Note sur la division polynomiale

Alexis Michelat*

4 mars 2025

Proposition 1. *Soit $\mathbb{K}$ un corps et $P, Q \in \mathbb{K}[X]$ deux polynômes non-nuls sur $\mathbb{K}$. Alors il existe un unique couple de polynômes $(R, S) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tels que $P = QR + S$, où $\deg(S) < \deg(P)$.*

Démonstration. Soit $d = \deg(P) \geq 0$ et $m = \deg(Q) \geq 0$ les degrés de P et Q. Si $Q = b_0 \in \mathbb{K}[X]$ est un polynôme constant, comme $Q \neq 0$ par hypothèse, il suffit de prendre $R = b_0^{-1} P$ et $S = 0$ pour obtenir la conclusion souhaitée. De plus, si $\deg(Q) > \deg(P)$, on choisit $R = 0$ et $S = P$. On note que c'est le seul choix possible car s'il existait $R \in \mathbb{K}[X] \neq \{0\}$ et $S \in \mathbb{K}[X]$ tel que $\deg(S) < \deg(P)$ et $P = QR + S$, alors on aurait $\deg(P) = \deg(Q) + \deg(R) \geq \deg(R) > \deg(P)$. On peut donc supposer que $\deg(P) \geq \deg(Q) \geq 1$. Soit $a_i, b_j \in \mathbb{K}$ tels que

$$P = \sum_{i=0}^{d} a_i X^i \qquad \text{et} \qquad Q = \sum_{j=0}^{m} b_j X^j.$$

Par hypothèse, on a $a_d \neq 0$ et $b_m \neq 0$. On prouve le théorème par récurrence sur le degré $d \geq m$ de P. L'initialisation est déjà établie pour $0 \leq d \leq m - 1$, et on peut donc supposer le théorème prouvé pour tous les polynômes de degré au plus $d - 1$. On a

$$\begin{aligned} P - a_d b_m^{-1} X^{d-m} Q &= \sum_{i=0}^{d} a_i X^i - a_d X^d - \sum_{j=0}^{m-1} a_d b_m^{-1} b_j X^{m+j} = \sum_{i=0}^{d-1} a_i X_i - \sum_{k=m}^{d-1} a_d b_m^{-1} b_{k-m} X^k \\ &= \sum_{i=0}^{m-1} a_i X_i + \sum_{i=m}^{d-1} \left(a_i - a_d b_m^{-1} b_{k-m}\right) X^i. \end{aligned}$$

On voit que le polynôme $P - a_d b_m^{-1} X^{d-m} Q$ est de degré au plus $d - 1$, et on peut donc appliquer la récurrence pour trouver $R', S' \in \mathbb{K}[X]$ tels que $\deg(S') \leq \deg(P - a_d b_m^{-1} X^{d-m} Q) \leq d - 1$ et

$$P - a_d b_m^{-1} X^{d-m} Q = QR' + S',$$

ce qu'on réécrit en

$$P = Q(R' + a_d b_m^{-1} X^{d-m}) + S'.$$

On choisit donc $R = R' + a_d b_m^{-1} X^{d-m}$ et $S = S'$. Comme $\deg(R') < d - m - 1$, on en déduit que R est uniquement déterminé. De même, S est déterminé de manière unique, ce qui conclut la preuve de la proposition. □

On voit donc qu'on dispose d'un algorithme pour calculer la division euclidienne des polynômes. Par exemple, si $P = 2X^6 + 3X^2 + 1$ et $Q = X^2 + 1$, on calcule

$$P - 2X^4 Q = 2X^6 + 3X^2 + 1 - (2X^6 + 2X^4) = -2X^4 + 3X^2 + 1 = P'.$$

De même, on a

$$P' + 2X^2 Q = -2X^4 + 3X^2 + 1 + 2X^4 + 2X^2 = 5X^2 + 1 = P''.$$

*EPFL B, Station 8, CH-1015 Lausanne, Switzerland alexis.michelat@epfl.ch

Finalement, on a

$$P'' - 5Q = 5X^2 + 1 - (5X^2 + 5) = -4,$$

ce qui donne

$$P = (2X^4 - 2X^2 + 5)Q - 4.$$

On a donc $R = 2X^4 - 2X^2 + 5$ et $S = -4$. On vérifie sans peine le résultat [*] :

$$\begin{aligned}(2X^4 - 2X^2 + 5)Q &= (2X^4 - 2X^2 + 5)(X^2 + 1) \\ &= 2X^6 + 2X^4 - 2X^4 - 2X^2 + 5X^2 + 5 \\ &= 2X^6 + 3X^2 + 5 \\ &= P + 4.\end{aligned}$$

∗. Le jour de l'examen, il peut être utile de vérifier le résultat de cette manière.