Chapitre 3 : Polynômes

Reda Chhaibi

Bureau 212 – Bâtiment 1R2
reda.chhaibi@math.univ-toulouse.fr

Jeudi 26 Novembre 2020

CM18 : Polynômes irréductibles

($\mathbb{K}[X]$)

Divisibilité
+ Div eucl

$\mathbb{Z}$

Analogue des nombres premiers (sur $\mathbb{N}$)

Divisibilité
+ Division eucl

But : quel est la décomposition en produit d'irréductibles de X^4+X^2+1 ?

Plan :

- les polynômes irréductibles,
- factoriser dans $\mathbb{C}[X]$,
- factoriser dans $\mathbb{R}[X]$.

Important.

Rappel

Théorème 4

Si $r_1, \ldots, r_k$ sont des racines (distinctes) de P de multiplicités respectives $m_1, \ldots, m_k$, alors

$$P(X) = (X - r_1)^{m_1}(X - r_2)^{m_2} \cdots (X - r_k)^{m_k} Q(X).$$

Une fois toutes les racines « extraites » :

- Q peut-il être non-constant ?
- si oui, peut-on encore le décomposer comme un produit de polynômes ?

1. Polynôme irréductible

Exemple :

si $a \in \mathbb{R}$

$(X-a)$ irréd. dans $\mathbb{R}$ & $\mathbb{C}$.

Definition

Un polynôme est dit ***irréductible dans $\mathbb{K}[X]$*** si

- il est non-constant
- et il ne peut pas s'écrire comme un produit de deux polynômes de $\mathbb{K}[X]$ **tous les deux non-constants**.

/!\ Analogue à nb premier sur $\mathbb{N}$.

$p \in \mathbb{N}$ premier si

- $p \neq 1$
- on ne peut écrire $p = ab$ où $(a,b) \in \mathbb{N} \times \mathbb{N}$, $a, b \geqslant 1$

Question 1

Est-ce le polynôme $X^2 + X + 1$ est un polynôme irréductible ?

1. ~~Oui car il est non constant~~
2. Oui car il n'a pas de racine dans $\mathbb{R}$
3. Non car il est constant
4. Non car il a des racines
5. On ne peut pas savoir

$\Delta = b^2 - 4ac = -3$

racines conjuguées dans $\mathbb{C}$:

$-\frac{1}{2} \pm i\frac{\sqrt{3}}{2} = e^{\pm i\frac{2\pi}{3}}$

$(X^2+X+1) = (X-j)(X-\bar{j})$

Quand on parle d'irréductibilité, il faut toujours préciser dans quel $\mathbb{K}[X]$ on se place !

Le polynôme $P(X) = X^2 + 1$ peut-être vu au choix comme un polynôme de $\mathbb{R}[X]$ ou de $\mathbb{C}[X]$.

- Dans $\mathbb{C}[X]$, le polynôme P **n'est pas irréductible** car

$$P(X) = \underbrace{(X-i)}_{\in\mathbb{C}[X]}\underbrace{(X+i)}_{\in\mathbb{C}[X]}.$$

- Dans $\mathbb{R}[X]$, le polynôme P est **irréductible**.

But pour la suite de ce cours :
décomposer un polynôme en produit de polynômes irréductibles.

Quels sont les polynômes irréductibles sur $\mathbb{C}$ et sur $\mathbb{R}$?

2. Décomposition dans $\mathbb{C}[X]$

Théorème 5. de D'Alembert. Admis

Sur $\mathbb{C}$, tout polynôme de degré supérieur ou égal à 1 admet au moins une racine.

On revient sur le théorème précédent : si P a pour seules racines $r_1, \ldots, r_k$ $\in \mathbb{C}$ d'ordres respectifs $m_1, \ldots, m_k$, alors

$$P(X) = (X - r_1)^{m_1} (X - r_2)^{m_2} \cdots (X - r_k)^{m_k} Q(X)$$

$\Longrightarrow$ Le polynôme Q n'a pas de racine (sinon ce serait aussi une racine de P), donc il est de degré strictement inférieur à 1.

⚠ $\deg Q \leqslant 0 \implies Q = \text{cste}$

Théorème 6. Décomposition en polynômes irréductibles sur $\mathbb{C}$ - (~~admis~~)

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
- Tout polynôme $P \in \mathbb{C}[X]$ se décompose en produit de polynômes irréductibles :

$$P(X) = a(X - r_1)^{m_1}(X - r_2)^{m_2} \cdots (X - r_k)^{m_k}$$

où :

- a est le coefficient dominant de P,
- $r_1, \ldots, r_k$ sont les racines de P et
- $m_1, \ldots, m_k$ leurs multiplicités.

• $\deg P = \sum_{i=1}^{k} m_i$

De plus, cette décomposition est unique à l'ordre des facteurs près.

Preuve : Utiliser d'Alembert.

Exemple

1 n'est pas racine multiple : $\neq 0$ en 1

On considère le polynôme

$$P(X) = X^n - 1. = (X-1)\underbrace{(X^{n-1} + \dots + X^2 + X + 1)}$$

Les racines de P sont exactement les racines n-ièmes de l'unité :

$$\xi_k = e^{i\frac{2k\pi}{n}}, \qquad k = 0, 1, \dots, n-1.$$

Dur à faire pour tous les ξ_k

Il y en a n !

Ainsi :

$$X^n - 1 = (X-1)^{m_1} \times \left(X - e^{i\frac{2\pi}{n}}\right)^{m_2} \times \cdots \times \left(X - e^{i\frac{2(n-1)\pi}{n}}\right)^{m_n}$$

$$\begin{cases} m_1 + m_2 + \dots + m_n = n \\ m_i \geq 1 \end{cases} \Longrightarrow m_i = 1.$$

Donc ξ_k racine simples !

Dans $\mathbb{C}[X]$, on a toujours

$$m_1 + m_2 + \cdots + m_k = \deg(P).$$

$P(2) = 8 - 2 \times 4 - 2 + 2 = 0$

$P(1) = 1 - 2 - 1 + 2 = 0$

$P(-1) = -1 - 2 + 1 + 2 = 0$

Question 2

On considère le polynôme :

$$P(X) = X^3 - 2X^2 - X + 2.$$

Sa décomposition en irréductibles est l'une des propositions ci-dessous. Laquelle ?

1. $\cancel{(X-2)^3}$
2. $\cancel{(X-1)^3}$
3. $\cancel{(X+1)^3}$
4. $(X-2)(X-1)^2$
5. $\cancel{(X-2)(X+1)^2}$
6. $\cancel{(X-1)(X+1)^2}$
7. $(X-2)(X-1)(X+1)$

suggère de tester $X = 2, 1, -1$

3. Décomposition dans $\mathbb{R}[X]$

Dans ce cas là, il y a d'autres irréductibles que $(X-a)_{a\in\mathbb{R}}$. Lesquels ? Par ex : X^2+1, X^2+X+1

Proposition 6

Soit $P(X) = aX^2 + bX + c \in \mathbb{R}[X]$.

$$P \text{ est irréductible dans } \mathbb{R}[X] \iff b^2 - 4ac < 0.$$

Preuve : En prenant la négation :

P réductible dans $\mathbb{R}[X] \iff b^2-4ac \geq 0$

Or $\deg P = 2$ donc P réductible $\iff P = a\,A.B$, $\deg A, \deg B \geq 1$

mais $\deg P = \deg A + \deg B$

$\iff P(X) = a(X-\alpha)(X-\beta)$ car $\deg A = \deg B = 1$

$\iff P$ a deux racines réelles

$\iff \Delta \geq 0$ ☒

Par exemple, X^2+1 est irréductible dans $\mathbb{R}[X]$.

Tout polynôme $P \in \mathbb{R}[X]$ est aussi un polynôme de $\mathbb{C}[X]$.

Lemme 2. ♥

Soit $P \in \mathbb{R}[X]$. Alors pour tout $z \in \mathbb{C}$,

$$P(z) = 0 \iff P(\overline{z}) = 0.$$

De plus, si z et $\overline{z}$ sont racines de P (vu dans $\mathbb{C}[X]$), alors elles ont même multiplicité.

Preuve : $P(X) = \sum a_k X^k$ avec $a_k \in \mathbb{R}$

Donc $\overline{P(z)} = \overline{\sum a_k z^k} = \sum \overline{a_k}\, \overline{z}^k = \sum a_k \overline{z}^k = P(\overline{z})$

Attention : cette équivalence n'est pas vraie pour $P \in \mathbb{C}[X]$.

Ainsi $\overline{P(z)} = P(\overline{z})$

Donc $P(z) = 0 \iff \overline{P(z)} = 0 \iff P(\overline{z}) = 0$

Question 3

On a

$$(X - z)(X - \overline{z}) = \ ?$$

1. $X^2 - z^2$
2. $X^2 + z^2$
3. $X^2 - |z|^2$
4. $X^2 + |z|^2$
5. $X^2 - 2Re(z)X + |z|^2$
6. $X^2 + 2Re(z)X + |z|^2$
7. $X^2 - 2Im(z)X + |z|^2$
8. $X^2 + 2Im(z)X + |z|^2$

Pour tout $z \in \mathbb{C}$,

$$\underbrace{(X-z)}_{\in \mathbb{C}[X]}\underbrace{(X-\overline{z})}_{\in \mathbb{C}[X]} = \underbrace{X^2 - 2Re(z)X + |z|^2}_{\in \mathbb{R}[X]}$$

à priori (si $z \in \mathbb{C}\setminus\mathbb{R}$)

Pourquoi $\overline{z_i}$ a même multiplicité que z_i ?

Finalement :

1. $P \in \mathbb{R}[X] \subset \mathbb{C}[X]$ est décomposable dans $\mathbb{C}[X]$ sous la forme :

$$P(X) = a(X-z_1)^{m_1}(X-z_2)^{m_2}\cdots(X-z_k)^{m_k}$$

2. D'après le lemme 2, si z_i n'est pas réel, alors un facteur $(X-\overline{z}_i)^{m_i}$ apparaît aussi dans la décomposition.

   $\hookrightarrow$ Vrai mais un peu rapide

3. En regroupant $(X-z_i)^{m_i}$ et $(X-\overline{z}_i)^{m_i}$ on obtient le polynôme irréductible

$$(X^2 - 2Re(z_i)X + |z_i|^2)^{m_i} \in \mathbb{R}[X]$$

$z_i \in \mathbb{C}\setminus\mathbb{R}$ $\iff$ $Im\, z_i \neq 0$ $\iff$ $\Delta = b^2 - 4ac = 4\,Re(z_i)^2 - 4|z_i|^2 = -4\,Im(z_i)^2 < 0$ $\iff$ $X^2 - 2Re(z_i)X + |z_i|^2$ irréductible

$(X-1)P(X) = X^4 - 1$

Exemple

On a que $P(X) = X^3 + X^2 + X + 1$ se décompose dans $\mathbb{C}$ en

$$P(X) = (X+1)(X-\mathrm{i})(X+\mathrm{i}).$$

On a bien que i et son conjugué $-\mathrm{i}$ sont racines de multiplicité 1. En conséquence la décomposition de $P(X)$ dans $\mathbb{R}$ est

$$P(X) = (X+1)(X^2 - \mathrm{i}^2) = (X+1)(X^2+1).$$

Remarque: $(X^2+X+1) = (X-j)(X-\bar{j})$ où $j = e^{i\frac{2\pi}{3}}$

Exemple 7

1. Décomposer dans $\mathbb{C}[X]$ le polynôme X^4+X^2+1.
2. Décomposer dans $\mathbb{R}[X]$ le polynôme X^4+X^2+1.

① $(X^4+X^2+1) = (X^2-j)(X^2-\bar{j}) = (X-e^{i\frac{\pi}{3}})(X+e^{i\frac{\pi}{3}})(X-e^{-i\frac{\pi}{3}})(X+e^{-i\pi/3})$

② $= \left[(X-e^{i\frac{\pi}{3}})(X-e^{-i\frac{\pi}{3}})\right]\left[(X+e^{i\frac{\pi}{3}})(X+e^{-i\frac{\pi}{3}})\right]$

$= (\underbrace{X^2-X+1}_{\in\mathbb{R}[X]})(\underbrace{X^2+X+1}_{\in\mathbb{R}[X]})$ et irréd. $(\Delta<0)$

Théorème 7. Décomposition en irréductibles sur $\mathbb{R}$

- Les polynômes irréductibles dans $\mathbb{R}[X]$ sont :
  - les polynômes de degré 1,
  - les polynômes de degré 2 de discriminant < 0.

- Tout polynôme $P \in \mathbb{R}[X]$ se décompose sous la forme :

$$P(X) = a(X-r_1)^{m_1} \cdots (X-r_k)^{m_k} (X^2+b_1X+c_1)^{n_1} \cdots (X^2+b_\ell X+c_\ell)^{n_\ell}$$

où

  - a est le coefficient dominant de P,
  - $r_1, \ldots, r_k$ sont les racines réelles distinctes de P,
  - $m_1, \ldots, m_k$ leurs multiplicités respectives,
  - $X^2 + b_i X + c_i$ sont des polynômes distincts à coefficients réels vérifiant $b_i^2 - 4c_i < 0$.

De plus, cette décomposition est unique à l'ordre des facteurs près.

Conclusion : Comment factoriser dans $\mathbb{R}[X]$?

$P \in \mathbb{R}[X]$ polynôme de degré $d \geqslant 1$

$\downarrow$

dans $\mathbb{C}$

P admet d racines complexes $r_1, \dots, r_d$ (comptées avec multiplicité)

$\downarrow$

$$P(X) = a(X - r_1)(X - r_2)\cdots(X - r_d) \text{ dans } \mathbb{C}[X]$$

$\downarrow$

Si r_i n'est pas un réel, on peut l'associer à son conjugué dans le produit ci-dessus

$\downarrow$

On redescend

$$P(X) = a(X - r'_1)\dots(X - r'_k) \times (\text{polynômes irréductibles de degré } 2)$$

Question 4

On considère le polynôme

$$P(X) = X^4 + X^2 + 1.$$

Laquelle de ces propositions est exacte ?

1. ~~P n'a pas de racine réelle, donc il est irréductible dans $\mathbb{R}[X]$~~
2. P n'a pas de racine réelle, mais il n'est pas irréductible dans $\mathbb{R}[X]$
3. ~~P est de degré $\geqslant 3$ donc il a nécessairement une racine réelle~~
4. Aucune des proposition ci-dessus n'est exacte

$X^{10}+1$ n'a pas de racine dans $\mathbb{R}$

Question 5

Dans $\mathbb{R}[X]$, si P est de degré 3, alors :

1. il a au moins une racine réelle
2. il a au moins deux racines réelles
3. il a trois racines réelles
4. ~~il n'a pas forcément de racine réelle~~

car par TVI
+ $\lim\limits_{x \to +\infty} P(x) = +\infty$
+ $\lim\limits_{x \to -\infty} P(x) = -\infty$

$\exists\, x \in \mathbb{R}, P(x) = 0$

NON car $X \cdot (X^2+1)$ a une seule racine réelle.

Exercice (Même raisonnement).

Soit P un polynôme de degré impair de $\mathbb{R}[X]$. Démontrez de deux façons différentes que P admet au moins une racine réelle.

À venir

- TD 18 : préparer les question 1 et 2 de l'exercice 13
- Dates limites DM WIMS :
  - DM8 - Racines carrées et équations du second degré - 29 novembre 2020
  - DM9 - Polynômes, degré et multiplicité des racines - 6 décembre 2020
  - DM10 - Fractions rationnelles et décomposition en éléments simples - 13 décembre 2020
  - ...