16

Polynômes

Dans tout le chapitre, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

16.1 Ensemble des polynômes à une indéterminée

16.1.1 Définition et règles de calcul

Définition 1: Polynôme

Un polynôme à cœfficients dans $\mathbb{K}$ est la donnée d'une suite presque nulle $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$, i.e. une suite à valeurs dans $\mathbb{K}$ pour laquelle il existe un entier $n_0 \in \mathbb{N}$ tel que pour tout $n \geqslant n_0, a_n = 0$ et on note alors

$$P = \sum_{k=0}^{n_0-1} a_k X^k,$$

où X est appelée l'indéterminée du polynôme P.
Les scalaires $(a_0, \ldots, a_{n_0-1})$ sont appelés les cœfficients du polynôme P.
L'ensemble des polynômes à une indéterminée à cœfficients dans $\mathbb{K}$ se note $\mathbb{K}[X]$.

Remarque 1. • Un polynôme de la forme $P(X) = a_n X^n$ est appelé un monôme.

• Un polynôme est dit constant s'il est de la forme $P(X) = a$, où $a \in \mathbb{K}$. En particulier, si $a = 0$, on dit que c'est le polynôme nul et on le note $0_{\mathbb{K}[X]}$.

Exemple 1. • Si $a_0 = 0, a_1 = 1$ et pour tout $n \geqslant 2, a_n = 0$, alors $P = X$.

• Si $a_0 = 1$ et pour tout $n \geqslant 1, a_n = 0$, alors $P = 1$.

• Si $a_0 = 2, a_1 = -3, a_2 = 0, a_3 = -4$ et pour tout $n \geqslant 4, a_n = 0$, alors $P = -4X^3 - 3X + 2$.

Définition 2: Opérations sur les polynômes

Soient $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ deux polynômes de $\mathbb{K}[X]$.

1. On définit pour tout $(\lambda, \mu) \in \mathbb{K}^2$ le polynôme $\lambda P + \mu Q \in \mathbb{K}[X]$ par
$$\lambda P + \mu Q = \sum_{k=0}^{\max(n,m)} (\lambda a_k + \mu b_k) X^k$$
avec éventuellement $a_k = 0$ si $k > n$ et $b_k = 0$ si $k > m$.
2. On définit le produit $PQ \in \mathbb{K}[X]$ par
$$PQ = \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ 0 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant m}} a_i b_j \right) X^k.$$
3. Pour tout $k \in \mathbb{N}$, on définit P^k par
$$P^k = \begin{cases} 1 & \text{si } k = 0 \\ \underbrace{P \times \cdots \times P}_{k \text{ fois}} & \text{si } k > 0. \end{cases}$$
4. On définit $P \circ Q$ par
$$P \circ Q = \sum_{k=0}^{n} a_k Q^k.$$

Exemple 2. Soient $P = 2X^2 + X - 1$ et $Q = X^3 - 5X + 2$.

Alors $2P + 3Q = 3X^3 + 4X^2 - 13X + 4$ et $PQ = 2X^5 + X^4 - 11X^3 - X^2 + 7X - 2$.

Remarque 2. Puisque le produit dans $\mathbb{K}$ est commutatif, on constate que le produit dans $\mathbb{K}[X]$ est commutatif. En particulier, on retrouve la formule du bnôme de Newton.

Proposition 1: Formule du binôme de Newton

Soient $(P, Q) \in \mathbb{K}[X]^2$.
Soit $n \in \mathbb{N}$.
On a
$$(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k} = \sum_{k=0}^{n} \binom{n}{k} P^{n-k} Q^k.$$

16.1.2 Degré d'un polynôme

Définition 3: Degré d'un polynôme

Soit $P = \sum_{k=0}^{n} a_k X^k$ où $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{R}^{n+1}$.
On suppose que P n'est pas le polynôme nul, c'est à dire qu'il existe $k \in [\![0, n]\!]$, tel que $a_k \neq 0$.

Soit $d = \max\{k \in [\![0, n]\!], a_k \neq 0\}$, i.e. $d \in [\![0, n]\!]$ et $P = \sum_{k=0}^{d} a_k X^k$ avec $a_d \neq 0$ (et pour tout $k \in [\![d+1, n]\!], a_k = 0$).
On dit que l'entier naturel d est le degré du polynôme P et on note

$$d = \deg(P).$$

Le cœfficient a_d est appelé le cœfficient dominant de P. Si $a_d = 1$, on dit que le polynôme P est unitaire.

Remarque 3. • Si $a_n \neq 0$, alors $\deg(P) = d = n$ et dans ce cas $[\![d+1, n]\!]$ est vide.
• Par convention, le degré du polynôme nul est $-\infty$, ce qu'on note $\deg(0) = -\infty$.
• Concrètement, le degré d'un polynôme non nul est la plus grande puissance de X apparaissant dans le polynôme.
• Les polynômes constants non nuls sont de degré 0.
• Pour tout $n \in \mathbb{N}$, l'ensemble des polynômes à cœfficients dans $\mathbb{K}$ de degré inférieur ou égal à n est noté $\mathbb{K}_n[X]$. En particulier, $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants dans $\mathbb{K}$.

Exemple 3. • Pour tout $n \in \mathbb{N}, \deg(X^n) = n$.
• $\deg(2X^3 + X - 1) = 3$ et le cœfficient dominant de ce polynôme est 2.

Proposition 2: Opérations sur les degrés

Soient $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ deux polynômes de $\mathbb{K}[X]$ avec $a_n \neq 0$ et $b_m \neq 0$.

1. Pour tout $\lambda \in \mathbb{K}^*, \lambda P$ est un polynôme de degré $\deg(P)$ et on a
$$\lambda P(X) = \sum_{k=0}^{n} (\lambda a_k) X^k.$$
2. On a
$$\deg(P + Q) \leqslant \max(\deg(P), \deg(Q)).$$
L'inégalité est une égalité si $\deg(P) \neq \deg(Q)$.
3. On a $\deg(PQ) = \deg(P) + \deg(Q)$.
4. Si Q est non constant, alors
$$\deg(P \circ Q) = \deg(P) \deg(Q).$$

Remarque 4. • Si $\lambda = 0, \lambda P = 0$.
• Si $Q = 0$, alors $P + Q = P$ et $PQ = 0$. On retrouve $\deg(PQ) = \deg(P) + \deg(Q)$ avec la convention $\deg(P) + (-\infty) = -\infty$.

Démonstration.

1. Soit $\lambda \in \mathbb{K}^*$.
   On a alors pour tout $\lambda P = \lambda \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{n} (\lambda a_k X^k)$, avec $\lambda a_n \neq 0$, d'où le résultat.
2. • Supposons que $\deg(P) \neq \deg(Q)$. Sans perte de généralité, on peut supposer (quitte à échanger P et Q) que $\deg(Q) < \deg(P)$, i.e. $m < n$.
   On pose alors pour tout $k \in [\![m+1, n]\!], b_k = 0$.
   Il vient
   $$P + Q = \sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{n} b_k X^k = \sum_{k=0}^{n} (a_k + b_k) X^k,$$
   avec $a_n + b_n = a_n \neq 0$ donc $\deg(P+Q) = n = \deg(P) = \max(\deg(P), \deg(Q))$.
   • Supposons que $\deg(P) = \deg(Q)$, i.e. $n = m$. On a comme précédemment
   $$P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k.$$
   Ainsi, $\deg(P+Q) = n$ si $a_n + b_n \neq 0$ et $\deg(P+Q) < n$ si $a_n + b_n = 0$ donc dans tous les cas, $\deg(P+Q) \leqslant n = \max(\deg(P), \deg(Q))$.
3. On a
   $$PQ = \left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} \left(\sum_{\substack{i+j=k \\ 1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} a_i b_j\right) X^k.$$
   Pour $k = n + m$, on a $\sum_{\substack{i+j=k \\ 1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}} a_i b_j = a_n b_m \neq 0$ donc $\deg(PQ) = n + m = \deg(P) + \deg(Q)$.
4. On a
   $$P \circ Q = \sum_{k=0}^{n} a_k Q^k = \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{m} b_i X^i\right)^k = \sum_{k=0}^{n} a_k (b_m^k X^{km} + \cdots + b_0^k)$$
   donc si $m \neq 0$, i.e. si Q n'est pas constant, on constate que le cœfficient dominant de $P \circ Q$ est $a_n b_m^n \neq 0$ et est situé devant x^{nm} d'où le résultat.

■

Remarque 5. • Si $\deg(P) = \deg(Q)$, on peut avoir $\deg(P+Q) < \max(\deg(P), \deg(Q))$.
En effet, si $P = X+1$ et $Q = -X$, on a $\deg(P) = \deg(Q) = 1$ donc $\max(\deg(P), \deg(Q)) = 1$ et $P + Q = 1$ donc $\deg(P+Q) = 0 < \max(\deg(P), \deg(Q))$.
• Si Q est constant, on peut avoir $\deg(P \circ Q) \neq \deg(P)\deg(Q)$. Par exemple, si $P(X) = X - 1$ et $Q(X) = 1$, alors $P \circ Q(X) = 0$ donc $\deg(P \circ Q) = -\infty$, tandis que $\deg(P)\deg(Q) = 1 \times 0 = 0$.
• Le produit de deux polynômes non nuls est non nul. En effet, si $\deg(P) \geqslant 0$ et $\deg(Q) \geqslant 0$, alors $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0$ donc $PQ \neq 0$.

Exemple 4. • Soit $P = 2X^3 - X$ et $Q = 3X^2 + X + 2$. On a $\deg(P) = 3$ et $\deg(Q) = 2$.
Alors $PQ = 6X^5 + 2X^4 + X^3 - X^2 - 2X$ donc $\deg(PQ) = 5 = \deg(P) + \deg(Q)$ et
$$Q \circ P = 3(2X^3 - X)^2 + 2X^3 - X + 2 = 12X^6 - 12X^4 + 2X^3 + 3X^2 - X + 2$$
donc $\deg(Q \circ P) = 6 = \deg(P) \times \deg(Q)$.

16.1.3 Divisibilité et division euclidienne

Définition 4: Divisibilité dans $\mathbb{K}[X]$

Soient $(P, Q) \in \mathbb{K}[X]^2$.
On dit que P divise Q s'il existe un polynôme $R \in \mathbb{K}[X]$ tel que

$$Q = PR.$$

Dans ce cas, on dit que Q est divisible par P ou est un multiple de P et que P est un diviseur de Q.

Remarque 6. • Le polynôme nul est divisible par tous les polynômes de $\mathbb{K}[X]$.

• Les polynômes constants non nuls divisent tous les polynômes.

En effet, pour tout $\lambda \in \mathbb{K}^*$, pour tout $P \in \mathbb{K}[X], P = \lambda \times \left(\frac{1}{\lambda} P\right)$.

Exemple 5. • Pour tout $n \in \mathbb{N}^*, X$ divise X^n puisque $X^n = X \times X^{n-1}$.

• Pour tout $a \in \mathbb{K}$, pour tout $n \in \mathbb{N}^*, X - a$ divise $X^n - a^n$ car

$$X^n - a^n = (X - a) \sum_{k=0}^{n-1} a^{n-1-k} X^k.$$

• Le polynôme $X^2 - 2X + 3$ divise $X^3 - X + 6$ car $(X^2 - 2X + 3)(X + 2) = X^3 - X + 6$.

Théorème 1: Théorème de la division euclidienne

Soient $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0$.
Alors il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que

$$\begin{cases} A & = & BQ + R \\ \deg(R) & < & \deg(B) \end{cases}.$$

On dit que Q est le quotient de la division euclidienne de A par B et que R en est le reste.

Démonstration.

• **Existence :**

Notons $B = \sum_{k=0}^{m} b_k X^k$ avec $\deg(B) = m \geqslant 0$ par hypothèse. En particulier, $b_m \neq 0$.

L'existence du couple (Q, R) est évidente si $\deg(A) < \deg(B)$. En effet, il suffit alors de prendre $Q = 0$ et $R = A$.

Montrons alors par récurrence sur $n \geqslant m$ le résultat suivant :

$$\ll \text{ Si } A \in \mathbb{K}_n[X], \text{alors il existe} (Q, R) \in (\mathbb{K}[X])^2 \text{ avec } \deg(R) < \deg(B) \text{ tel que } A = BQ + R. \gg$$

▷ *Initialisation :* Pour $n = m$, on a $\deg(A) \leqslant n = m$. On a déjà vu que le résultat est évident si $\deg(A) < \deg(B)$.

Supposons donc que $\deg(A) = m$ et posons $A = \sum_{k=0}^{m} a_k X^k$.

Posons $R = A - \dfrac{a_m}{b_m}\displaystyle\sum_{k=0}^{m} b_k X^k$. En comparant les degrés et les cœfficients dominants de A et de $\dfrac{a_m}{b_m}\displaystyle\sum_{k=0}^{m} b_k X^k$, on constate qu'ils sont identiques donc $\deg(R) < m = \deg(B)$ et on a bien $A = BQ + R$ avec $Q = \dfrac{a_m}{b_m}$.

La propriété est donc vraie au rang $n = m$.

▷ *Hérédité :* Soit $n \geqslant m$ fixé. Supposons la propriété vraie au rang n. Montrons qu'elle est vraie au rang $n + 1$.

Posons $A = \displaystyle\sum_{k=0}^{n+1} a_k X^k \in \mathbb{K}_{n+1}[X]$. Si $a_{n+1} = 0$, alors $A \in \mathbb{K}_n[X]$ et la propriété est vraie par hypothèse de récurrence.

Supposons donc que $a_{n+1} \neq 0$. Posons alors $S = A - \dfrac{a_{n+1}}{b_m} X^{n+1-m} B$.

On a $\deg\left(\dfrac{a_{n+1}}{b_m} X^{n+1-m} B\right) = n + 1 - m + \deg(B) = n + 1 = \deg(A)$ et son cœfficient dominant est a_{n+1}.

Ainsi, A et $\dfrac{a_{n+1}}{b_m} X^{n+1-m} B$ ont même degré et même cœfficient dominant donc

$$\deg(S) = \deg\left(A - \frac{a_{n+1}}{b_m} X^{n+1-m} Q\right) < \deg(A) = n + 1,$$

i.e. $S \in \mathbb{K}_n[X]$.

Par hypothèse de récurrence, il existe $(Q_1, R_1) \in (\mathbb{K}[X])^2$ avec $\deg(R_1) < \deg(B)$ tel que $S = BQ_1 + R_1$. Il vient alors $A = S + \dfrac{a_{n+1}}{b_m} X^{n+1-m} B = B\left(Q_1 + \dfrac{a_{n+1}}{b_m} X^{n+1-m}\right) + R_1$.

En posant $Q = Q_1 + \dfrac{a_{n+1}}{b_m} X^{n+1-m}$ et $R = R_1$, on a bien $A = BQ + R$ avec $\deg(R) < \deg(B)$, ce qui prouve la propriété au rang $n + 1$ et achève la récurrence.

L'existence est donc prouvée.

• **Unicité :**

Supposons qu'il existe $(Q, Q_1, R, R_1) \in (\mathbb{K}[X])^4$ avec $\deg(R) < \deg(B)$ et $\deg(R_1) < \deg(B)$ tels que $A = BQ + R = BQ_1 + R_1$.

Ainsi, $B(Q - Q_1) = R_1 - R$.

On a $\deg B(Q - Q_1) = \deg(R_1 - R) \leqslant \max(\deg(R_1), \deg(R)) < \deg(B)$.

Or, si on avait $Q \neq Q_1$, on aurait $Q - Q_1 \neq 0$ donc $\deg(B(Q - Q_1)) = \deg(B) + \underbrace{\deg(Q - Q_1)}_{\geqslant 0} \geqslant \deg(B)$, ce qui mènerait à une contradiction.

Ainsi, $Q = Q_1$ et il en découle que $R = R_1$ d'où l'unicité du couple (Q, R). ■

Exemple 6. Soit $A = 2X^7 + X^5 - 3X^4 + 5X^2 - X + 1$ et $B = X^4 + X^2 - 2X - 3$.

La division euclidienne de A par B est

$$2X^7 + X^5 - 3X^4 + 5X^2 - X + 1 = (X^4 + X^2 - 2X - 3)(2X^3 - X + 1) + 7X^3 + 2X^2 - 2X + 4.$$

On a donc $A = BQ + R$ avec $Q = 2X^3 - X + 1$ et $R = 7X^3 + 2X^2 - 2X + 4$ où $\deg(R) = 3 < \deg(B) = 4$.

Remarque 7. A l'instar de l'algorithme d'Euclide sur les entiers, on peut élaborer un algorithme de divison euclidienne sur les polynômes de la manière suivante : étant donnés deux polynômes A_0 et B_0 avec $B_0 \neq 0$, on réalise la division euclidienne de A_0 par B_0 :

$$A_0 = B_0 Q_0 + R_0 \quad \text{avec } \deg(R_0) < \deg(B_0).$$

Tant que $R_n \neq 0$, on pose $A_{n+1} = B_n$ et $B_{n+1} = R_n$, puis on réalise la division euclidienne de A_{n+1} par $B_{n+1} = R_n \neq 0$:

$$A_{n+1} = B_{n+1}Q_{n+1} + R_{n+1} \quad \text{avec} \deg(R_{n+1}) < \deg(B_{n+1}) = \deg(R_n).$$

On obtient donc une suite strictement décroissante d'entiers

$$\deg(R_0) > \deg(R_1) > \cdots > \deg(R_n) > \deg(R_{n+1}).$$

Nécessairement, au bout d'un certain nombre d'étapes, il existera un entier p tel que $R_p = 0$. Lorsqu'on divise le dernier reste non nul R_{p-1} par son cœfficient dominant, le polynôme obtenu est alors le PGCD des polynômes A_0 et B_0.

Exemple 7. Posons $A_0 = X^4 - X^2 + X + 1$ et $B_0 = X^3 - 1$.

On a $A_0 = XB_0 - X^2 + 2X - 1$ donc $R_0 = -X^2 + 2X - 1$. Posons $A_1 = B_0$ et $B_1 = R_0$.

On a alors $A_1 = B_1(-X - 2) + 3X - 3$ donc $R_1 = 3X - 3$.

Posons $A_2 = B_1 = R_0 = -X^2 + 2X - 1$ et $B_2 = R_1 = 3X - 3$.

On constate que B_2 divise A_2 puisque $A_2 = -\dfrac{1}{3}(X - 1)B_2$ donc $R_2 = 0$.

Le dernier reste non nul est $R_1 = 3X - 3$ donc le PGCD de A_0 et B_0 est $\dfrac{1}{3}R_1 = X - 1$.

16.2 Racines et factorisation

16.2.1 Fonction polynomiale

Définition 5: Fonction polynomiale

Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.

On appelle fonction polynomiale associée à P la fonction

$$P : \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & \displaystyle\sum_{k=0}^{n} a_k x^k \end{array}.$$

Exemple 8. • Les fonctions affines $P : x \longmapsto ax + b$, où $(a, b) \in \mathbb{K}^2$ sont des fonctions polynomiales.

• Les fonctions puissances entières $P : x \longmapsto x^n$, où $n \in \mathbb{N}$, étudiées dans le chapitre ≪ Fonctions d'une variable réelles ≫sont des fonctions polynomiales.

Remarque 8. • Quitte à considérer sa fonction polynomiale associée, on peut donc évaluer un polynôme en un nombre complexe.

Par exemple, si $P = X^3 + X^2 - 1$, alors $P(2) = 2^3 + 2^2 - 1 = 11$.

• Une méthode efficace pour évaluer un polynôme $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ en un scalaire α est la méthode de Horner : au lieu de calculer toutes les puissances de α jusqu'à α^n, puis de faire le produit avec les cœfficients du polynôme et enfin la somme des résultats obtenus, il est plus judicieux de faire comme suit :

$$P(\alpha) = ((\ldots((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + \ldots)\alpha + a_1)\alpha + \alpha,$$

ce qui fait beaucoup moins de produits à calculer.

Exemple 9. Soit $P = X^3 - X^2 + 2X - 5$. Alors

$$P(4) = ((1 \times 4 - 1) \times 4 + 2) \times 4 - 5 = 51.$$

En pratique, on commet souvent l'abus de confondre un polynome et la fonction polynomiale associée à celui-ci. Cet abus est justifié par ce qui suit, à savoir qu'un polynôme est entièrement déterminé par sa fonction polynomiale associée.

Proposition 3: Unicité de l'écriture du polynôme nul

Soit $P : x \longmapsto \sum_{k=0}^{n} a_k x^k$, où $n \in \mathbb{N}$ et $(a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$.
P est la fonction nulle si et seulement si pour tout $k \in [\![0, n]\!], a_k = 0$.

Démonstration. • Si pour tout $k \in [\![0, n]\!], a_k = 0$, il est clair que P est le polynôme nul.
• Montrons par récurrence sur $n \in \mathbb{N}$ la propriété suivante :

$$\ll \text{ Si pour tout } x \in \mathbb{R}, P(x) = \sum_{k=0}^{n} a_k x^k = 0, \text{ alors pour tout } k \in [\![0, n]\!], a_k = 0. \gg$$

Pour $n = 0$, on a pour tout $x \in \mathbb{R}, P(x) = a_0 = 0$ donc la propriété est vraie au rang $n = 0$.
Soit $n \in \mathbb{N}$ fixé. On suppose la propriété vraie au rang n. Montrons qu'elle est vraie au rang $n + 1$.

Soient $(a_0, \ldots, a_{n+1}) \in \mathbb{K}^{n+2}$ tels que pour tout $x \in \mathbb{R}, P(x) = \sum_{k=0}^{n+1} a_k x^k = 0$.

La fonction P est constante égale à 0 sur $\mathbb{R}$ donc P est dérivable sur $\mathbb{R}$ et on a pour tout $x \in \mathbb{R}$,

$$0 = P'(x) = \sum_{k=1}^{n+1} k a_k x^{k-1} = \sum_{k=0}^{n} (k+1) a_{k+1} x^k.$$

Par hypothèse de récurrence, on en déduit que pour tout $k \in [\![0, n]\!] (k+1) a_{k+1} = 0$ d'où pour tout $k \in [\![1, n+1]\!], a_k = 0$.

Ainsi, pour tout $x \in \mathbb{R}, P(x) = a_0 = 0$, donc pour tout $k \in [\![0, n+1]\!], a_k = 0$, ce qui prouve la propriété au rang $n + 1$ et achève la récurrence. ■

16.2.2 Polynôme dérivé

Définition 6: Polynôme dérivé

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, avec $a_n \neq 0$.
On appelle polynôme dérivé de P le polynôme

$$P' = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

Remarque 9. • La fonction $P' : x \longmapsto P'(x)$ est la dérivée sur $\mathbb{R}$ de la fonction $P : x \longmapsto P(x)$.

En effet, si pour tout $x \in \mathbb{R}, P(x) = \sum_{k=0}^{n} a_k x^k$ avec $a_n \neq 0$, alors pour tout $x \in \mathbb{R}$,

$$P'(x) = \sum_{k=1}^{n} k a_k x^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k.$$

• Ce lien entre polynôme dérivé et dérivée de la fonction polynomiale associée permet d'étendre les opérations connues sur les dérivées aux polynômes. En particulier, les formules donnant la dérivée d'une combinaison linéaire, d'un produit, ou encore la formule de Leibniz restent valables pour les polynômes.

• Si $n = 0$, i.e. si P est constant, alors $P' = 0$ (en effet, la somme va de 0 à -1 et est donc vide). Réciproquement, si $P' = 0$, alors P est un polynôme constant.

• Le polynôme dérivé du polynômé nul est le polynôme nul.

Exemple 10. Si $P(X) = -2X^5 + X^3 + 3X^2 - 1$, alors $P'(X) = -10X^4 + 3X^2 + 6X$.

Proposition 4: Degré du polynôme dérivé

Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$.
Alors $\deg(P') = n - 1$.

Démonstration. Soit $n \in \mathbb{N}^*$. Soit $P(X) = \displaystyle\sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$ de telle sorte que $\deg(P) = n$.

Alors $P'(X) = \displaystyle\sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$.

Le cœfficient dominant de P' est $na_n \neq 0$ et il est situé devant X^{n-1} donc

$$\deg(P') = n - 1 \in \mathbb{N}.$$

■

Remarque 10. Si $\deg(P) = 0$, alors $\deg(P') = -\infty$.

Proposition 5: Dérivée p-ème

Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$, avec $a_n \neq 0$, i.e. $\deg(P) = n$.
Soit $p \in \mathbb{N}$. On note $P^{(p)}$ la dérivée p-ème de P.
Alors

$$P^{(p)} = \begin{cases} \displaystyle\sum_{k=0}^{n-p} \frac{(k+p)!}{k!} a_{k+p} X^k & \text{si } p \leqslant n \\ 0 & \text{si } p > n \end{cases}$$

En particulier, si $p \leqslant n, \deg(P^{(p)}) = n - p$.

Démonstration. Soit $k \in [\![0, n]\!]$.

On sait que la dérivée p-ème de $x \longmapsto x^k$ est $x \longmapsto \dfrac{k!}{(k-p)!} x^{k-p}$ si $p \in [\![0, k]\!]$ et 0 sinon.

Par linéarité de la dérivation, on trouve que si $p \in [\![0, n]\!]$,

$$P^{(p)} = \sum_{k=p}^{n} a_k \frac{k!}{(k-p)!} X^{k-p} = \sum_{k=0}^{n-p} \frac{(k+p)!}{k!} a_{k+p} X^k$$

et si $p > n, P^{(p)} = 0$. ■

16.2.3 Racines d'un polynôme

Définition 7: Racines d'un polynôme

Soit $P \in \mathbb{K}[X]$. Soit $\alpha \in \mathbb{K}$.
On dit que α est une racine (ou un zéro) de P si

$$P(\alpha) = 0.$$

Exemple 11. • Le polynôme $P = X + 1$ admet comme unique racine $\alpha = -1$.

• Le polynôme $P = X^2 - 2X + 1 = (X-1)^2$ admet comme unique racine $\alpha = 1$.

• Le polynôme $P = X^2 - 5X + 6 = (X-2)(X-3)$ admet comme racines $\alpha_1 = 2$ et $\alpha_2 = 3$.

• Le polynôme $P = X^3 - 1$ admet comme unique racine réelle $\alpha = 1$. Il admet trois racines complexes : $1, j$ et j^2.

• Le polynôme $P = X^2 + 1$ n'admet aucune racine réelle mais admet deux racines complexes que sont i et $-i$.

Proposition 6

Soit $P \in \mathbb{R}[X]$ de degré impair.
Alors P admet au moins une racine réelle.

Démonstration. Soit $n = \deg(P) \in \mathbb{N}^*$. Alors il existe $(a_0, \dots, a_n) \in \mathbb{R}^{n+1}$ avec $a_n \neq 0$ tels que pour tout $x \in \mathbb{R}, P(x) = \displaystyle\sum_{k=0}^{n} a_k x^k$.

Puisque n est impair, on a $\displaystyle\lim_{x\to+\infty} x^n = +\infty$ et $\displaystyle\lim_{x\to-\infty} x^n = -\infty$.

• Si $a_n > 0$, on a alors $\displaystyle\lim_{x\to+\infty} a_n x^n = +\infty$ et $\displaystyle\lim_{x\to-\infty} a_n x^n = -\infty$, d'où $\displaystyle\lim_{x\to+\infty} P(x) = +\infty$ et $\displaystyle\lim_{x\to-\infty} P(x) = -\infty$.

• Si $a_n < 0$, on a alors $\displaystyle\lim_{x\to+\infty} a_n x^n = -\infty$ et $\displaystyle\lim_{x\to-\infty} a_n x^n = +\infty$, d'où $\displaystyle\lim_{x\to+\infty} P(x) = -\infty$ et $\displaystyle\lim_{x\to-\infty} P(x) = +\infty$.

Dans les deux cas, la fonction P est continue sur $\mathbb{R}$ et prend des valeurs positives et négatives.

D'après le théorème des valeurs intermédiaires, il existe nécessairement un réel α tel que $P(\alpha) = 0$. ■

Remarque 11. Ce n'est plus nécessairement le cas pour les polynômes de degré pair puisque le polynôme $P = X^2 + 1$ n'admet pas de racine réelle. En effet, pour tout réel $x, P(x) > 0$.

Lemme 1: Division euclidienne par $(X - \alpha)$

Soit $P \in \mathbb{K}[X]$, soit $\alpha \in \mathbb{K}$.
Il existe un unique polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha)Q + P(\alpha).$$

Démonstration. D'après le théorème de la division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = (X-\alpha)Q + R$ et $\deg(R) < \deg(X - \alpha) = 1$. Ainsi, $\deg(R) = 0$ ou $\deg(R) = -\infty$ donc R est un polynôme constant, éventuellement nul.

De plus, en évaluant l'égalité $P = (X-\alpha)Q + R$ en α, on obtient $R = P(\alpha)$, d'où le résultat voulu. ■

Corollaire 1: Factorisation d'un polynôme admettant une racine

Soit $P \in \mathbb{K}[X]$, soit $\alpha \in \mathbb{K}$.
Le scalaire α est racine de P si et seulement s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$, autrement dit, $(X - \alpha)$ divise P.
En outre, le polynôme Q est unique s'il existe.

Démonstration. • S'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q$, alors

$$P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0,$$

ce qui implique que α est racine de P.

• Réciproquement, supposons que α est racine de P, i.e. $P(\alpha) = 0$.
D'après le lemme précédent, il existe un unique polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha)Q + P(\alpha) = (X - \alpha)Q.$$

■

Exemple 12. • $X^3 - 1 = (X - 1)(X^2 + X + 1)$.
• $X^3 - X^2 - X + 1 = (X^2 - 2X + 1)(X + 1)$.
•$X^3 - 6X^2 + 11X - 6 = (X - 1)(X^2 - 5X + 6)$.

Corollaire 2: Factorisation d'un polynôme admettant plusieurs racines

Soit $P \in \mathbb{K}[X]$ admettant des racines distinctes $\alpha_1, \dots, \alpha_p$.
Alors il existe $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)(X - \alpha_2) \dots ...(X - \alpha_p)Q.$$

Démonstration. D'après la proposition précédente, il existe $Q_1 \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)Q_1.$$

Puisque α_2 est une racine de P, on a $0 = P(\alpha_2) = (\alpha_2 - \alpha_1)Q_1(\alpha_2)$.
Or, $\alpha_2 \neq \alpha_1$ donc $Q_1(\alpha_2) = 0$.
On en déduit qu'il existe $Q_2 \in \mathbb{K}[X]$ tel que $Q_1 = (X - \alpha_2)Q_2$ d'où $P = (X - \alpha_1)(X - \alpha_2)Q_2$.
On en déduit que α_3 est une racine de Q_2 et ainsi de suite.
A la fin, on obtient bien un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)(X - \alpha_2) \dots ...(X - \alpha_p)Q.$$

■

Exemple 13. • $X^3 - X^2 - X + 1 = (X^2 - 2X + 1)(X + 1) = (X - 1)^2(X + 1)$.
•$X^3 - 6X^2 + 11X - 6 = (X - 1)(X^2 - 5X + 6) = (X - 1)(X - 2)(X - 3)$.
• $X^3 - 1 = (X - 1)(X - j)(X - j^2)$.

Corollaire 3: Nombre de racines d'un polynôme non nul

Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$.
Le nombre de racines de P est inférieur ou égal à n.

Démonstration. Soient $\alpha_1, \dots, \alpha_p$ des racines distinctes de P.

D'après le corollaire précédent, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)(X - \alpha_2)\ldots\ldots(X - \alpha_p)Q.$$

Notons que Q ne peut pas être le polynôme nul, puisque P ne l'est pas, donc $\deg(Q) \geqslant 0$. En comparant les degrés, on a

$$n = \deg(P) = p + \deg(Q) \geqslant p,$$

d'où le résultat. ∎

Remarque 12. • Le polynôme nul admet une infinité de racines. En fait, si on sait qu'un polynôme P est de degré inférieur ou égal à n et qu'il admet un nombre de racines strictement supérieur à n, alors P est le polynôme nul.

• S'il existe une infinité de scalaires α pour lesquels $P(\alpha) = Q(\alpha)$, alors le polynôme $P - Q$ admet une infinité de racines donc $P - Q$ est le polyôme nul donc $P = Q$.

En particulier, si I est un intervalle de $\mathbb{R}$ non réduit à un singleton tel que pour tout $x \in I, P(x) = Q(x)$, alors $P = Q$ et on peut en déduire que pour tout $x \in \mathbb{C}, P(x) = Q(x)$.

• Un polynôme constant non nul n'admet pas de racines.

Exemple 14. • Le polynôme $P = X^3 - 1 = (X-1)(X^2 + X + 1)$ est de degré 3 et admet pour unique racine réelle $\alpha = 1$ car le polynôme $Q = X^2 + X + 1$ n'admet pas de racine réelle.

• Le polynôme $P = X^3 - 6X^2 + 11X - 6$ est de degré 3 et admet 3 racines réelles distinctes : $1, 2$ et 3.

Ainsi, un polynôme de degré n admet au maximum n racines distinctes. S'il admet exactement n racines, on connaît sa factorisation :

Corollaire 4: Factorisation d'un polynôme admettant autant de racines que son degré

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$. On suppose que P admet n racines distinctes $\alpha_1, \ldots, \alpha_n$.
Alors

$$P = a_n(X - \alpha_1)\ldots(X - \alpha_n)$$

où a_n est le cœfficient dominant de P.

Démonstration. D'après le Corollaire 3, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha_1)\ldots(X - \alpha_n)Q.$$

En comparant les degrés, on a $n = \deg(P) = n + \deg(Q)$ donc $\deg(Q) = 0$, i.e. Q est un polynôme constant.

Notons $Q = a_n \in \mathbb{K}^*$.

Alors $P = a_n(X - \alpha_1)\ldots(X - \alpha_n)$ et en développant, on remarque que a_n est le cœfficient devant X^n, donc a_n est bien le cœfficient dominant de P. ∎

Remarque 13. On a déjà vu que pour un trinôme du second degré $P = aX^2 + bX + c$ admettant deux racines distinctes x_1 et x_2, on a $P = a(X - x_1)(X - x_2)$.

Exemple 15. • $2X^2 - 10X + 12 = 2(X-2)(X-3)$.

• Soit $n \in \mathbb{N}^*$. Soit $\omega = e^{\frac{2i\pi}{n}}$. On sait que les $(\omega^k)_{k \in [\![0,n-1]\!]}$ sont n racines distinctes du polynôme $X^n - 1 = 0$ qui est de degré n et unitaire.

Ainsi, $X^n - 1 = \displaystyle\prod_{k=0}^{n-1}(X - \omega^k)$.

Corollaire 5: Unicité de l'écriture des polynômes

Soient $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$ deux polynômes où $(n,m) \in \mathbb{N}^2, (a_0,\dots,a_n) \in \mathbb{K}^{n+1}, (b_0,\dots,b_m) \in \mathbb{K}^{m+1}$ avec $a_n \neq 0$ et $b_m \neq 0$.
Alors $P = Q$ si et seulement si $n = m$ et pour tout $k \in [\![0,n]\!], a_k = b_k$.

Démonstration. • Si $n = m$ et pour tout $k \in [\![0,n]\!], a_k = b_k$, il est clair que $P = Q$.

• Supposons que $P = Q$. Montrons que $n = m$ et que pour tout $k \in [\![0,n]\!], a_k = b_k$.

Puisque $P = Q$, en considérant les fonctions polynomiales associées à P et à Q, on a pour tout $x \in \mathbb{K}, P(x) = Q(x)$, i.e. $(P - Q)(x) = 0$.

Ainsi, le polynôme $P - Q$ admet une infinité de racines : c'est donc le polynôme nul.

D'après l'unicité de l'écriture du polynôme nul, on en déduit que tous les cœfficients de $P - Q$ sont nuls, ce qui implique que $n = m$ et que pour tout $k \in [\![0,n]\!], a_k = b_k$.

■

Remarque 14. • L'écriture d'un polynôme est donc unique. En particulier, un polynôme est entièrement déterminé par la donnée de ses cœfficients.

• Ceci légitime les processus d'identification des cœfficients entre deux polynômes.

Par exemple, si pour tout $x \in \mathbb{R}, P(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 3x^4 - x^2 + 2x + 1$, on en déduit que

$$\begin{cases} a_4 &= 3 \\ a_3 &= 0 \\ a_2 &= -1 \\ a_1 &= 2 \\ a_0 &= 1 \end{cases}.$$

Définition 8: Ordre de multiplicité d'une racine

Soit $P \in \mathbb{K}[X]$ un polynôme non nul, soit $\alpha \in \mathbb{K}$ une racine de P.
On appelle ordre de multiplicité de la racine α le plus grand entier $m \in \mathbb{N}^*$ tel que $(X - \alpha)^m$ divise P, i.e. le plus grand entier $m \in \mathbb{N}^*$ pour lequel il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$P = (X - \alpha)^m Q.$$

• Si $m = 1$, on dit que α est une racine simple de P.
• Si $m = 2$, on dit que α est une racine double de P.
• Si $m \geqslant 2$, on dit que α est une racine multiple de P.

Remarque 15. • Si α est une racine d'ordre de multiplicité m de P, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)^m Q$ et dans ce cas, on a nécessairement $Q(\alpha) \neq 0$.

Sinon, on aurait $Q = (X - \alpha)R$, d'où $P = (X - \alpha)^{m+1}R$, ce qui contredit le fait que α est une racine d'ordre m de P.

• Si P est de degré $n \in \mathbb{N}^*$, l'ordre de multiplicité m de toute racine α de P vérifie $m \leqslant n$.

En effet, si $P = (X - \alpha)^m Q$, alors $\deg(P) = m + \deg(Q) \geqslant m$.

Exemple 16. Soit $P = X^3 - X^2 - X + 1 = (X - 1)^2(X + 1)$. Alors P admet une racine double qui est 1 et une racine simple qui est -1.

Définition 9: Polynôme scindé

Soit $P \in \mathbb{K}[X]$.
• On dit que P est scindé sur $\mathbb{K}$ s'il existe des scalaires $(x_1, \dots, x_p) \in \mathbb{K}^p$ deux à deux distincts et des entiers $(m_1, \dots, m_p) \in (\mathbb{N}^*)^p$ tels que

$$P = a \prod_{k=1}^{p} (X - x_k)^{m_k},$$

où a est le cœfficient dominant de P.
• On dit dans ce cas que P est scindé à racines simples si pour tout $k \in [\![1, p]\!], m_k = 1$.

Remarque 16. • Un polynôme de degré 1 sur $\mathbb{K}$ est scindé (à racines simples) sur $\mathbb{K}$.
En effet, si $P = aX + b$ avec $(a, b) \in \mathbb{K}^2$ et $a \neq 0$, alors $P = a(X + \frac{b}{a})$.

• Soit $P \in \mathbb{R}[X]$ un polynôme de degré 2. Alors P est scindé sur $\mathbb{R}$ si et seulement si $\Delta \geqslant 0$. De plus, P est scindé à racines simples sur $\mathbb{R}$ si $\Delta > 0$.

• Soit $P \in \mathbb{C}[X]$ un polynôme de degré 2. Alors P est scindé sur $\mathbb{C}$. De plus, P est scindé à racines simples sur $\mathbb{C}$ si et seulement si $\Delta \neq 0$.

Exemple 17. • Le polynôme $P = (X-1)^2(X+1)$ est scindé. 1 est une racine double de P et -1 en est une racine simple.

• Le polynôme $P = X^3 - 1 = (X-1)(X^2 + X + 1) = (X-1)(X-j)(X-j^2)$ n'est pas scindé sur $\mathbb{R}$, mais il est scindé à racines simples sur $\mathbb{C}$.

Proposition 7: Somme et produit des racines d'un polynôme scindé

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ un polynôme scindé.
Soient $(x_1, \dots, x_n) \in \mathbb{K}^n$ les racines de P (non nécessairement distinctes), i.e.

$$P = a_n \prod_{k=1}^{n} (X - x_k),$$

où $a_n \neq 0$ est le cœfficient dominant de P.
Alors

$$\sum_{k=1}^{n} x_k = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \prod_{k=1}^{n} x_k = (-1)^n \frac{a_0}{a_n}.$$

Ces formules sont appelées les relations cœfficients-racines (ou formules de Viète).

Démonstration. On a

$$P = \sum_{k=0}^{n} a_k X^k = a_n \prod_{k=1}^{n} (X - x_k) = a_n \left(X^n + \left(-\sum_{k=1}^{n} x_k \right) X^{n-1} + \cdots + (-1)^n \prod_{k=1}^{n} x_k \right).$$

Par unicité des cœfficients d'un polynôme, en identifiant les cœfficients devant X^{n-1} et les cœfficients constants, on obtient

$$\begin{cases} a_{n-1} & = & = -a_n \left(\sum_{k=1}^{n} x_k\right) \\ a_0 & = & (-1)^n a_n \prod_{k=1}^{n} x_k \end{cases}$$

d'où le résultat voulu. ∎

Remarque 17. Si $P = a_n \prod_{k=1}^{p} (X - x_k)^{m_k}$, où les racines $(x_1, \ldots, x_p)$ sont deux à deux disticintes et où m_k est la multiplicité de la racine x_k, alors les résultats précédents deviennent

$$\sum_{k=1}^{p} m_k x_k = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \prod_{k=1}^{p} x_k^{m_k} = (-1)^n \frac{a_0}{a_n}.$$

Exemple 18. • Soit $P = 2X^5 + 2X^4 - 10X^3 - 2X^2 + 16X - 8 = 2(X-1)^3(X+2)^2$.
Alors $3 \times 1 + 2 \times (-2) = -\frac{a_4}{a_5} = -\frac{2}{2} = -1$ et $1^3 \times (-2)^2 = (-1)^5 \frac{a_0}{a_5} = \frac{8}{2} = 4$.
• Soit $n \geqslant 2$. Soit $\omega = e^{\frac{2i\pi}{n}}$.
On sait que $X^n - 1 = \prod_{k=0}^{n-1} (X - \omega^k)$.
D'après les relations précédentes, on retrouve les formules déjà vues dans le chapitre « Nombres complexes » :

$$\sum_{k=0}^{n-1} \omega^k = 0 \quad \text{et} \prod_{k=0}^{n-1} \omega^k = (-1)^n \times (-1) = (-1)^{n-1}.$$

16.2.4 Formule de Taylor polynomiale et conséquences

Proposition 8: Formule de Taylor

Soit $n \in \mathbb{N}$. Soit $P \in \mathbb{K}[X]$ de degré n. Soit $a \in \mathbb{K}$.
Alors

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

où $P^{(k)}$ désigne la dérivée k-ème de P.

Démonstration. Raisonnons par récurrence sur $n = \deg(P)$.
•**Initialisation :** Si $n = 0, P$ est un polynôme constant et on a alors

$$P(X) = P(a) = \sum_{k=0}^{0} \frac{P^{(k)}(a)}{k!} (X-a)^k,$$

donc la propriété est vraie au rang $n = 0$.
•**Hérédité :** Soit $n \in \mathbb{N}$. Supposons la propriété vraie au rang n et montrons-la au rang $n+1$.
Soit $P \in \mathbb{K}[X]$ de degré $n+1$. Alors P' est de degré n donc par hypothèse de récurrence, on a pour tout $t \in \mathbb{R}$,

$$P'(t) = \sum_{k=0}^{n} \frac{P'^{(k)}(a)}{k!} (t-a)^k = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} (t-a)^k.$$

Soit $x \in \mathbb{R}$. En intégrant l'égalité qu'on vient d'obtenir entre a et x, on trouve :

$$\int_a^x P'(t)dt = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} \int_a^x (t-a)^k dt \Leftrightarrow P(x) - P(a) = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!} \left[\frac{(t-a)^{k+1}}{k+1} \right]_a^x$$

d'où $P(x) = P(a) + \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{(k+1)!}(x-a)^{k+1} = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(x-a)^k$. Puisque l'égalité est vraie pour tout $x \in \mathbb{R}$, on en déduit que $P = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(X-a)^k$, ce qui prouve la formule au rang $n+1$ et achève la récurrence. ■

Corollaire 6: Caractérisation de la multiplicité d'une racine

Soit $P \in \mathbb{K}[X]$. Soit $a \in \mathbb{K}$, soit $m \in \mathbb{N}^*$.
Alors a est racine d'ordre m de P si et seulement si $\forall k \in [\![0, m-1]\!], P^{(k)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Démonstration. Raisonnons par double implication.

• Supposons que a est racine d'ordre m de P, i.e. il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$, avec $Q(a) \neq 0$.

Alors $P' = m(X-a)^{m-1}Q + (X-a)^m Q' = (X-a)^{m-1}(mQ + (X-a)Q') = (X-a)^{m-1}R$ avec $R = mQ + (X-a)Q'$.

Puisque $Q(a) \neq 0$, on a $R(a) = mQ(a) \neq 0$ donc a est racine d'ordre $m-1$ de P' (et n'est donc pas racine de P' si $m=1$).

En réitérant le raisonneemnt, on trouve que a est racine d'ordre $m-2$ de P'', d'ordre $m-3$ de $P^{(3)}$ et plus généralement, pour tout $k \in [\![0, m-1]\!], a$ est racine d'ordre $m-k$ de $P^{(k)}$.

Ainsi, a est racine simple de P^{m-1} et n'est donc pas racine de $P^{(m)}$ d'où le résultat.

• Réciproquement, supposons que pour tout $k \in [\![0, m-1]\!], P^{(k)}(a) = 0$ et $P^{(m)}(a) \neq 0$ (ce qui implique que $n \geqslant m$ car $P^{(n+1)} = 0$).

D'après la formule de Taylor établie à la question précédente, on a alors

$$P(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = (X-a)^m \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}.$$

Posons $Q(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}$.

On a alors $P(X) = (X-a)^m Q(X)$ avec $Q(a) = \frac{P^{(m)}(a)}{m!} \neq 0$ par hypothèse.

Par définition, ceci signifie que a est racine de P d'ordre m. ■

Exemple 19. • Soit $P = X^3 - X^2 - X + 1 = (X-1)^2(X+1)$.

On a $P' = 3X^2 - 2X - 1 = 3(X-1)(X+\frac{1}{3})$.

On remarque que puisque 1 est racine double de P, alors 1 est racine simple de P. De même, puisque -1 est racine simple de P, alors -1 n'est pas racine de P'.

En revanche, $-\frac{1}{3}$ est racine de P' mais $-\frac{1}{3}$ n'est pas racine de P.

• Soit $P = X^5 + X^4 - 5X^3 - X^2 + 8X - 4 = (X-1)^3(X+2)^2$. Puisque 1 est racine de P de multiplicité 3 et -2 est racine de P de multiplicité 2, alors $P'(1) = P''(1) = 0, P^{(3)}(1) \neq 0, P'(-2) = 0$ et $P''(-2) \neq 0$.

En effet, $P' = 5X^4 + 4X^3 - 15X^2 - 2X + 8 = (X-1)^2(X+2)(5X+4)$.

Puis $P'' = 20X^3 + 12X^2 - 30X - 2 = (X-1)(20x^2 + 32x + 2)$ et on remarque que $P''(-2) \neq 0$.

Enfin, $P^3 = 60X^2 + 24X - 30$ et on remarque que $P^{(3)}(1) \neq 0$.

16.3 Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

16.3.1 Polynômes irréductibles de $\mathbb{C}[X]$

Théorème 2: Théorème de d'Alembert-Gauss

Tout polynôme de $\mathbb{C}[X]$ non constant admet au moins une racine complexe.

Démonstration. Hors programme. ■

Exemple 20. On sait qu'un polynôme non constant de $\mathbb{R}[X]$ peut ne pas avoir de racine dans $\mathbb{R}$, comme le montre l'exemple de $P = X^2+1$. Mais il admet alors toujours au moins une racine complexe.

Corollaire 7

Tout polynôme de $\mathbb{C}[X]$ non constant est scindé sur $\mathbb{C}$.

Démonstration. Montrons la propriété $P(n)$:≪ Tout polynôme de $\mathbb{C}[X]$ de degré n est scindé sur $\mathbb{C}$ ≫par récurrence sur $n \in \mathbb{N}^*$.

•**Initialisation :** Pour $n = 1$, la propriété est immédiate car tout polynôme de degré 1 est scindé sur $\mathbb{C}$.

•**Hérédité** : Soit $n \in \mathbb{N}^*$ fixé. Supposons la propriété $P(n)$ vraie et montrons que $P(n+1)$ est vraie.

Soit P un polynôme de degré $n+1$. Puisque $n+1 > 0, P$ n'est pas constant donc d'après le théorème de d'Alembert-Gauss, P admet au moins une racine $\alpha \in \mathbb{C}$.

Ainsi, il existe un polynôme Q de degré n tel que $P = (X-\alpha)Q$. Puisque Q est de degré n, d'après l'hypothèse de récurrence, on en déduit que Q est scindé sur $\mathbb{C}$. Il existe donc des scalaires $(x_1, \dots, x_p) \in \mathbb{C}^p$ et des multiplicités $(m_1, \dots, m_p) \in (\mathbb{N}^*)^p$ tels que $Q = a\displaystyle\prod_{k=1}^{p}(X-x_k)^{m_k}$, où a est le cœfficient dominant de Q.

Ainsi, $P = a(X-\alpha)\displaystyle\prod_{k=1}^{p}(X-x_k)^{m_k}$ est scindé sur $\mathbb{C}$, ce qui prouve la propriété au rang $n+1$ et achève la récurrence. ■

Remarque 18. Evidemment, un polynôme non constant de $\mathbb{C}[X]$ n'est pas nécessairement scindé à racines simples, comme le montre l'exemple de $P = (X-i)^2$.

Définition 10: Polynômes irréductibles de $\mathbb{K}[X]$

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.
On dit que P est irréductible sur $\mathbb{K}$ si la propriété suivante est vérifiée :
pour tout couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $P = QR$, alors Q ou R est un polynôme constant non nul.
Autrement dit, P ne peut être divisible que par un polynôme de même degré que P ou par un polynôme constant non nul.

Exemple 21. Le polynôme X^2+1 n'est pas irréductible sur $\mathbb{C}$ car $X^2+1 = (X-i)(X+i)$.

Proposition 9: Polynômes irréductibles de $\mathbb{C}[X]$

Soit $P \in \mathbb{C}[X]$.
Alors P est irréductible sur $\mathbb{C}$ si et seulement si $\deg(P) = 1$.

Démonstration. Soit $P \in \mathbb{C}[X]$ de degré $n \in \mathbb{N}^*$.

• Supposons que $n = 1$. Supposons qu'il existe $(Q, R) \in \mathbb{C}[X]^2$ tel que $P = QR$.

En comparant les degrés, on a $1 = \deg(P) = \deg(Q) + \deg(R)$.

Nécessairement, il vient $\begin{cases} \deg(Q) &= 0 \\ \deg(R) &= 1 \end{cases}$ ou $\begin{cases} \deg(Q) &= 1 \\ \deg(R) &= 0 \end{cases}$, donc l'un des deux polynômes Q ou R est constant, ce qui prouve que P est irréductible sur $\mathbb{C}$.

• Supposons que $n > 1$. D'après le théorème de d'Alembert-Gauss, P admet une racine $a \in \mathbb{C}$ donc il existe un polynôme $Q \in \mathbb{C}[X]$ de degré $n - 1 > 0$ tel que $P = (X - \alpha)Q$. Puisqu'aucun des deux polynômes $X - \alpha$ ou Q n'est constant, on en déduit que P n'est pas irréductible sur $\mathbb{C}$.

Ainsi, P est irréductible si et seulement si $n = \deg(P) = 1$. ■

Théorème 3: Théorème de décomposition en facteurs irréductibles dans $\mathbb{C}[X]$

Soit $P \in \mathbb{C}[X]$ un polynôme non constant.
Alors P est produit de polynômes irréductibles dans $\mathbb{C}[X]$, i.e. il existe des polynômes $(P_1, \ldots, P_n) \in \mathbb{C}[X]^n$ de degré 1 et des entiers $(m_1, \ldots, m_n) \in (\mathbb{N}^*)^n$ tels que

$$P = \prod_{i=1}^{n} P_i^{m_i}.$$

Démonstration. Il s'agit simplement d'utiliser le fait que P est scindé sur $\mathbb{C}$. ■

Remarque 19. Ceci signifie que pour tout polynôme $P \in \mathbb{C}[X]$ non constant, il existe $\lambda \in \mathbb{C}^*$, des nombres complexes $(x_1, \ldots, x_n) \in \mathbb{C}^n$, des entiers non nuls $(m_1, \ldots, m_n) \in (\mathbb{N}^*)^n$ tels que

$$P = \lambda \prod_{i=1}^{n} (X - x_i)^{m_i}.$$

Corollaire 8: Caractérisation de la divisibilité dans $\mathbb{C}[X]$

Soient $(P, Q) \in (\mathbb{C}[X])^2$ non constants.
Notons $Z(P)$ (resp. $Z(Q)$) l'ensemble des racines de P (resp. de Q). Pour chacune des racines α de P (resp. de Q), notons $m_P(\alpha)$ (resp. $m_Q(\alpha)$) la multiplicité de α en tant que racine de P (resp. de Q).
Alors P divise Q si et seulement si $Z(P) \subset Z(Q)$ et pour tout $\alpha \in P, m_P(\alpha) \leqslant m_Q(\alpha)$.

Démonstration. • Supposons que P divise Q. Alors il existe $R \in \mathbb{C}[X]$ tel que $Q = PR$.

▷ Montrons que $Z(P) \subset Z(Q)$.

Soit $\alpha \in Z(P)$. Alors $P(\alpha) = 0$ donc $Q(\alpha) = P(\alpha)R(\alpha) = 0$ donc $\alpha \in Z(Q)$, ce qui prouve que $Z(P) \subset Z(Q)$.

▷ Soit $\alpha \in Z(P) \subset Z(Q)$. Montrons que $m_P(\alpha) \leqslant m_Q(\alpha)$.

Par définition, $(X - \alpha)^{m_P(\alpha)}$ divise P donc il existe $S \in \mathbb{C}[X]$ tel que $P = (X - \alpha)^{m_P(\alpha)} S$, d'où $Q = (X - \alpha)^{m_P(\alpha)} SR$.

Or, par définition $m_Q(\alpha)$ est la plus grande puissance de $(X - \alpha)$ qui divise Q donc $m_P(\alpha) \leqslant m_Q(\alpha)$.

• Réciproquement, supposons que $Z(P) \subset Z(Q)$ et que pour tout $\alpha \in P, m_P(\alpha) \leqslant m_Q(\alpha)$.

Notons $Z(P) = \{\alpha_1, \ldots, \alpha_n\}$.

Alors $P = \lambda \prod_{i=1}^{n} (X - \alpha_i)^{m_P(\alpha_i)}.$, où $\lambda \in \mathbb{C}^*$. Puisque $Z(P) \subset Z(Q)$, il existe un polynôme

$R \in \mathbb{C}[X]$ tel que

$$Q = \prod_{i=1}^{n} (X - \alpha_i)^{m_Q(\alpha_i)} R = \frac{1}{\lambda} \prod_{i=1}^{n} (X - \alpha_i)^{m_Q(\alpha_i) - m_P(\alpha_i)} PR$$

donc P divise Q. ■

16.3.2 Polynômes irréductibles de $\mathbb{R}[X]$

Lemme 2

Soit $P \in \mathbb{R}[X]$. Soit $\alpha \in \mathbb{C}$ une racine de P.
Alors $\overline{\alpha}$ est également une racine de P. De plus, α et $\overline{\alpha}$ ont le même ordre de multiplicité en tant que racines de P.

Démonstration. • Montrons que $P(\overline{\alpha}) = 0$.

Notons $P = \sum_{k=0}^{n} a_k X^k$, où $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{R}^n$. Puisque pour tout $k \in [\![0, n]\!]$, $a_k \in \mathbb{R}$, alors $\overline{a_k} = a_k$. On a alors

$$P(\overline{\alpha}) = \sum_{k=0}^{n} a_k \overline{\alpha}^k = \sum_{k=0}^{n} \overline{a_k} \overline{\alpha^k} = \overline{\sum_{k=0}^{n} a_k \alpha^k} = \overline{P(\alpha)} = \overline{0} = 0.$$

• Notons n la multiplicité de α et m la multiplicité de $\overline{\alpha}$. Montrons que $n = m$.

Supposons par l'absurde que $n \neq m$. Sans perte de généralité, supposons que $n > m$ (l'autre cas étant analogue).

Par caractérisation de la multiplicité d'une racine, on a alors $P^{(m)}(\alpha) = 0$ et $P^{(m)}(\overline{\alpha}) \neq 0$, puisque $n > m$, et que la première dérivée de P qui n'annule pas α est $P^{(n)}$.

Or, $P^{(m)} \in \mathbb{R}[X]$ donc d'après le point précédent, puisque $P^{(m)}(\alpha) = 0$, on a également $P^{(m)}(\overline{\alpha}) = 0$, d'où la contradiction.

Nécessairement, $n = m$. ■

Remarque 20. • On a déjà remarqué ce phénomène dans le chapitre « Nombres complexes »pour des polynômes à cœfficients réels de degré 2, dans le cas où $\Delta < 0$.

• Ce résultat est évidemment faux pour un polynôme à cœfficients dans $\mathbb{C}$. En effet, le polynôme $P = X - i$ admet i comme racine, mais pas $\overline{i} = -i$.

Théorème 4: Polynômes irréductibles de $\mathbb{R}[X]$

Soit $P \in \mathbb{R}[X]$.
Alors P est irréductible sur $\mathbb{R}$ si et seulement si $\deg(P) = 1$ ou $\deg(P) = 2$ avec $\Delta < 0$.

Démonstration. Soit $P \in \mathbb{R}[X]$ de degré $n \in \mathbb{N}^*$.

• Si $n = 1$, la même preuve que sur $\mathbb{C}$ montre que P est irréductible sur $\mathbb{R}$.

• Supposons que $n = 2$ (P est donc un trinôme de second degré) et que $\Delta < 0$. Ainsi P n'admet pas de racine réelle, mais admet deux racines complexes conjuguées. Si P n'était pas irréductible sur $\mathbb{R}$, il existerait deux polynômes Q et R de degré 1 tels que $P = QR$. Or, tout polynôme de degré 1 sur $\mathbb{R}$ admet une racine réelle, donc P aurait une racine réelle, ce qui est absurde. Ainsi, P est bien irréductible sur $\mathbb{R}$.

• Supposons que $n = 2$ et que $\Delta \geqslant 0$. Alors P admet une racine réelle α donc il existe $Q \in \mathbb{R}[X]$ de degré 1 tel que $P = (X - \alpha)Q$ donc P n'est pas irréductible sur $\mathbb{R}$.

• Supposons que $n \geqslant 3$. Il y a deux cas :

▷ Supposons que P admette une racine réelle α. Alors il existe un polynôme $Q \in \mathbb{R}[X]$ de dgré $n-1 \geqslant 2$ tel que $P = (X-\alpha)Q$, donc P n'est pas irréductible sur $\mathbb{R}$.

▷ Supposons que P n'admette pas de racine réelle. D'après le théorème de d'Alembert-Gauss, P admet au moins une racine complexe α. D'après le lemme précédent, $\overline{\alpha}$ est également une racine de P donc P est divisible par $(X-\alpha)(X-\overline{\alpha}) = (X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)$, qui est un polynôme de $\mathbb{R}[X]$ de degré 2. On en déduit qu'il existe un polynôme $Q \in \mathbb{R}[X]$ de degré $n-2 \geqslant 1$ tel que $P = (X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)Q$, donc P n'est pas irrédutible sur $\mathbb{R}$.

Finalement, les seuls polynômes de $\mathbb{R}[X]$ irréductibles sont ceux de degré 1, et ceux de degré 2 de discriminant strictement négatif. ■

Exemple 22. On a vu que X^2+1 n'est pas irréductible sur $\mathbb{C}$, mais il l'est sur $\mathbb{R}$.

Théorème 5: Théorème de décomposition en facteurs irréductibles dans $\mathbb{R}[X]$

Soit $P \in \mathbb{R}[X]$ un polynôme non constant.
Alors P est produit de polynômes irréductibles dans $\mathbb{R}[X]$, i.e. il existe des polynômes $(P_1, \dots, P_n) \in \mathbb{R}[X]^n$ irréductibles et des entiers $(m_1, \dots, m_n) \in (\mathbb{N}^*)^n$ tels que

$$P = \prod_{i=1}^{n} P_i^{m_i}.$$

Démonstration. Utilisons la décomposition en facteurs irréductibles de P dans $\mathbb{C}[X]$.
On obtient une décomposition de la forme

$$P = \lambda \prod_{i=1}^{n} (X - x_i)^{m_i} \prod_{j=1}^{p} (X-\alpha_j)^{m'_j}(X - \overline{\alpha_j})^{m'_j},$$

où λ est le cœfficient dominant de $P, (x_1, \dots, x_n)$ sont les racines réelles de P (de multiplicité $(m_1, \dots, m_n)$ éventuellement nulles si P n'admet pas de racine réelle), et $(\alpha_1, \overline{\alpha}_1, \dots, \alpha_p, \overline{\alpha}_p)$ sont les racines complexes conjuguées deux à deux de P, avec les mêmes multiplicités pour les racines qui sont conjuguées.

On obtient alors $P = \lambda \prod_{i=1}^{n} (X-x_i)^{m_i} \prod_{j=1}^{p} (X - 2\mathrm{Re}(\alpha_j)X + |\alpha_j|^2)^{m'_j}$. Tous les polynômes de degré 1 apparaissant dans ce produit sont bien évidemment irréductibles, et ceux de degré 2 également puisqu'ils sont de discriminant strictement négatif, d'où le résultat.

■

Remarque 21. En pratique, la décomposition en facteurs irréductibles de $P \in \mathbb{R}[X]$ s'écrit sous la forme

$$P = \prod_{i=1}^{n} (X-x_i)^{m_i} \prod_{j=1}^{p} (a_j X^2 + b_j X + c_j)^{m'_j},$$

où les polynômes $(a_j X^2 + b_j X + c_j)^{m'_j}$ sont de discriminant strictement négatif.

Exemple 23. Donnons la décomposition en facteurs irréductibles de X^4+1 dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.
Sur $\mathbb{C}$, on a $x^4 + 1 = 0 \Leftrightarrow (x^2)^2 = -1 = i^2 \Leftrightarrow x^2 = i = e^{i\frac{\pi}{2}}$ ou $x^2 = -i = e^{3i\frac{\pi}{2}}$ d'où

$$X^4 + 1 = (X - e^{i\frac{\pi}{4}})(X - e^{\frac{5i\pi}{4}})(X - e^{\frac{3i\pi}{4}})(X - e^{\frac{7i\pi}{4}}).$$

Pour obtenir la décomposition dans $\mathbb{R}$, on multiplie entre eux les termes conjugués deux à deux.

En effet, on a $\overline{e^{i\frac{\pi}{4}}} = e^{-i\frac{\pi}{4}} = e^{\frac{7i\pi}{4}}$ et $\overline{e^{3i\frac{\pi}{4}}} = e^{\frac{-3i\pi}{4}} = e^{\frac{5i\pi}{4}}$ d'où

$$\begin{aligned}
X^4+1 &= (X-e^{i\frac{\pi}{4}})(X-\overline{e^{i\frac{\pi}{4}}})(X-e^{\frac{3i\pi}{4}})(X-\overline{e^{\frac{3i\pi}{4}}}) \\
&= (X^2-(e^{i\frac{\pi}{4}}+e^{-i\frac{\pi}{4}})X+1)((X^2-(e^{\frac{3i\pi}{4}}+e^{\frac{-3i\pi}{4}})X+1) \\
&= (X^2-2\cos\left(\frac{\pi}{4}\right)X+1)(X^2-\cos\left(\frac{3\pi}{4}\right)X+1) \\
&= (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).
\end{aligned}$$

16.4 Décomposition en éléments simples de certaines fonctions rationnelles

Définition 11: Fonctions rationnelles

On appelle fraction rationnelle toute fonction de la forme $x \mapsto \frac{P(x)}{Q(x)}$, où P et Q sont des polynômes de $\mathbb{K}[X]$, avec $Q \neq 0$.

Remarque 22. Une telle fonction est définie pour les x tels que $Q(x) \neq 0$.

Théorème 6: Décomposition en éléments simples des fonctions rationnelles à pôles simples

Soit $F : x \mapsto \frac{P(x)}{Q(x)}$, où $P \in \mathbb{K}[X]$ et $Q = \prod_{i=1}^{n}(X-x_i) \in \mathbb{K}[X]$ est un polynôme scindé à racines simples (les $(x_1,\dots,x_n)$ sont appelés les pôles simples de F).
Alors il existe $T \in \mathbb{K}[X]$ et des scalaires $(a_1,\dots,a_n) \in \mathbb{K}^n$ tels que

$$\forall x \in \mathbb{K} \setminus \{x_1,\dots,x_n\}, F(x) = T(x) + \sum_{i=1}^{n} \frac{a_i}{X-x_i}.$$

Démonstration. Hors-programme. ∎

Remarque 23. • En pratique, on commence par faire la division euclidienne $P = QT + R$, où $\deg(R) < \deg(Q)$ et on a $\frac{P}{Q} = T + \frac{R}{Q}$. Ainsi, T est le quotient de la division euclidienne de P par Q. Les scalaires $(a_1,\dots,a_n)$ se trouvent ensuite par identification.

• Ceci est très utile en pratique pour calculer des intégrales, ou pour calculer des dérivées.

Exemple 24. Posons pour tout $t \in \mathbb{R} \setminus \{1,-3\}, F(t) = \frac{t^3+3t^2+4}{t^2+2t-3} = \frac{t^3+3t^2+4}{(t-1)(t+3)}$.

La division euclidienne de X^3+3X^2+4 par X^2+2X-3 est

$$X^3+3X^2+4 = (X^2+2X-3)(X+1)+X+7$$

donc pour tout $t \in \mathbb{R} \setminus \{1,-3\}, F(t) = t+1+\frac{t-7}{(t-1)(t+3)}$.

Pour tout $t \in \mathbb{R} \setminus \{1,-3\}$, on a

$$\frac{t+7}{t^2+2t-3} = \frac{a}{t-1} + \frac{b}{t+3} \Leftrightarrow \frac{t+7}{t^2+2t-3} = \frac{(a+b)t+3a-b}{t^2+2t-3} \Leftrightarrow t+7 = (a+b)t+3a-b.$$

Par identification, on en déduit

$$\left\{\begin{array}{rcl} a+b & = & 1 \\ 3a-b & = & 7 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} a & = & 2 \\ b & = & -1 \end{array}\right. .$$

Ainsi, pour tout $t \in \mathbb{R} \setminus \{1,-3\}, F(t) = t+1+\dfrac{2}{t-1}-\dfrac{1}{t+3}$.

On a alors

$$\int_{-2}^{0} F(t) = \int_{-2}^{0} \left(t+1+\frac{2}{t-1}-\frac{1}{t+3}\right) dt.$$

Par linéarité de l'intégrale, on en déduit

$$\begin{array}{rcl} \displaystyle\int_{-2}^{0} F(t) & = & \displaystyle\int_{-2}^{0}(t+1)dt + 2\int_{-2}^{0}\frac{dt}{t-1} - \int_{-2}^{0}\frac{dt}{t+3} \\ & = & \displaystyle\left[\frac{t^2}{2}+t\right]_{-2}^{0} + 2[\ln(|t-1|)]_{-2}^{0} - [\ln(|t+3|)]_{-2}^{0} \\ & = & -3\ln(3). \end{array}$$