Exemple de calcul de coefficients de BÉZOUT.

$$A = X^2+X+1 \qquad B = X^2-1$$

On divise A par B $\qquad X^2+X+1 = 1.(X^2-1) + \underbrace{X+2}_{R_1}$

On divise B par R_1

$$\begin{array}{r|l} X^2 \qquad -1 & X+2 \\ -(X^2+2X) \quad & X-2 \\ -2X-1 & \\ -(-2X-4) & \\ 3 & \end{array}$$

donc $\quad X^2-1 = (X+2)(X-2) + 3$

R_2 dernier reste non nul

on a
$$\begin{aligned} 3 &= X^2-1 - (X+2)(X-2) \\ &= B(X) - R_1(X)\,(X-2) \qquad\qquad R_1(X) = A(X) - B(X) \\ &= B(X) - (A(X)-B(X))\,(X-2) \\ &= (-X+2)A(X) + (X-1)B(X) \end{aligned}$$

donc $\quad 1 = \underbrace{\frac{-X+2}{3}}_{U(X)} A(X) + \underbrace{\frac{X-1}{3}}_{V(X)} B(X)$

coefficients de BÉZOUT

PPCM

Soient A, B deux polynômes non nuls.

L'ensemble des polynômes unitaires multiples de A et de B admet un unique élément de plus petit degré.
On le note PPCM(A, B)

Exemple $A(X) = 2X(X+1)$
$B(X) = \frac{1}{3}(X+1)^2(X^2+2)$ ← factorisés en produit d'irréductibles dans $\mathbb{R}[X]$.

$PGCD(A, B) = X+1$

$PPCM(A, B) = X(X+1)^2(X^2+2)$

(on ignore les facteurs 2 et $\frac{1}{3}$ car le PGCD et le PPCM sont irréductibles par définition)

Proposition Soient $A, B \in \mathbb{K}[X]$, non nuls.
Alors $\exists \lambda \in \mathbb{K}^*$ tel que $PGCD(A,B) \cdot PPCM(A,B) = \lambda AB$

(permet de calculer le PPCM sans factoriser A et B, en passant par le PGCD obtenu par l'algorithme d'Euclide).

Racines multiples d'un polynôme

Rappel : si $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$
alors α est racine de $P \iff P(\alpha) = 0 \iff X - \alpha$ divise P.

Définition Soit $P \in \mathbb{K}[X]$ et ~~...~~ $\alpha \in \mathbb{K}$ une racine de P.
Pour $n \in \mathbb{N}^*$, on dit que α est racine d'ordre $\geq n$ de P si $(X-\alpha)^n$ divise P

on dit que α est racine d'ordre n de P si $(X-\alpha)^n$ divise P
et $(X-\alpha)^{n+1}$ ne divise pas P

La multiplicité de α (ou l'ordre de α) est le plus grand $n \geq 1$ tel que $(X-\alpha)^n$ divise P

Racine d'ordre 2 = racine double

Racine d'ordre ≥ 2 = racine multiple

Racine d'ordre 1 = racine simple

Théorème Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$, $n \in \mathbb{N}^*$

Alors $(X-\alpha)^n$ divise $P \iff P(\alpha) = P'(\alpha) = \dots = P^{(n-1)}(\alpha) = 0$

dérivée $(n-1)^{\text{ème}}$

Ainsi α racine simple de $P \iff P(\alpha) = 0,\ P'(\alpha) \neq 0$

α racine double de $P \iff P(\alpha) = P'(\alpha) = 0,\ P''(\alpha) \neq 0$

Exemple : $P(X) = X^3 - 2X^2 + X$

1 est racine "évidente" de P. Quel est son ordre ?

$P(1) = 0$
$P'(X) = 3X^2 - 4X + 1$ et $P'(1) = 0$
$P''(X) = 6X - 4$ et $P''(1) = 2 \neq 0$

donc 1 est racine double de P

La preuve du théorème utilise la formule de LEIBNIZ pour les dérivées d'un produit

$$(fg)' = f'g + fg'$$
$$(fg)'' = f''g + 2f'g' + fg''$$

Plus généralement $\forall n \in \mathbb{N}^*$

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)} g^{(n-k)}$$

(se démontre par récurrence sur n)

Preuve du théorème $\Rightarrow$ Si $(X-\alpha)^n$ divise P, on peut écrire

$P = QR$ avec $Q(X) = (X-\alpha)^n$

$Q'(X) = n(X-\alpha)^{n-1}$

$Q''(X) = n(n-1)(X-\alpha)^{n-2}$ ..

$$\varphi^{(m)}(X) = m!$$

et on a donc $\varphi(\alpha) = \varphi'(\alpha) = \dots = \varphi^{(m-1)}(\alpha) = 0$.

par la formule de LEIBNIZ, si $m \leq n-1$

$$P^{(m)}(\alpha) = \sum_{k=0}^{m} \binom{m}{k} \underbrace{\varphi^{(k)}(\alpha)}_{=0} R^{(m-k)}(\alpha)$$

donc $P^{(m)}(\alpha) = 0$

$\Leftarrow$ se démontre en utilisant la division euclidienne ∎

RELATIONS COEFFICIENTS-RACINES

Un trinôme unitaire est de la forme $X^2 - sX + p = A(X)$ pour $p, s \in \mathbb{C}$

Si $A(X) = (X - z_1)(X - z_2)$ est la factorisation irréductible dans $\mathbb{C}[X]$,

alors $\begin{cases} s = z_1 + z_2 \\ p = z_1 z_2 \end{cases}$

En degré 3 : $(X - z_1)(X - z_2)(X - z_3) = X^3 - \underbrace{(z_1 + z_2 + z_3)}_{\text{somme}} X^2 + (z_1 z_2 + z_1 z_3 + z_2 z_3) X - \underbrace{z_1 z_2 z_3}_{\text{produit}}$

Plus généralement

Si $P \in \mathbb{C}[X]$ est un polynôme unitaire de degré n de la forme $P(X) = X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ de racines (comptées avec multiplicité) $z_1, \dots, z_n \in \mathbb{C}$

alors $a_{n-k} = (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} z_{i_1} z_{i_2} \dots z_{i_k}$

En particulier $a_{n-1} = -(z_1 + \dots + z_n)$ $(k=1)$

$a_0 = (-1)^n z_1 \dots z_n$