1.3 Décomposition en facteurs irréductibles

Définition 1.12 *Un polynôme $P \in \mathbb{K}[X]$ est dit* irréductible *si ce n'est pas une constante et s'il n'y a pas de factorisation de P en deux polynômes non constants (autrement dit P n'est pas constant et ses seuls diviseurs sont les constantes non nulles et les polynômes de la forme cP où c est une constante non nulle).*

Un polynôme du premier degré est toujours irréductible. Soit P un polynôme irréductible. Si P ne divise pas le polynôme A, alors P est premier avec A. Si Q est un autre polynôme irréductible, alors ou bien il existe une constante non nulle c telle que $Q = cP$, ou bien P et Q sont premiers entre eux.

Les polynômes irréductibles jouent le rôle des nombres premiers.

Théorème 1.13 *Soit A un polynôme non constant de $\mathbb{K}[X]$. Alors il existe une décomposition*

$$A = cP_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où c est une constante non nulle, $P_1, \ldots, P_k$ sont des polynômes irréductibles unitaires distincts de $\mathbb{K}[X]$, et $\alpha_1, \ldots, \alpha_k$ des entiers strictement positifs. De plus, une telle décomposition est unique, à l'ordre des facteurs irréductibles près.

L'identification des polynômes irréductibles sur $\mathbb{C}$ et $\mathbb{R}$ repose sur le fameux

Théorème 1.14 (D'Alembert - Gauss) *Tout polynôme non constant de $\mathbb{C}[X]$ a une racine dans $\mathbb{C}$.*

La démonstration de ce théorème sort du cadre du cours. On en déduit :

Théorème 1.15 *Sur $\mathbb{C}$, les polynômes irréductibles unitaires sont les $X - c$ avec $c \in \mathbb{C}$. Sur $\mathbb{R}$, les polynômes irréductibles unitaires sont les $X - c$ avec $c \in \mathbb{R}$ et les $X^2 + bX + c$ sans racine réelle (c.-à-d. avec $b^2 - 4c < 0$).*

Rappelons que, si c est un nombre complexe, $(X - c)(X - \overline{c}) = X^2 - 2\,\mathrm{Re}(c)X + |c|^2 \in \mathbb{R}[X]$.

Exercice 1.19

Soit $P(X) = 3X^3 - 2X^2 - 7X - 2$ et $Q(X) = 2X^2 + 3X + 1$.

1. Utiliser l'algorithme d'Euclide pour déterminer le pgcd de P et Q.
2. Donner la décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$.
3. Quel est le ppcm de P et Q ?

Exercice 1.20

Décomposer dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$ les polynômes suivants en facteurs irréductibles

$$\begin{array}{lll} X^3 + 1 & X^3 - 1 & X^3 + 2X^2 + 2X + 1 \\ X^4 + 1 & X^4 + X^2 + 1 & 1 + X + X^2 + X^3 + X^4 + X^5 \end{array}$$

Exercice 1.21

Décomposer dans $\mathbb{R}[X]$, puis dans $\mathbb{Q}[X]$ le polynôme $P(X) = X^4 + 1$.

Exercice 1.22

Montrer qu'un polynôme de degré 2 ou 3 est irréductible sur un corps $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$. En est-il de même pour un polynôme de degré 4 ?

Exercice 1.23

Soient m et n deux entiers naturels non nuls.

1. Déterminer le reste de la division euclidienne de $P(X) = X^{2m} + (X+1)^n - 1$ par $X(X+1)$.

Dans toute la suite, on désigne par $A(X)$ un polynôme de degré supérieur ou égal à 1 de $\mathbb{C}[X]$ et on pose $B(X) = [A(X)]^{2m} + (A(X)+1)^n - 1$.

2. Montrer que $[A(X)]^2 + A(X)$ divise $B(X)$.
3. Montrer que, si x_0 est racine de multiplicité 1 de $A(X)$, alors x_0 est racine de multiplicité 1 de $B(X)$.
4. On suppose que $A(X) = X^2+1$, $m = 1$, et $n = 3$. Donner la décomposition en produit de facteurs irréductibles du polynôme $B(X)$ dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
5. On suppose que $A(X) = 1 - X + X^2$, $m = 1$ et $n = 2$.
   Donner la décomposition en produit de facteurs irréductibles du polynôme $B(X)$ dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.

Exercice 1.24

Soit P un polynôme à coefficients réels. Montrer que, si $P(x) \geq 0, \forall x \in \mathbb{R}$, alors il existe A et B dans $\mathbb{R}[X]$ tels que $P = A^2 + B^2$.

On pourra montrer que, si $A, B, C, D \in \mathbb{R}[X]$, alors $(A^2+B^2)(C^2+D^2)$ est encore une somme de deux carrés dans $\mathbb{R}[X]$.

Décomposer $X^4 + X^2 + 1$ en une somme de deux carrés dans $\mathbb{R}[X]$.