Rappel P est irréductible si il ne peut pas s'écrire $P = QR$ avec $d^\circ Q < d^\circ P$, $d^\circ R < d^\circ P$.

Sur $\mathbb{C}$: P irréductible $\Leftrightarrow$ $d^\circ P = 1$

Sur $\mathbb{R}$, P irréductible $\Leftrightarrow$ $\begin{cases} d^\circ P = 1 \\ \text{ou} \\ d^\circ P = 2 \text{ avec } \Delta < 0 \end{cases}$

Théorème Tout polynôme $P \in \mathbb{K}[X]$ peut s'écrire sous la forme $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

$$P = \lambda P_1^{n_1} \cdots P_k^{n_k}$$

où – les polynômes P_i sont irréductibles et unitaires (le coeff. de + haut degré $= 1$)

– $\lambda \in \mathbb{K}$

– $n_1 \dots n_k \in \mathbb{N}$

Et cette écriture est unique (à l'ordre des P_i près).

- sur $\mathbb{C}$ le théorème devient

$$P(X) = \lambda (X - a_1)^{n_1} \cdots (X - a_k)^{n_k}$$

avec $\lambda \in \mathbb{C}$ $a_1 \dots a_k \in \mathbb{C}$, $n_1 \dots n_k \in \mathbb{N}$

Tout polynôme complexe se factorise en produit de polynômes de degré 1.

- sur $\mathbb{R}$ le théorème devient

$$P(X) = \lambda (X - a_1)^{n_1} \cdots (X - a_j)^{n_j} (X^2 + b_1 X + c_1)^{m_1} \cdots (X^2 + b_k X + c_k)^{m_k}$$

avec $\lambda \in \mathbb{R}$ $a_1 \dots a_j \in \mathbb{R}$ $b_1 \dots b_k \in \mathbb{R}$ $c_1 \dots c_k \in \mathbb{R}$ et $b_i^2 - 4c_i < 0$

$n_1 \dots n_j$ $m_1 \dots m_k \in \mathbb{N}$

Une méthode possible pour obtenir la factorisation dans $\mathbb{R}[X]$ est de factoriser dans $\mathbb{C}[X]$ puis de regrouper les racines conjuguées.

$$\left[(X - re^{i\theta})(X - re^{-i\theta}) = X^2 - X(re^{i\theta} + re^{-i\theta}) + r^2 = X^2 - 2r\cos\theta\, X + r^2 \right]$$

Exemple Soit $P(X) = X^6 - 1$.

Factoriser P comme produit de polynômes irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

- dans $\mathbb{C}$ le polynôme a pour racines les racines 6èmes de l'unité $e^{i\frac{2k\pi}{6}}$ $k = 0, 1, 2, 3, 4, 5$

$$1 \quad e^{i\frac{\pi}{3}} \quad e^{i\frac{2\pi}{3}} \quad -1 \quad e^{i\frac{4\pi}{3}} \quad e^{i\frac{5\pi}{3}}$$

et donc P s'écrit

1 e e

et donc P s'écrit

$$P(X) = (X-1)(X-e^{i\pi/3})(X-e^{2i\pi/3})(X+1)(X-e^{4i\pi/3})(X-e^{5i\pi/3})$$

- dans $\mathbb{R}$ on regroupe les racines conjuguées
$e^{4i\pi/3} = e^{-2i\pi/3}$ $\quad e^{5i\pi/3} = e^{-i\pi/3}$

$$(X-e^{i\pi/3})(X-\underbrace{e^{5i\pi/3}}_{=e^{-i\pi/3}}) = X^2 - 2\cos(\tfrac{\pi}{3})X + 1 = X^2 - X + 1$$

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

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** Si A, B sont 2 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 $\rightarrow$ le PGCD s'obtient en gardant les facteurs communs.

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

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

- Division euclidienne de A par B

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

$$\begin{array}{l} -(3X^3 \qquad +6X-9) \\ \hline \qquad -X^2-X-3 \end{array}$$

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

- Division euclidienne de B par R

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

on obtient 0

- le PGCD est le dernier reste non nul, soit $-X^2-X-3$.

On a défini le PGCD comme étant unitaire,

donc $\mathrm{PGCD}(A,B) = X^2+X+3$.

Si on avait connu la factorisation de A et B, la réponse aurait été plus rapide.

$$A(X) = (X^2+X+3)(X^2+2X-4)$$
$$= (X^2+X+3)(X+1-\sqrt{5})(X+1+\sqrt{5})$$
$$B(X) = (X^2+X+3)(X-1)$$

et donc $\mathrm{PGCD}(A,B) = X^2+X+3$ (seul facteur commun).

On dit que A et B sont premiers entre eux si $\mathrm{PGCD}(A,B)=1$.

Théorème de BEZOUT

Soient A et B deux polynômes non nuls.

Alors A et B sont premiers entre eux si et seulement si $\exists\, U, V$ polynômes tels que $AU+BV=1$

Alors A et B sont p...
si $\exists\, U, V$ polynômes tels que $AU + BV = 1$

Comme pour les entiers, on peut trouver U et V en remontant l'algorithme d'EUCLIDE.

Théorème de GAUSS

Soient A, B, C 3 polynômes non nuls. Si A et B sont premiers entre eux et si $A \mid BC$, alors $A \mid C$.

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

Exemple de calcul de coefficients de BÉZOUT.

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

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

On divise B par R_1

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

$$X^2 - 1 = (X+2)(X-2) + \underbrace{3}_{R_2}$$

$$3 = (X^2 - 1) - (X+2)(X-2)$$

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

$$3 = (X^2 - 1) - \left[(X^2 + X + 1) - (X^2 - 1)\right](X-2)$$

$$= -(X-2)\underbrace{(X^2 + X + 1)}_{A(X)} + (X^2 - 1) + (X^2 - 1)(X-2)$$

$$= -(X-2)\,A(X) + (X-1)\,B(X)$$

On a donc $\qquad 1 = -\dfrac{(X-2)}{3} A(X) + \dfrac{X-1}{3} B(X)$

coefficients de BÉZOUT.

coèfficients de BEZOU..