
On dit alors aussi dans ce cas que B est un multiple de A

Exemple Soient $A = (X - 1)^2(2X + 3)$ et $B = 2X + 3$. A est un multiple de B

Propriété La relation « être un diviseur de » est reflexive, transitive et antisymétrique.

- Réflexive : $\forall A \in \mathbb{K}[X], A|A$
- Transitive : Soient A, B et C trois polynômes de $\mathbb{K}[X]$. Si $A|B$ et $B|C$ alors $A|C$
- Antisymétrique : Soient A, B deux polynômes de $\mathbb{K}[X]$ non nuls. Si $A|B$ et $B|A$ alors $\exists \lambda \in \mathbb{K}$ tel que $A = \lambda B$

Preuve

- $A = A * 1$. Donc A divise A
- $A|B \Rightarrow \exists F \in \mathbb{K}[X]$ tel que $B = AF$. $B|C \Rightarrow \exists G \in \mathbb{K}[X]$ tel que $C = BG$ donc $C = BG = AFG$ donc $A|C$
- $A|B \Rightarrow \exists F \in \mathbb{K}[X]$ tel que $B = AF$. $B|A \Rightarrow \exists G \in \mathbb{K}[X]$ tel que $A = BG$ donc $A = AFG \Rightarrow \deg A = \deg A + \deg F + \deg G \Rightarrow \deg F = \deg G = 0$. F et G étant des polynômes de degré nuls, ils sont réduits à des constantes. Nous avons bien $\exists \lambda \in \mathbb{K}$ tel que $A = \lambda B$

Propriété Soient A et B deux polynômes de $\mathbb{K}[X]$ avec $A|B$. Alors $\deg(A) \leq \deg(B)$

Preuve

$$A|B \Rightarrow \exists P \in \mathbb{K}[X] \text{ tel que } B = AP \Rightarrow \deg(B) = \deg(A) + \deg(P) \Rightarrow \deg(A) \leq \deg(B)$$

Propriété Soient A, B et C trois polynômes de $\mathbb{K}[X]$.
Si $A|B$ et $A|C$ alors $\forall (F, G) \in (\mathbb{K}[X])^2, A|FB + GC$

Preuve

$A|B \Rightarrow \exists M \in \mathbb{K}[X]$ tel que $B = AM$.
 $A|C \Rightarrow \exists N \in \mathbb{K}[X]$ tel que $C = AN$
Donc $FB + GC = FAM + GAN = A(FM + GN)$ donc $A|FB + GC$

Propriété Soient A, B, C et D quatre polynômes de $\mathbb{K}[X]$.
Si $A|B$ et $C|D$ alors $AC|BD$

Preuve

$A|B \Rightarrow \exists M \in \mathbb{K}[X]$ tel que $B = AM$.
 $C|D \Rightarrow \exists N \in \mathbb{K}[X]$ tel que $D = NC$
Donc $BD = AMNC = (AC)(MN) \Rightarrow AC|BD$

Théorème Soient A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq \tilde{0}$
 $\exists! (Q, R) \in (\mathbb{K}[X])^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$
Ce théorème est dit théorème de la division euclidienne dans $\mathbb{K}[X]$. A est le dividende de la division, B le diviseur, Q le quotient, R le reste

Preuve

- Existence :

Si B divise A alors $A = B * Q + 0$. $R = \tilde{0}$ l'existence est donc démontrée. Dans le cas contraire :

Soit $F = \{\deg(A - BL), L \in \mathbb{K}[X]\}$

F est une sous partie de $\mathbb{N}$. Elle admet donc un plus petit élément : n .

Soient Q et R tels que $A = BQ + R$ avec $\deg(R) = n$.

Supposons que $\deg(R) \geq \deg(B)$. $\exists Q' \in \mathbb{K}[X]$ tel que $\deg(R - Q'B) < \deg(R)$. (Il suffit de choisir Q' pour que le coefficient dominant de R soit égal au coefficient dominant de $Q'B$)

Posons $R' = R - Q'B$. Nous avons $A = BQ + R = BQ + R' + Q'B = B(Q + Q') + R'$

Or $\deg(R') < \deg(R)$ nous sommes donc arrivés à une contradiction sur le fait que $\deg(R)$ soit le plus petit élément de $F = \{\deg(A - BL), L \in \mathbb{K}[X]\}$

- Unicité :

Supposons $\exists(Q_1, R_1)$ tel que $A = B * Q_1 + R_1$ avec $\deg(R_1) < \deg(B)$ et $\exists(Q_2, R_2)$ tel que $A = B * Q_2 + R_2$ avec $\deg(R_2) < \deg(B)$. Bien entendu nous supposons $Q_1 \neq Q_2$ et $R_1 \neq R_2$

En soustrayant ces deux lignes il nous vient :

$\tilde{0} = B(Q_1 - Q_2) + R_1 - R_2 \Rightarrow R_1 - R_2 = B(Q_2 - Q_1) \Rightarrow \deg(R_1 - R_2) \geq \deg(B)$

Or $\deg(R_1 - R_2) \leq \max(\deg(R_1), \deg(-R_2)) < \deg(B)$

Nous sommes donc arrivés à une contradiction. $Q_1 = Q_2$ et $R_1 = R_2$

Exemple	Réalisons la division euclidienne de $A = X^5 - X^4 - X^3 + 3X^2 - 2X$ par $B = X^2 - X + 1$
	$ \begin{array}{r} A = \quad X^5 \quad -X^4 \quad -X^3 \quad +3X^2 \quad -2X \quad +0 \\ \quad -X^5 \quad +X^4 \quad -X^3 \\ \qquad \qquad \qquad -2X^3 \quad +3X^2 \quad -2X \\ \qquad \qquad \qquad +2X^3 \quad -2X^2 \quad +2X \\ \qquad \qquad \qquad \qquad \qquad +X^2 \\ \qquad \qquad \qquad \qquad \qquad -X^2 \quad +X \quad -1 \\ R = \qquad \qquad \qquad \qquad \qquad +X \quad -1 \end{array} \left \begin{array}{l} X^2 \quad -X \quad +1 = B \\ X^3 \quad -2X \quad +1 = Q \end{array} \right. $
Propriété	Soient A et B deux polynômes de $\mathbb{K}[X]$. $A B$ dans $\mathbb{R}[X]$ ssi $A B$ dans $\mathbb{C}[X]$
Preuve	
<p>$A B$ dans $\mathbb{R}[X] \Rightarrow \exists Q \in \mathbb{R}[X]$ tel que $B = AQ \Rightarrow \exists Q \in \mathbb{C}[X]$ tel que $B = AQ$ donc $A B$ dans $\mathbb{C}[X]$</p> <p>Si $A B$ dans $\mathbb{C}[X]$ alors la division euclidienne dans $\mathbb{C}[X]$ nous permet d'écrire $B = AQ + \tilde{0}$ avec $Q \in \mathbb{C}[X]$</p> <p>Cette même division euclidienne dans $\mathbb{R}[X]$ nous permet d'écrire $B = AQ' + R'$ avec Q' et $R' \in \mathbb{R}[X]$</p> <p>Mais cette division euclidienne dans $\mathbb{R}[X]$ est aussi valable dans $\mathbb{C}[X]$.</p> <p>L'unicité de la division euclidienne dans $\mathbb{C}[X]$ nous permet donc de conclure $Q' = Q$ et $R' = \tilde{0}$</p> <p>Donc $A B$ dans $\mathbb{R}[X]$</p>	