Exemple d'application : systèmes de congruences

Théorème Soient $a, b \in \mathbb{Z}^*$ deux entiers premiers entre eux.
Soient $y, z \in \mathbb{Z}$.

Alors le système d'inconnue $x \in \mathbb{Z}$

$$\begin{cases} x \equiv y \ [a] \\ x \equiv z \ [b] \end{cases}$$

admet une unique solution $x_0 \in \{0, 1, \dots, ab-1\}$.

L'ensemble des solutions dans $\mathbb{Z}$ est $\{x_0 + kab, \ k \in \mathbb{Z}\}$

Plutôt que de retenir l'énoncé du théorème, il est important de savoir l'appliquer sur des exemples.

Exemple Déterminer les entiers $x \in \mathbb{Z}$ vérifiant

$$\begin{cases} x \equiv 3 \ [4] \\ x \equiv 5 \ [9] \end{cases}$$

3 Etapes

① On écrit une relation de BÉZOUT pour les entiers $a=4$ $b=9$, c'est-à-dire $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$

Ici on peut directement donner $9 - 2 \times 4 = 1$ $a=-2$ $b=1$

On écrit ensuite $x = (au)x + (bv)x$. Ici $x = 9x - 2 \times 4x$

② Si x vérifie le système, on calcule $ax \ [ab]$
$bx \ [ab]$

$x \equiv 3 \ [4] \Rightarrow \exists k_1 \in \mathbb{Z}$ t.q. $x = 4k_1 + 3 \Rightarrow 9x = 36k_1 + 27$ donc $9x \equiv 27 \ [36]$

on peut directement multiplier par 9 à condition de multiplier aussi le module

$x \equiv 5 \ [9] \Rightarrow$ ... $\Rightarrow 4x \equiv 20 \ [36]$

③ On a $x = 9x - 2 \times 4x$

donc $x \equiv 27 - 2 \times 40 \ [36]$

$\equiv -13 \ [36]$

$\equiv 23 \ [36]$

Ainsi $x = 23$ est une solution du système

et l'ensemble des solutions dans $\mathbb{Z}$ est $\{23 + 36k,\ k \in \mathbb{Z}\}$

Chapitre 8 — POLYNÔMES

Définition Si $a_0 \dots a_n$ sont des nombres réels ou complexes,

$$P(X) = a_0 + a_1 X + \dots + a_n X^n$$

est un polynôme d'indéterminée X.

On note $\begin{cases} \mathbb{R}[X] \\ \mathbb{C}[X] \end{cases}$ l'ensemble des polynômes à coefficients $\begin{cases} \text{réels} \\ \text{complexes} \end{cases}$

Si on remplace X par x, on obtient une fonction

$$\mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto P(x) \quad \text{ou} \quad \mathbb{C} \longrightarrow \mathbb{C},\ x \longmapsto P(x)$$

Soit $P(X) = a_0 + a_1 X + \dots + a_n X^n$

le <u>degré</u> de P (noté $\deg(P)$ ou $d^\circ(P)$) est le plus grand entier d tel que $a_d \neq 0$.

Ex $P(X) = X^3 + 1$ $\quad d^\circ(P) = 3$

$Q(X) = X - 2$ $\quad d^\circ(Q) = 1$

$R(X) = 3$ $\quad d^\circ(R) = 0$

Par convention, le degré du polynôme nul est $-\infty$

Le <u>coefficient dominant</u> d'un polynôme de degré d est a_d.

Opération sur les polynômes : on peut

- les ajouter $(P+Q)$
- les multiplier $(P \cdot Q)$
- les dériver (P')
- les composer $(P \circ Q)$

Si $P(X) = a_0 + a_1 X + \dots + a_d X^d$

$P \circ Q(X) = a_0 + a_1 Q(X) + \dots + a_d Q(X)^d$

Propriétés du degré

Soient P et Q deux polynômes non constants

- $d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$
- $d^\circ(P+Q) \leq \max(d^\circ(P), d^\circ(Q))$ ⟸ Exemple $P(X) = X^2 + X$, $Q(X) = -X^2 - 1$, $(P+Q)(X) = X - 1$, $d^\circ(P+Q) < \max(d^\circ(P), d^\circ(Q))$
- $d^\circ(P') = d^\circ(P) - 1$
- $d^\circ(P \circ Q) = d^\circ(P) \cdot d^\circ(Q)$

DIVISION EUCLIDIENNE DES POLYNÔMES

Théorème Soient A, B deux polynômes (réel ou complexes) avec $B \neq 0$.

Il existe un unique couple (Q, R) de polynômes tels que

- $A = BQ + R$
- $d^\circ(R) < d^\circ(B)$ [inclut le cas $R = 0$]

Principe : on calcule les coefficients de Q en commençant par ceux de plus haut degré

Premier exemple $A = X^3 + X^2 - 1$ $\quad B = X - 1$

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

On a donc $X^3 + X^2 - 1 = (X-1)\underbrace{(X^2+2X+2)}_{Q(X)} + \underbrace{1}_{R(X)}$

Deuxième exemple $A = 6X^3 - 10X^2 + X + 3$ $\quad B = X^2 - X + 1$

$$\begin{array}{r|l} 6X^3 - 10X^2 + X + 3 & X^2 - X + 1 \\ -(6X^3 - 6X^2 + 6X) & 6X - 4 \\ \hline -4X^2 - 5X + 3 & \\ -[-4X^2 + 4X - 4] & \\ \hline -9X + 7 & \end{array}$$

On a donc $A(X) = B(X) \cdot \underbrace{(6X-4)}_{Q(X)} + \underbrace{(-9X+7)}_{R(X)}$

Définition Soient A, B deux polynômes, $B \neq 0$.

On dit que B divise A s'il existe un polynôme Q tel que $A = B \cdot Q$

(autrement dit, si le reste de la division euclidienne de A par B est nul).

Lien entre divisibilité et racines

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ $\quad P \in \mathbb{K}[X]$ et $z \in \mathbb{K}$.

Alors $\quad P(z) = 0 \iff X - z$ divise P

Preuve

$\Leftarrow$ Si $P(X) = (X-z)Q(X)$ alors $P(z) = (z-z)Q(z) = 0$

$\Rightarrow$ On écrit la division euclidienne de P par $X-z$

$P(X) = Q(X)(X-z) + \underbrace{R(X)}_{d^\circ(R) < 1}$ donc R est constant

$P(z) = Q(z)(z-z) + R(z)$ donc $R(z) = 0$ et

donc $R = 0$, donc

$(X-z)$ divise P