Chapitre 16

Arithmétique des polynômes

16.1 Division euclidienne

Théorème 16.1

Soit $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]$ non nul, il existe un unique couple de polynômes (Q, R) tel que $A = BQ + R$ avec $\deg R < \deg B$. Le polynôme Q est appelé **quotient** et R le **reste**.

Existence :
On raisonne par récurrence sur le degré de A.

- Pour $n = \deg A = 0$. Soit $A \in \mathbb{K}[X]$.
  - Si $\deg B > 0$, alors $(0, A)$ convient.
  - Si $\deg B = 0$, le couple $(B^{-1} \times A, 0)$ convient (comme B est constant et non nul), alors $B \in \mathbb{K}^*$ donc inversible).
- On suppose le résultat vrai pour tout $A \in \mathbb{K}_n[X]$.
  Soit $A \in \mathbb{K}_{n+1}[X]$ avec $\deg A = n + 1$.
  On écrit $A = \underbrace{a}_{\neq 0} X^{n+1} + A_1$ avec $A_1 \in \mathbb{K}_n[X]$.
  - Si $\deg A < \deg B$, le couple $(0, A)$ convient.
  - Si $\deg A \geq \deg B$ et on note b le coefficient dominant de B :
  $$A - ab^{-1}B \times X^{n+1-\deg B} \in \mathbb{K}_n[X]$$
  D'après l'hypothèse de récurrence, on choisit $(Q, R) \in \mathbb{K}[X]^2$ tel que $\deg R < \deg B$ et $A - ab^{-1}B \times X^{n+1-\deg B} = QB + R$.
  Donc :
  $$A = \left[Q + ab^{-1}X^{n+1-\deg A}\right] \times B + R$$

Unicité :
On suppose que $A = BQ + R = BQ_1 + R_1$.
Donc :

$$\begin{aligned}
B(Q - Q_1) &= R_1 - R \\
\text{donc } \underbrace{\deg\left(B(Q - Q_1)\right)}_{\deg B + \deg Q - Q_1} &= \deg\left(R_1 - R\right) \\
&\leq \max(\deg R_1, \deg R) \\
&< \deg B \\
\text{donc } \deg\left(Q - Q_1\right) &< 0 \\
\text{donc } Q - Q_1 &= 0 \\
\text{puis } R_1 - R &= 0
\end{aligned}$$

16.7 Proposition 16.7

Propostion 16.7

On a :

1. Soit A et P deux polynômes non nuls. Si $A|P$ et si $P|A$, alors il existe $\alpha \in \mathbb{K}^*$ tel que $P = \alpha A$. (La relation de divisibilité n'est pas antisymétrique)
2. Si $A|B$ et si $B|C$, alors $A|C$. La relation de divisibilité est transitive.
3. Pour tout $A \in \mathbb{K}[X]$ non nul, $A|A$. La relation de divisibilité est réflexive.

1. $P \neq 0$, $A \neq 0$. Si $A|P$ et $P|A$, alors (16.6.2) :
$$\deg A \leq \deg P \text{ et } \deg P \leq \deg A$$
Donc :
$$\deg P = \deg A$$

Or $A|P$, alors :

$$P = A \times Q$$

Puis :

$$\deg P = \deg(AQ) = \deg A + \deg Q \text{ } (\mathbb{K} \text{ est intègre})$$

Donc :

$$\deg Q = 0$$

Donc :

$$Q = \alpha \in \mathbb{K}^*$$

2. RAS
3. RAS

16.15 Principalité de $\mathbb{K}[X]$

Théorème 16.15

Soit I un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. Il existe un unique polynôme unitaire D tel que

$$I = D\mathbb{K}[X]$$

Existence :
Soit $I \neq \{0\}$ un idéal.
On note $A = \{\deg P, P \in I \backslash \{0\}\} \subset \mathbb{N}$.
$A \neq \emptyset$ ($I \neq \{0\}$), d'après la propriété fondamentale de $\mathbb{N}$, A possède un plus petit élément noté $n \geq 0$.
Comme $n \in A$, on choisit $D \in I$ tel que $\deg D = n$.
Comme I est un idéal de $\mathbb{K}[X]$ et que $\mathbb{K} = \mathbb{K}_0[X] \subset \mathbb{K}[X]$, on a :

$$\forall \alpha \in \mathbb{K}, \alpha D \in I$$

On peut donc supposer D unitaire. Comme I est un idéal de $\mathbb{K}[X]$, on a :

$$D \times \mathbb{K}[X] \subset I$$

Soit $P \in I$. On effectue la division euclidienne de P par D ($\neq 0$) :

$$P = BD + R$$

avec $\deg R \subset \deg D$.
Or :

$$R = \underbrace{P}_{\in I} - \underbrace{BD}_{\in I}$$
$$\in I$$

Par définition de $\deg D = n$, $R = 0$.

Unicité :

$$I = D\mathbb{K}[X] = J\mathbb{K}[X]$$

avec D et J unitaires.
Or ils sont associés, donc égaux.

16.17 Existence de *pgcd*

Propostion 16.17

Si A et B sont deux polynômes non nuls, de tels PGCD existent.

Soit A, B dans $\mathbb{K}[X]$, $(A, B) \neq (0,0)$.
On note $\mathcal{C} = \{\deg P, P|A \text{ et } P|B \text{ et } P \neq 0\} \subset \mathbb{N}$.
$\mathcal{C} \neq \emptyset$ car $0 \in \mathcal{C}$ et $\mathcal{C}$ est majoré par $\deg B$ $(\max(\deg A, \deg B))$.
L'existence est assurée par la propriété fondamentale de $\mathbb{N}$.

16.18 Principalité de $\mathbb{K}[X]$

Propostion 16.18

Soit A et B deux polynômes non tous deux nuls. Soit $D \in \mathbb{K}[X]$. Alors Δ est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

D'après (16.15), on choisit $F \in \mathbb{K}[X]$ tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Soit $D \in \mathbb{K}[X]$.

$\boxed{\Rightarrow}$

On suppose que D est un PGCD.
Donc $D|A$ et $D|B$.
Donc $D|F$ (combinaison $F \in A\mathbb{K}[X] + B\mathbb{K}[X]$).
Or $F|A$ et $F|B$ $(A \in F\mathbb{K}[X],\ B \in F\mathbb{K}[X])$.
Par maximalité de $\deg D$, on a F et D associés.

$\boxed{\Leftarrow}$

$$D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X] = F\mathbb{K}[X]$$

Donc $D|A$ et $D|B$.
Pour tout diviseur commun P de A et B, $P|A$ et $P|B$.
Donc $P|D$ $(D \in A\mathbb{K}[X] + B\mathbb{K}[X])$.
Donc $\deg D$ est maximal pour la divisibilité.