Polynômes

Dans tout le chapitre, $\mathbb{K}$ désignera l'un des ensembles $\mathbb{R}$ ou $\mathbb{C}$.

1. Généralités

1.1. Unicité de l'écriture polynomiale

a) **Théorème :** soient $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ avec $(a_0, a_1, \ldots, a_n) \in \mathbb{K}^{n+1}$. Alors :

$$\boxed{(\forall x \in \mathbb{K},\ P(x) = 0) \iff a_n = a_{n-1} = \ldots = a_0 = 0.}$$

Autrement dit, **une fonction polynômiale est nulle si et seulement si ses coefficients sont nuls**.

b) **Principe d'identification des coefficients :** on considère $P(x) = \sum\limits_{k=0}^{n} a_k x^k$ et $Q(x) = \sum\limits_{k=0}^{m} b_k x^k$,
avec $(a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$, $(b_0, \ldots b_m) \in \mathbb{K}^{m+1}$, $a_n \neq 0$, et $b_m \neq 0$. Alors :

$$\boxed{(\forall x \in \mathbb{K},\ P(x) = Q(x)) \Leftrightarrow \begin{cases} n = m \\ \forall k \in [[0, n]],\ a_k = b_k \end{cases}}$$

c) **Moralité :** une fonction polynomiale est entièrement déterminée par son degré n et la suite ("presque nulle") de ses coefficients $a_0, a_1, \ldots, a_n, \ldots$, en convenant que $a_k = 0$ pour $k > n$.
Nous allons donc pouvoir travailler avec des polynômes **formels**, sans se préoccuper de la variable.

1.2. Définitions

a) **Ecriture générale :** on appelle **polynôme** (formel) à coefficients dans $\mathbb{K}$ une expression P de la forme :

$$\boxed{P = \sum_{k=0}^{+\infty} a_k X^k} \quad \text{(on note indifféremment } P \text{ ou } P(X)\text{)}$$

où (a_n) est une suite d'éléments de $\mathbb{K}$ **nulle à partir d'un certain rang**, et appelée suite des **coefficients** de P.
Cette écriture est unique, et permet donc l'identification des coefficients.
Si tous les coefficients sont nuls, $P = 0$ est appelé **polynôme nul**.

> ***Remarque :*** X est appelée **indéterminée**. Ce n'est pas un nombre, mais un polynôme (un **monôme**).
> On ne peut donc pas écrire "$X = 2$". (cela entrainerait $1 = 0$ et $0 = 2$ par identification!!)
> L'expression "$\forall X$" n'a **aucun sens**.

b) **Ecriture courante :** si $P = \sum\limits_{k=0}^{\infty} a_k X^k$ est un polynôme **non nul**, on note

$$\boxed{\deg P = \max\{k \in \mathbb{N} \ / \ a_k \neq 0\}} \text{ et par convention } \boxed{\deg 0 = -\infty}$$

Alors, si P est **non nul**, P s'écrit ainsi **de manière unique**, en notant $n = \deg P$:

$$\boxed{P = \sum_{k=0}^{n} a_k X^k = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0} \quad \text{avec } \begin{cases} n \in \mathbb{N} \\ (a_0, \ldots, a_n) \in \mathbb{K}^{n+1} \\ \boxed{a_n \neq 0} \end{cases}$$

> ***Attention :*** pour affirmer que $\sum\limits_{k=0}^{n} a_k X^k$ est de degré n, il faut s'assurer que $\boxed{a_n \neq 0}$

c) <u>Vocabulaire</u> :

- $\boxed{\text{On note } \mathbb{K}|X] \text{ l'ensemble des polynômes à coefficients dans } \mathbb{K}.}$
- $\boxed{\text{On note } \mathbb{K}_n\left[X\right] \text{ l'ensemble des polynômes de degré } \textbf{inférieur ou égal} \text{ à } n}$
- Si $\deg P = n \geqslant 0,\ a_n$ est appelé **coefficient de plus haut degré**, ou **coefficient dominant**.
- Si le coefficient dominant de P vaut 1, on dit que P est **unitaire**.
- a_0 est appelé **coefficient constant** de P.
- si $\deg P = 0$, on dit que P est un **polynôme constant**.
- si $P \in \mathbb{K}\left[X\right]$ et $\lambda \in \mathbb{K}^*$, le polynôme λP est dit **associé** à P.
  Il a même degré et mêmes racines que P

Remarque 1 : un polynôme P est non nul si et seulement si $\deg P \geqslant 0$

Remarque 2 : si a_n est le coefficient dominant de P, alors $\frac{1}{a_n}P$ est unitaire et associé à P.

Exemple : si $(a,b) \in \mathbb{K}^2,\ a \neq 0$ et $\lambda = -\frac{b}{a}$ alors $P = aX + b$ et $Q = X - \lambda$ sont associés.

1.3. Opérations sur les polynômes

Soient deux polynômes de degré n et m à coefficients dans $\mathbb{K}$:

$$P = \sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{+\infty} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{m} b_k X^k = \sum_{k=0}^{+\infty} b_k X^k$$

a) <u>Somme</u> : $P + Q$ est un polynôme de $\mathbb{K}\left[X\right]$ d'expression: $\boxed{P + Q = \sum_{k=0}^{+\infty} \left(a_k + b_k\right) X^k}$

On voit alors que

$$\boxed{\deg\left(P + Q\right) \leqslant \max\left(\deg P, \deg Q\right)}$$

Plus spécialement,

$$\boxed{\text{si } \deg Q < \deg P, \text{ alors } \deg\left(P + Q\right) = \deg P}$$

b) <u>Produit</u> : PQ est le polynôme de $\mathbb{K}\left[X\right]$ d'expression : $\quad PQ = \sum_{k=0}^{+\infty} d_k X^k, \quad$ avec

$$\boxed{\forall k \in \mathbb{N},\ d_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}}$$

En particulier, on a

$$\boxed{d_0 = a_0 b_0}, \quad \boxed{d_1 = a_1 b_0 + a_0 b_1} \quad \text{et} \quad \boxed{d_{n+m} = a_n b_m \neq 0}$$

De plus, si $k > m + n$, on voit que $d_k = 0$, de sorte que

$$P\left(X\right) Q\left(X\right) = a_n b_m X^{n+m} + \cdots + \left(a_1 b_0 + a_0 b_1\right) X + a_0 b_0$$

On en déduit

$$\boxed{\deg\left(PQ\right) = \deg P + \deg Q}$$

Conséquence : $\forall \left(P, Q\right) \in \mathbb{K}\left[X\right]^2$, on a : $\boxed{PQ = 0 \Longleftrightarrow \left(P = 0 \text{ ou } Q = 0\right)}$

Remarque : si $P \neq 0$, alors $\boxed{PQ = PR \Longleftrightarrow Q = R}$

1.4. Dérivation

a) Définition : si $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, sa dérivée est le polynôme $P' = D(P)$ d'expression :

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

On vérifie alors les propriétés suivantes, valables pour tous polynômes P et Q (et $(\lambda, \mu) \in \mathbb{K}^2$)

- $\boxed{(\lambda P + \mu Q)' = \lambda P' + \mu Q' \quad ; \quad (PQ)' = PQ' + P'Q}$
- $\boxed{\text{Si } \deg P \geqslant 1, \text{ alors } \deg(P') = \deg P - 1. \text{ Sinon } \quad P' = 0}$

Conséquence : $\boxed{P' = 0 \Leftrightarrow P \text{ est un polynôme constant}}$.

b) Dérivées d'ordre supérieur : on note $D^k(P)$ ou $P^{(k)}$ la dérivée k-ième de P, avec $D^0(P) = P^{(0)} = P$.

(i) Degré :

$$\boxed{\text{Si } \deg P = n \geqslant 0 \text{ , alors } \begin{cases} \text{si } k > n, & P^{(k)} = 0 \\ \text{si } k \leqslant n & \deg P^{(k)} = n - k \end{cases}}$$

(ii) Dérivées de X^n : soit $n \geqslant 0$ on a

$$D(X^n) = nX^{n-1} \quad ; \quad D^2(X^n) = n(n-1)X^{n-2} \ldots$$

$$\boxed{\begin{array}{ll} \text{Si } k \leqslant n, & D^k(X^n) = n(n-1)\ldots(n-k+1)\, X^{n-k} = \dfrac{n!}{(n-k)!} X^{n-k} \\ \text{Si } k > n, & D^k(X^n) = 0 \end{array}}$$

Remarque : on a en fait la formule vraie pour tout entier k :

$$\boxed{D^k(X^n) = k! \binom{n}{k} X^{n-k}}$$

Cas particulier : $\boxed{D^n(X^n) = n!}$

Généralisation : $\forall a \in \mathbb{K}, \ \forall k \in \mathbb{N}$,

$$\boxed{D^k\left((X-a)^n\right) = k! \binom{n}{k} (X-a)^{n-k}}$$

c) Formule de Taylor :

(i) Formule en 0 : soit $P = \sum_{k=0}^{\infty} a_k X^k$ un polynôme. Alors $\forall k \in \mathbb{N}$, $\boxed{a_k = \dfrac{P^{(k)}(0)}{k!}}$

Autrement dit, le polynôme P s'écrit

$$\boxed{P = \sum_{k=0}^{\infty} \frac{P^{(k)}(0)}{k!} X^k} \quad \text{ou si} \quad \deg P = n, \boxed{P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k}$$

(ii) Formule en $a \in \mathbb{K}$ quelconque :

Tout polynôme $P \in \mathbb{K}[X]$ se décompose en combinaison linéaire des puissances de $X - a$:

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

où $n = \deg P$. **Cette décomposition est unique**.

1.5. Substitution

a) **Fonction polynomiale associée à un polynôme :** si $P = \sum\limits_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, et $\lambda \in \mathbb{K}$, on pose

$$P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k \in \mathbb{K}$$

On dit qu'on a **substitué** le scalaire λ à l'indéterminée X.

On peut alors définir la **fonction polynomiale** $\widetilde{P} : \mathbb{K} \to \mathbb{K}$ **associée à** P par $\widetilde{P}(x) = P(x)$.

Par abus, on la note encore P, et l'étude faite au 1.1.montre qu'il revient au même de donner la fonction $\widetilde{P}$ et le polynôme P.

Remarque 1 : $\mathbb{R}[X] \subset \mathbb{C}[X]$: si P est un polynôme **réel**, on peut considérer $P : \mathbb{C} \to \mathbb{C}$.

Remarque 2 : la dérivée d'une fonction polynomiale complexe est purement formelle ici.

Remarque 3 : égalité de deux polynômes : $P = Q \iff \forall x \in \mathbb{K},\ P(x) = Q(x)$

b) **Racines-équations :**

- On dit que $a \in \mathbb{K}$ est **racine** de P (ou **zéro** de P) lorsque $P(a) = 0$.
- On appelle **équation algébrique** sur $\mathbb{K}$ toute équation (E) pouvant s'écrire

$$P(x) = 0$$

où P est un polynôme de $\mathbb{K}|X]$. Les **solutions** de (E) sont donc les **racines** de P.

2. Divisibilité dans $\mathbb{K}[X]$

2.1. Factorisation

a) **Définition :** soient P et Q deux polynômes de $\mathbb{K}[X]$. On dit que Q **divise** P lorsque

$$\exists R \in \mathbb{K}[X]\ /\ P = QR$$

On dit aussi que P **est divisible** par Q ou que P **est factorisable** par Q.

Exemple 1 : $X^2 + 1$ divise $X^4 - 1$

Exemple 2 : $\forall a \in \mathbb{K}, \forall n \in \mathbb{N}$, $X - a$ divise $X^n - a^n$

Remarque : **tout** polynôme divise 0, et 0 ne divise **aucun** polynôme non nul.

b) **Propriétés :**

(i) Si Q divise P et $P \neq 0$, alors $\deg Q \leqslant \deg P$.

(ii) Si Q divise $P_1, P_2, \ldots, P_n$, alors Q divise $\lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_n P_n$. (les λ_i dans $\mathbb{K}$)

(iii) Application : $\boxed{\forall a \in \mathbb{K},\ X - a \text{ divise } P - P(a)}$

(iv) **Conséquence fondamentale** : $\boxed{\text{si } a \text{ est racine de} P \text{, si et seulement si } X - a \text{ divise } P(X)}$

c) **Polynômes irréductibles :** soit $P \in \mathbb{K}[X]$ un polynôme non constant.

On dit que P est **irréductible sur** $\mathbb{K}$ s'il n'est divisible que par ses associés et les polynômes constants.

Cela revient à dire que si P se décompose en $P = QR$, alors Q est constant ou R est constant.

Exemple 1 : les polynômes de degré 1 sur $\mathbb{K}$ sont irréductibles sur $\mathbb{K}$

Exemple 2 : les polynômes de degré 2 sur $\mathbb{R}$ à discriminant négatif sont irréductibles sur $\mathbb{R}$, mais ne sont pas irréductibles sur $\mathbb{C}$.

2.2. Division euclidienne dans $\mathbb{K}[X]$

a) <u>**Théorème**</u> **:** soient A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$:

$$\boxed{\exists!\,(Q,R) \in \mathbb{K}[X]^2 \text{ tels que } \quad A = BQ + R \quad \textbf{et} \quad \deg R < \deg B}$$

Q est appelé **quotient** et R est appelé **reste** de la division euclidienne de A par B.

Exemple 1 : division euclidienne de $2X^5 - 4X^3 + 3X^2 - X + 2$ par $X^2 - X + 1$.

$$\begin{array}{r|l}
\boxed{A =}\, 2X^5 \qquad - 4X^3 + 3X^2 + X + 2 & X^2 - X + 1\, \boxed{= B} \\ \hline
2X^4 - 6X^3 + 3X^2 + X + 2 & 2X^3 + 2X^2 - 4X - 3\, \boxed{= Q} \\
-4X^3 - 8X^2 + X + 2 & \\
-12X^2 + 5X + 2 & \\
\boxed{R =}\, 2X + 5 &
\end{array}$$

Ainsi

$$2X^5 - 4X^3 + 3X^2 - X + 2 = \left(X^2 - X + 1\right)\left(2X^3 + 2X^2 - 4X - 3\right) + 2X + 5$$

Exemple 2 : division euclidienne de $A = 4X^3 + X^2$ par $B = X + (1 + i)$

b) <u>**Lien avec la divisibilité**</u> **:** $\boxed{B \text{ divise } A \text{ si et seulement si le reste de la division euclidienne de } A \text{ par } B \text{ est } 0}$

Exemple : $X^2 + X + 1$ divise $X^5 + X^3 - X^2 - 1$

c) <u>**Recherche du reste**</u> **:** (sans connaitre le quotient)

Exemple 1 : soit $P = (X - 3)^{2n} + (X - 2)^n - 2 \quad (n \geqslant 2)$.

Déterminer le reste de la division euclidienne de P par $X^2 - 5X + 6$, puis par $X^2 - 4X + 4$

Exemple 2 : $\boxed{\text{Le reste de la division de } P \text{ par } X - a \text{ est le polynôme constant } P(a)}$

3. Racines et divisibilité

3.1. Factorisation par $X - a$

a) <u>**Rappel**</u> **:** $\boxed{\text{soit } P \in \mathbb{K}[X] \text{ et } a \in \mathbb{K}. \text{ Alors } a \text{ est racine de } P \text{ si et seulement si } X - a \text{ divise } P}$

Exemple : 2 est racine de $P = X^3 - 8X^2 + 13X - 2$. Factoriser P (deux méthodes).

b) <u>**Généralisation**</u> **:**

$$\boxed{a_1, \dots, a_m \text{ sont racines } \textbf{distinctes} \text{ de } P \text{ si et seulement si } (X - a_1) \dots (X - a_m) \text{ divise } P.}$$

Exemple 1 : soit $P = X^5 - X^4 - 2X^3 - X^2 + X + 2$.
En remarquant que $1, -1, 2$ sont racines de P, factoriser P.

Remarque : les factorisations successives sont beaucoup plus inefficaces.

Exemple 2 : montrer que j et j^2 sont racines de $P = X^5 + 3X^4 + 3X^3 - X^2 - 3X - 3$

c) <u>**Annulation des fonctions polynômes**</u> **:**

$$\boxed{\text{un polynôme de degré } n \geqslant 1 \text{ ne peut avoir plus de } n \text{ racines distinctes.}}$$

ou par contraposée :

$$\boxed{\text{si } \deg P \leqslant n \text{ et si } P \text{ s'annule en au moins } n+1 \text{ points, alors } P \text{ est le polynôme nul.}}$$

Exemple 1 : déterminer tous les polynômes P de $\mathbb{K}[X]$ vérifiant : $P(X+1) \overset{(*)}{=} P(X)$.

Cas particuliers : on peut affirmer que le polynôme P est le polynôme nul lorsque :

- P s'annule sur $\mathbb{K}$ sauf un nombre fini de points
- P s'annule sur un intervalle $[a, b]$ non réduit à un point.
- P s'annule sur $\mathbb{N}$.
- P (complexe) s'annule sur $\mathbb{R}$.

Cas d'égalités : on peut affirmer que $P = Q$ lorsque :

- $P(x) = Q(x)$ pour tout $x \in \mathbb{K}$ sauf un nombre fini de points
- $P(x) = Q(x)$ pour tout $x \in [a, b]$ non trivial.
- $P(x) = Q(x)$ pour tout $x \in \mathbb{N}$.
- $P(x) = Q(x)$ pour tout $x \in \mathbb{R}$ (P et Q complexes).

Il suffit en effet d'appliquer les résultats précédents à $R = P - Q$.

Exemple 2 : unicité du n-ième polynôme de Tchébychev :

On rappelle que si $n \in \mathbb{N}$, il existe un polynôme T_n vérifiant $\forall \theta \in \mathbb{R},\ T_n(\cos \theta) = \cos(n\theta)$

Montrer que T_n est unique.

Exemple 3 : trouver a, b, c réels tels ue $\forall x \in \mathbb{R} \backslash \{-1, 0, 1\}$, $\dfrac{1}{x^3 - x} = \dfrac{a}{x} + \dfrac{b}{x-1} + \dfrac{c}{x+1}$

3.2. Racines multiples

a) **Définition :** soit $P \in$, $k \in \mathbb{N}^*$, et $a \in \mathbb{K}$.

$$\boxed{\text{on dit que } a \text{ est } \textbf{racine d'ordre } k \textbf{ de } P \text{ lorsque } \begin{cases} (X-a)^k \text{ divise } P \\ (X-a)^{k+1} \text{ ne divise pas } P \end{cases}}$$

k est appelé **ordre de multiplicité** de la racine a. Cette définition revient à :

$$\boxed{a \text{ est racine d'ordre } k \text{ de } P \text{ si et seulement si } \exists Q \in \mathbb{K}[X] \ / \ P = (X-a)^k Q, \textbf{ et } Q(a) \neq 0}$$

Exemple : montrer que 1 est racine d'ordre 3 de $P = X^6 - 6X^5 + 9X^4 - 5X^3 + 6X^2 - 9X + 4$

b) **Généralisation :**

$$\boxed{\text{si } a_1, \ldots, a_p \textbf{ distincts} \text{ sont racines d'ordre au moins } k_1, \ldots, k_p \text{ de } P, \text{ alors } (X-a_1)^{k_1} \ldots (X-a_p)^{k_p} \text{ divise } P.}$$

c) **Caractérisation par les dérivées :**

$$\boxed{a \text{ est racine d'ordre } k \text{ de } P \Longleftrightarrow \begin{cases} P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}}$$

Exemple : montrer que 1 est racine d'ordre 3 de $P = X^6 - 6X^5 + 9X^4 - 5X^3 + 6X^2 - 9X + 4$

4. Décomposition des polynômes

4.1. Polynômes scindés

a) **Définition :** soit $P \in \mathbb{K}[X]$ un polynôme non constant.
On dit que Pest **scindé sur** $\mathbb{K}$ lorsqu'on peut le décomposer en produit de facteurs du premier degré sur $\mathbb{K}$, autrement dit si P s'écrit sous la forme :

$$\boxed{P = \lambda (X - \alpha_1) \ldots (X - \alpha_n) = \lambda \prod_{k=1}^{n} (X - \alpha_k)} \quad \text{avec } (\lambda, \alpha_1, \ldots, \alpha_n) \in \mathbb{K}^{n+1}.$$

λ est alors nécessairement le coefficient dominant de P, n son degré,
et $\alpha_1, \ldots, \alpha_n$ ses racines comptées avec leur ordre de multiplicité (une racine d'ordre k apparait k fois).
Cette décomposition est donc unique à l'ordre des facteurs près (on dit **essentiellement unique**).

Exemple 1 : $P = X^3 - 1$ est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

Exemple 2 : $Q = 3X^4 + 6X^2 + 3$ est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.

b) **Autre forme :** comme dans ce dernier exemple, en regroupant les racines identiques, la décomposition d'un polynôme scindé s'écrit aussi (de manière essentiellement unique)

$$\boxed{P = \lambda (X - \alpha_1)^{k_1} \ldots (X - \alpha_m)^{k_m} = \lambda \prod_{i=1}^{m} (X - \alpha_i)^{k_i}}$$

où $\alpha_1, \ldots, \alpha_m$ sont cette fois les racines distinctes de P, d'ordre de multiplicité $k_1, \ldots, k_m$. On a $\sum\limits_{k=1}^{m} k_i = n$

4.2. Décompositions dans $\mathbb{C}[X]$

a) **Théorème de d'Alembert-Gauss :** $\boxed{\text{tout polynôme } \textbf{non constant} \text{ de } \mathbb{C}[X] \text{ admet (au moins) une racine}}$ (admis)

b) **Conséquence :** $\boxed{\text{tout polynôme non constant de } \mathbb{C}[X] \text{ est scindé sur } \mathbb{C}.}$ (récurrence sur $n = \deg P$)

c) **Lecture arithmétique :** le théorème de d'Alembert-Gauss entraine :

1. $\boxed{\text{Les seuls polynômes irréductibles de } \mathbb{C}[X] \text{ sont les polynômes de degré } 1}$

2. Tout polynôme complexe non constant se décompose de manière essentiellement unique en produit de polynômes irréductibles sur $\mathbb{C}[X]$

d) **Décompositions classiques :**

(i) A retenir dans les deux sens : $\boxed{X^2 - 2\cos(\theta) X + 1 = \left(X - e^{i\theta}\right)\left(X - e^{-i\theta}\right)}$

(ii) Racines de l'unité (1) : pour $n \in \mathbb{N}^*$,

$$\boxed{X^n - 1 = (X - 1)\left(X - e^{\frac{2i\pi}{n}}\right) \ldots \left(X - e^{\frac{2i(n-1)\pi}{n}}\right)} \quad \text{soit}$$

$$\boxed{X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{2ik\pi/n}\right) = \prod_{k=0}^{n-1} \left(X - \omega^k\right)} \quad \text{avec } \omega = e^{2i\pi/n}$$

Exemples : factoriser $X^2 - 1$, $X^3 - 1$, $X^4 - 1$ et $X^5 - 1$

- Racines de l'unité (2) : pour $n \geqslant 2$, $\boxed{X^{n-1} + X^{n-2} + \cdots + X^2 + X + 1 = \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right)}$

  Exemples : factoriser $X^2 + X + 1$, $X^3 + X^2 + X + 1$ et $X^4 + X^3 + X^2 + X + 1$

4.3. Décompositions dans $\mathbb{R}[X]$

Les polynômes réels sont scindés sur $\mathbb{C}$, mais on va montrer qu'ils se décomposent en produits de polynômes **réels** de degré 1 de degré 2 de discriminant strictement positif (on dira **irréductibles** sur $\mathbb{R}$).

a) **Racines conjuguées :** Si $a \in \mathbb{C}\backslash\mathbb{R}$ est racine d'ordre k de $P \in \mathbb{R}[X]$, alors $\bar{a}$ est racine d'ordre k de P

b) **Regroupements de termes :** Si $a \in \mathbb{C}\backslash\mathbb{R}$, alors $(X - a)(X - \bar{a}) = X^2 + pX + q$, avec $\begin{cases} (p, q) \in \mathbb{R}^2 \text{ et} \\ p^2 - 4q < 0 \end{cases}$

Plus précisément

$$(X - a)(X - \bar{a}) = X^2 - (a + \bar{a}) X + a\bar{a} = X^2 - 2\,\mathrm{Re}(a)\, X + |a|^2$$

Le discriminant est strictement négatif, sinon ce trinôme aurait deux racines réelles. le polynôme est donc irréductible sur $\mathbb{R}$

c) **Décomposition en produit d'irréductibles :**

Tout polynôme réel non constant se décompose en produit de polynômes réels de degré 1 et de polynômes réels de degré 2 à discriminant strictement négatif

Autrement dit, $P \in \mathbb{R}[X]$ non constant s'écrit

$$\boxed{P = \lambda (X - a_1)^{k_1} \cdots (X - a_s)^{k_s} \left(X^2 + p_1 X + q_1\right)^{m_1} \cdots \left(X^2 + p_r X + q_r\right)^{m_r}}$$

Où $a_1, \ldots, a_s, p_1, \ldots, p_r, q_1, \ldots, q_r$ sont des réels, $k_1, \ldots, k_s, m_1, \ldots, m_r$ des entiers $\geqslant 1$, vérifiant :

- λ est le coefficient dominant de P
- $a_1, \ldots, a_s$ sont les racines réelles distinctes de P d'ordre $k_1, \ldots, k_s$
- $\forall i \in [[1, r]]$, $p_i^2 - 4q_i < 0$
- $k_1 + \cdots + k_s + 2(m_1 + \cdots + m_r) = \deg P$

Cette décomposition est unique à l'ordre des facteurs près.

d) **Lecture arithmétique :** on a ainsi

1. Les seuls polynômes irréductibles de $\mathbb{R}[X]$ sont $\begin{cases} \text{les polynômes réels de degré 1} \\ \text{les polynômes réels de degré 2 irréductibles} \end{cases}$

2. Tout polynôme réel non constant se décompose de manière essentiellement unique en produit de polynômes irréductibles sur $\mathbb{R}[X]$

e) **Exemples de factorisations sur $\mathbb{R}$:**

Exemple 1 : factoriser $P = X^7 + 27X^4 - X^3 - 27$ sur $\mathbb{R}[X]$

Exemple 2 : factoriser $P = X^4 + 1$ et $Q = X^4 + X^2 + 1$ sur $\mathbb{R}[X]$ en passant par les complexes, puis directement.

Exemple 3 : factoriser $P = X^5 - 1$ sur $\mathbb{R}[X]$

4.4. Application : somme et produit des racines

Exemple : développer les polynômes $(X-\alpha)(X-\beta)\,,\ (X-\alpha)(X-\beta)(X-\gamma)$
et $(X-\alpha)(X-\beta)(X-\gamma)(X-\delta)$

Théorème : soit $P=\sum_{k=0}^{n}a_kX^k$ un polynôme de degré $n\geqslant 1$ et $\alpha_1,\ldots,\alpha_n$ ses racines complexes, comptées avec leur ordre de multiplicité. On note

$$\begin{cases}\sigma=a_1+\cdots+a_n \text{ la somme des racines}\\ \pi=a_1\cdots a_n \text{ le produit des racines}\end{cases}$$

Alors

$$\boxed{\begin{cases}\sigma=-\dfrac{a_{n-1}}{a_0}\\[2ex] \pi=(-1)^n\,\dfrac{a_0}{a_n}\end{cases}}$$

Remarque : si P est unitaire, $\sigma=-a_{n-1}$ et $\pi=(-1)^n\,a_0$.

Exemple 1 : somme et produit des racines de aX^2+bX+c, puis de aX^3+bX^2+cX+d.

Exemple 2 : soit $P=(X+1)^n-X^n \quad (n\geqslant 2)$ .Calculer la somme et le produit de ses racines complexes