6.3 Division euclidienne des polynômes

6.3.1 Théorème

Soit $\mathcal{A}$ un anneau commutatif unitaire et intègre.

Soit $B = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathcal{A}[X]$ non nul dont le coefficient dominant est inversible.

Alors, pour tout polynôme $A \in \mathcal{A}[X]$, il existe un unique couple de polynômes (Q, R) de $\mathcal{A}[X]$ tel que

$$A = BQ + R \text{ avec } \deg R < \deg B$$

Démonstration

1. Démonstration de l'existence

Nous posons :

$$A = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \cdots + \alpha_0 = \alpha_n X^n + \sum_{k=0}^{n-1} \alpha_k X^k \text{ avec } \alpha_n \neq 0$$

$$B = \beta_m X^m + \beta_{m-1} X^{m-1} + \cdots + \beta_0 = \beta_m X^m + \sum_{k=0}^{m-1} \beta_k X^k \text{ avec } \beta_m \text{ inversible}$$

Nous avons donc $\deg A = n$ et $\deg B = m$

$\Longrightarrow$ Si $\deg A < \deg B \Longleftrightarrow n < m$, alors $A = 0 \times B + A$ et, si nous posons $Q = 0$ et $A = R$, nous en avons prouvé l'existence

$\Longrightarrow$ Supposons $\deg A \geqslant \deg B \Longleftrightarrow n \geqslant m$.

Comme B n'est pas le polynôme nul, alors $\deg B \geqslant 0$ et comme nous avons $\deg A \geqslant \deg B \geqslant 0$ ceci veut dire que A n'est pas le polynôme nul.

⋆ Considérons le monôme $Q_1 = \alpha_n (\beta_m)^{-1} X^{n-m}$. Alors :

$$\begin{aligned} Q_1 B &= \alpha_n (\beta_m)^{-1} X^{n-m} \left(\beta_m X^m + \sum_{k=0}^{m-1} \beta_k X^k \right) \\ &= \alpha_n X^n + \alpha_n (\beta_m)^{-1} \sum_{k=0}^{m-1} \beta_k X^{k+n-m} \\ &= \alpha_n X^n + \alpha_n (\beta_m)^{-1} \sum_{k=n-m}^{n-1} \beta_{k+m-n} X^k \end{aligned}$$

Et donc

$$\begin{aligned} A - Q_1 B &= \alpha_n X^n + \sum_{k=0}^{n-1} \alpha_k X^k - \alpha_n X^n - \alpha_n (\beta_m)^{-1} \sum_{k=n-m}^{n-1} \beta_{k+m-n} X^k \\ &= \sum_{k=0}^{n-1} \alpha_k X^k - \alpha_n (\beta_m)^{-1} \sum_{k=n-m}^{n-1} \beta_{k+m-n} X^k \\ &= \left(\alpha_{n-1} - \alpha_n (\beta_m)^{-1} \beta_{m-1} \right) X^{n-1} + \sum_{k=0}^{n-m-1} \alpha_k X^k + \sum_{k=n-m}^{n-2} \left(\alpha_k - \alpha_n (\beta_m)^{-1} \beta_{k+m-n} \right) X^k \end{aligned}$$

⋆ En posant $R_1 = A - Q_1 B$, nous avons $\deg R_1 \leqslant n - 1 < \deg A$

Si $\deg R_1 < \deg B$, alors nous nous arrêtons et nos avons prouvé l'existence.

⋆ Si $\deg R_1 \geqslant \deg B$, nous recommençons la démarche et considérons le monôme

$$Q_2 = \left(\alpha_{n-1} - \alpha_n (\beta_m)^{-1} \beta_{m-1} \right) (\beta_m)^{-1} X^{n-1-m}$$

Nous avons alors :

$$Q_2 B = \left(\alpha_{n-1} - \alpha_n (\beta_m)^{-1} \beta_{m-1} \right) X^{n-1} + \left(\alpha_{n-1} - \alpha_n (\beta_m)^{-1} \beta_{m-1} \right) (\beta_m)^{-1} X^{n-1-m} \left(\sum_{k=0}^{m-1} \beta_k X^k \right)$$

En écrivant $R_2 = R_1 - Q_2 B$, nous avons, à nouveau, $\deg R_2 \leqslant n-2 < \deg R_1 < \deg A$

- ⋆ En itérant le processus, nous arrivons alors à une égalité de la forme $R_n = R_{n-1} - BQ_n$ avec $\deg R_n < \deg R_{n-1} < \ldots < \deg R_1 < \deg A$
  Nous avons affaire, là, à une suite décroissante d'entiers positifs.
  Il va donc exister un en tier $n_0 \in \mathbb{N}$ tel que $\deg R_{n_0} < \deg B$
  Et là, nous nous arrêtons!!

$\Longrightarrow$ A ce moment là, nous avons :

$$\begin{cases} R_1 = & A - BQ_1 \\ R_2 = & R_1 - BQ_2 \\ R_3 = & R_2 - BQ_3 \\ \vdots & \vdots \\ R_{n_0-1} = & R_{n_0-2} - BQ_{n_0-1} \\ R_{n_0} = & R_{n_0-1} - BQ_{n_0} \end{cases}$$

En additionnant, nous avons :

$$(R_1 + R_2 + \cdots + R_{n_0}) = (A + R_1 + R_2 + \cdots + R_{n_0-1}) - B(Q_1 + Q_2 + \cdots + Q_{n_0})$$
$$\Longleftrightarrow$$
$$R_{n_0} = A - B(Q_1 + Q_2 + \cdots + Q_{n_0-1} + Q_{n_0})$$

C'est à dire $A = B(Q_1 + Q_2 + \cdots + Q_{n_0-1} + Q_{n_0}) + R_{n_0}$ où $\deg R_{n_0} < \deg B$
En posant $Q = Q_1 + Q_2 + \cdots + Q_{n_0-1} + Q_{n_0}$ et $R = R_{n_0}$, nous obtenons $A = BQ + R$ avec $\deg R < \deg B$

Nous avons donc prouvé l'existence d'un couple de polynômes (Q, R) de $\mathcal{A}[X]$ tel que $A = BQ + R$ avec $\deg R < \deg B$

2. Démonstration de l'unicité de ce couple
   Comme toujours dans ces cas, nous supposons qu'il y en a 2

$$A = BQ_1 + R_1 \text{ avec } \deg R_1 < \deg B \text{ et } A = BQ_2 + R_2 \text{ avec } \deg R_2 < \deg B$$

Alors, nous avons :

$$A = BQ_1 + R_1 = BQ_2 + R_2 \Longleftrightarrow BQ_1 - BQ_2 = R_2 - R_1 \Longleftrightarrow B(Q_1 - Q_2) = R_2 - R_1$$

Donc $\deg(B(Q_1 - Q_2)) = \deg B + \deg(Q_1 - Q_2) = \deg(R_2 - R_1)$.
Si $Q_1 - Q_2 \neq 0$, alors $\deg(Q_1 - Q_2) \geqslant 0$ et $\deg(R_2 - R_1) \geqslant \deg B$.
Or, $\deg(R_2 - R_1) \leqslant \sup(\deg R_2, \deg R_1) < \deg B$. Il y a donc contradiction.
Donc, $Q_1 = Q_2$ et $R_1 = R_2$
Il y a donc unicité du couple (Q, R)

6.3.2 Corollaire

Soit $\mathcal{A}$ un anneau commutatif unitaire et intègre.
Le reste de la division d'un polynôme $P \in \mathcal{A}[X]$ par un polynôme unitaire du premier degré $g = X - c$ est égal à $\widetilde{P}(c)$

Démonstration

D'après l'algorithme de division vu dans le théorème 6.3.1, nous avons $P = Q(X - c) + R$ avec $\deg R < \deg(X - c)$, c'est à dire que $\deg R = 0$.
R est donc une constante, élément de $\mathcal{A}$.
Nous avons $\widetilde{P}(c) = \widetilde{Q}(c)(c - c) + R = R$. Donc, $R = \widetilde{P}(c)$.
Ce que nous voulions.

Remarque 9 :

Très souvent, maintenant, nous oublierons le tilde et écrirons $\widetilde{P}(c) = P(c)$ pour $c \in \mathcal{A}$

6.3.3 Corollaire : division euclidienne dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps

Si $\mathbb{K}$ est un corps commutatif et A et B deux polynômes de $\mathbb{K}[X]$ avec B non nul
Alors, il existe un unique couple de polynômes (Q, R) de $\mathbb{K}[X]$ tel que

$$A = BQ + R \text{ avec } \deg R < \deg B$$

Démonstration

$\mathbb{K}$ étant un anneau particulier, le théorème 6.3.1 doit pouvoir s'appliquer. Il s'applique d'autant mieux que tout élément non nul d'un corps $\mathbb{K}$ est inversible.

Ainsi, si $\deg B = n$, alors $B = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$ et donc inversible. Le théorème 6.3.1s'applique donc.

Exercice 3 :

Effectuer, dans $\mathbb{C}[X]$, la division euclidienne des polynômes $f \in \mathbb{C}[X]$ et $g \in \mathbb{C}[X]$ où :

1. $f = 7X^4 - X^3 + 2X - 4$ et $g = 2X^2 - 3X - 5$
2. $f = X^8 - 1$ et $g = X^3 - 1$
3. $f = 2X^5 - 5X^3 - 8X$ et $g = X + 3$
4. $f = 4X^3 + X^2$ et $g = X + (1 + i)$

Exercice 4 :

Est-il possible d'effectuer la division euclidienne de f par g, avec :

$$f = 6X^3 + X^2 + 7X \qquad g = 3X^2 + 2X - 1$$

dans $\mathbb{Z}[X]$?

Exercice 5 :

Soient $\mathbb{K}$ un corps et $a \in \mathbb{K}$ et $b \in \mathbb{K}$ tels que $a \neq b$. Soit aussi $P \in \mathbb{K}[X]$.
Exprimer le reste de la division de P par le polynôme $(X - a)(X - b)$ en fonction de $P(a)$ et $P(b)$