Corollaire Soit P un polynôme non nul de degré d.
Alors P a au plus d racines

Corollaire Un polynôme ayant une infinité de racines est le polynôme nul.

Polynômes irréductibles

C'est l'analogue pour les polynômes du concept de nombre premier pour les entiers.

⚠ C'est très différent selon qu'on est sur $\mathbb{R}$ ou sur $\mathbb{C}$.

Définition Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

On dit que $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ s'il n'est pas constant et s'il ne peut pas s'écrire comme $P = Q \cdot R$ avec $d^\circ(Q) < d^\circ(P)$, $d^\circ(R) < d^\circ(P)$

(Bien sûr, on peut toujours écrire $P = \frac{1}{\alpha}(\alpha P)$ pour tout $\alpha \in \mathbb{K}^*$)

Exemples :

- tout polynôme de degré 1 est irréductible
- $P(X) = X^2 + 1$
  - n'est pas irréductible dans $\mathbb{C}[X]$ car il s'écrit $P(X) = (X-i)(X+i)$
  - est irréductible dans $\mathbb{R}[X]$: si on avait $P(X) = Q(X)R(X)$ avec $d^\circ(Q) < 2$, $d^\circ(R) < 2$
    on aurait $d^\circ(Q) = d^\circ(R) = 1$
    donc Q, R seraient de la forme $Q(X) = X + a$, $R(X) = X + b$ $a, b \in \mathbb{R}$
    et $-a$ et $-b$ seraient des racines réelles de P — absurde

Théorème

① Un polynôme $P \in \mathbb{C}[X]$ est irréductible dans $\mathbb{C}[X]$ si et seulement si il est de degré 1.

② Un polynôme $P \in \mathbb{R}[X]$ est irréductible dans $\mathbb{R}[X]$ si et seulement si
- il est de degré 1
- (ou) il est de degré 2 à discriminant $\Delta < 0$

Exemple Le polynôme $P(X) = X^4 + 1$ n'est pas irréductible dans $\mathbb{R}[X]$ donc peut s'écrire $P(X) = A(X)B(X)$ avec $d^\circ(A) < 4$, $d^\circ(B) < 4$

Comment trouver A et B ?

Une méthode est de trouver les racines de X^4+1 dans $\mathbb{C}$. Elles sont 2 à 2 conjuguées, et on peut regrouper les racines conjuguées pour obtenir un polynôme de degré 2.

Mise en œuvre :

Soit $z \in \mathbb{C}$ $\quad P(z) = 0 \iff z^4 + 1 = 0 \iff z^4 = -1$

On cherche z sous la forme $z = re^{i\theta}$ $\quad r \geq 0$ $\quad \theta \in \mathbb{R}$

On a $r = 1$ et $e^{4i\theta} = -1 = e^{i\pi}$

donc $4\theta \equiv \pi \ [2\pi]$

$\theta \equiv \frac{\pi}{4} \ [\frac{\pi}{2}]$

Les racines sont donc $e^{i\frac{\pi}{4}}$, $e^{-i\frac{\pi}{4}}$, $e^{3i\pi/4}$, $e^{-\frac{3i\pi}{4}}$.

On a $X^4 + 1 = \underbrace{(X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})}_{X^2 - (e^{i\frac{\pi}{4}} + e^{-i\frac{\pi}{4}})X + 1} \underbrace{(X - e^{3i\pi/4})(X - e^{-3i\pi/4})}_{X^2 - (e^{\frac{3i\pi}{4}} + e^{-\frac{3i\pi}{4}})X + 1}$

$\boxed{e^{i\theta} + e^{-i\theta} = 2\cos\theta}$

$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$

$(X - e^{i\theta})(X - e^{-i\theta})$

$= X^2 - 2\cos(\theta)X + 1$

irréductibles dans $\mathbb{R}[X]$

Théorème $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

Tout polynôme non nul $P \in \mathbb{K}[X]$ peut s'écrire sous la forme

$P = \lambda P_1^{m_1} \dots P_k^{m_k}$ où

- les polynômes P_i sont irréductibles, unitaires (i.e. de coefficient dominant $= 1$) et distincts
- $\lambda \in \mathbb{K}$
- $m_1 \dots m_k \in \mathbb{N}^*$

De plus, cette écriture est unique (à l'ordre des P_i près)

Sur $\mathbb{C}$ le théorème devient

$$P(X) = \lambda (X - a_1)^{m_1} \dots (X - a_k)^{m_k}$$

$\lambda \in \mathbb{C}$, $a_1 \dots a_k \in \mathbb{C}$, $m_1 \dots m_k \in \mathbb{N}^*$

Sur $\mathbb{R}$ le théorème devient

$$P(X) = \lambda (X - a_1)^{m_1} \dots (X - a_k)^{m_k} (X^2 + b_1 X + c_1)^{m_1} \dots (X^2 + b_\ell X + c_\ell)^{m_\ell}$$

avec $\lambda \in \mathbb{R}$, $a_1 \dots a_k \in \mathbb{R}$, $m_1 \dots m_k \in \mathbb{N}^*$

$b_1 \dots b_\ell \in \mathbb{R}$, $c_1 \dots c_\ell \in \mathbb{R}$ vérifiant $b_i^2 - 4c_i < 0$, $m_1 \dots m_\ell \in \mathbb{N}^*$

Pour déterminer la factorisation en polynômes irréductibles dans $\mathbb{R}[X]$, on peut factoriser dans $\mathbb{C}[X]$ et regrouper les racines conjuguées.

Exemple Factoriser $P(X) = X^6 - 1$ en produit de polynômes irréductibles dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

dans $\mathbb{C}$: le polynôme P a pour racines les racines 6èmes de l'unité.

$e^{2ik\pi/6}$, $k = 0, 1, \dots, 5$

c'est à dire 1, $e^{i\pi/3}$, $e^{2i\pi/3}$, -1, $e^{-i\pi/3}$, $e^{-2i\pi/3}$

donc $P(X) = (X-1)(X - e^{i\pi/3})(X - e^{2i\pi/3})(X+1)(X - e^{-i\pi/3})(X - e^{-2i\pi/3})$

c'est la factorisation dans $\mathbb{C}[X]$

dans $\mathbb{R}$: on regroupe les racines complexe conjuguées

$(X-e^{i\pi/3})(X-e^{-i\pi/3}) = X^2 - 2\cos(\frac{\pi}{3})X + 1 = X^2 - X + 1$

$(X-e^{2i\pi/3})(X-e^{-2i\pi/3}) = X^2 - 2\cos(\frac{2\pi}{3})X + 1 = X^2 + X + 1$

d'où l'écriture

$P(X) = (X-1)(X+1)(X^2-X+1)(X^2+X+1)$

irréductibles dans $\mathbb{R}(X)$

Arithmétique des polynômes

PGCD

Soient A, B deux polynômes non nuls

L'ensemble des diviseurs unitaires communs à A et B a un unique élément de degré maximal appelé $PGCD(A,B)$

- Le PGCD est donc unitaire
- Comment calculer le PGCD ? Comme pour les entiers, 2 méthodes

① On connaît la factorisation de A et B en produit d'irréductibles.
→ le PGCD s'obtient en gardant les facteurs communs.

② Sinon, on peut toujours calculer le PGCD par l'algorithme d'Euclide

Exemple $A(X) = X^4 + 3X^3 + X^2 + 2X - 12$

$B(X) = X^3 + 2X - 3$

$PGCD(A,B)$??

On effectue l'algorithme d'Euclide

- Division euclidienne de A par B

$$\begin{array}{r|l} X^4+3X^3+X^2+2X-12 & X^3+2X-3 \\ -(X^4+2X^2-3X) & \hline \\ 3X^3-X^2+5X-12 & X+3 \\ -(3X^3+6X-9) & \\ \hline -X^2-X-3 & \end{array}$$

$R(X) = -X^2 - X - 3$ est le reste de la division euclidienne de A par B

- Division euclidienne de B par R

$$\begin{array}{r|l} X^3 + 2X - 3 & -X^2 - X - 3 \\ -(X^3 + X^2 + 3X) & \hline -X + 1 \\ \hline -X^2 - X - 3 & \\ -(-X^2 - X - 3) & \\ \hline 0 & \end{array}$$

Le dernier reste non nul est $-X^2 - X - 3$

Le PGCD (défini comme unitaire) est donc $PGCD(A,B) = X^2 + X + 3$

Si on avait connu la factorisation en irréductibles

$$A(X) = (X^2 + X + 3)(X + 1 - \sqrt{5})(X + 1 + \sqrt{5})$$
$$B(X) = (X^2 + X + 3)(X - 1)$$

la réponse aurait été immédiate

On dit que deux polynômes A et B sont premiers entre eux si $PGCD(A,B) = 1$.

Théorème de BEZOUT

Soit A, B deux polynômes non nuls. Alors

A, B premiers entre eux $\iff$ il existe des polynômes U, V tels que $AU + BV = 1$

Théorème de GAUSS

Soient A, B, C trois polynômes non nuls.

Si A et B sont premiers entre eux } alors A divise C
A divise BC

Corollaire Si un polynôme P irréductible divise AB,
alors P divise A ou P divise B