Chapitre
Polynômes

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

I Polynômes à une indéterminée

I.1 Définitions

Définition (Polynômes)

- On appelle **polynôme à une indéterminée à coefficients dans** $\mathbb{K}$ tout objet de la forme

$$P = \sum_{k=0}^{n} a_k X^k = a_0 + a_1 X + \cdots + a_n X^n \qquad \text{où } (a_0, \cdots, a_n) \in \mathbb{K}^n.$$

  X est un objet formel appelé **indéterminé**.
  L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.

- On appelle **polynôme nul** le polynome pour lequel tous les coefficients son nuls. Il est noté $0_{\mathbb{K}[X]}$ ou plus simplement 0.

- Si $P \neq 0_{\mathbb{K}[X]}$, on appelle **degré** de P et on note $\deg P$ le plus grand entier k pour lequel $a_k \neq 0$.
  Par convention $\deg 0_{\mathbb{K}[X]} = -\infty$.

- Si $P \neq 0_{\mathbb{K}[X]}$, on appelle **valuation** de P et on note val$P$ le plus petit entier k pour lequel $a_k \neq 0$.

- Le coefficient de degré $\deg P$ est appelé **coefficient dominant de** P et est noté $\mathrm{CD}(P)$.
  Si ce coefficient est 1, le polynôme P est dit **unitaire**.

- Pour $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré **inférieur ou égal** à n.

- On appelle monôme un polynôme de la forme $a_n X^n$ où $a_n \in \mathbb{K}$.
  En particulier, on appelle polynôme constant les polynômes de la forme $a_0 X^0$ où $a_0 \in \mathbb{K}$. On note souvent a_0 ce polynôme.

Remarques (Définition officielle, hors-programme.)

Un polynôme à une indéterminée à coefficients dans $\mathbb{K}$ est une suite $(a_0, a_1, a_2, ...) = (a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ **tous nuls à partir d'un certain rang**.
L'indéterminée X est la suite $(0, 1, 0, 0, ...)$ et X^0 est la suite $(1, 0, 0, ...)$ On ne remplace donc pas X par une valeur comme on pourrait le faire dans une fonction polynomiale.

Remarques (Notation)

1) Comme tous les coefficients sont nuls à partir d'un certain rang on pourra noter $P = \sum_{k=0}^{\infty} a_k X^k \in \mathbb{K}[X]$.

2) Parfois, on note $P(X)$ au lieu de P pour rappeler la notation de l'indéterminée.

Remarques (Identification des coefficients)

Deux polynômes de $\mathbb{K}[X]$ sont égaux si et seulement s'ils ont même degré et leurs coefficients sont égaux c'est à dire:

$$\sum_{k=0}^{n} a_k X^k = \sum_{k=0}^{m} b_k X^k \Leftrightarrow \begin{cases} m = n \\ \forall k \in [\![0, n]\!], \quad a_k = b_k \end{cases} .$$

I.2 Opérations sur les polynômes

Définition (Opérations sur les polynômes)

Soient $(P, Q) \in (\mathbb{K}[X])^2$ avec $P = \sum_{k=0}^{+\infty} a_k X^k$, $Q = \sum_{k=0}^{+\infty} b_k X^k$ et $\lambda \in \mathbb{K}$. On définit les lois :

- **Somme**. $P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$
- **Multiplication par un scalaire**. $\lambda P = \sum_{k=0}^{+\infty} \lambda a_k X^k$.
- **Produit**. $PQ = \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k = \sum_{k=0}^{+\infty} \left(\sum_{i+j=k} a_i b_j \right) X^k$.
- **Composition**. $P \circ Q$: $P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k$.

Remarques

La somme et le produit correspondent à ce que l'on aurait aimé avoir.
La composition est analogue à la composition de fonctions.

Théorème (Propriétés calculatoires)

1) $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.
   Le neutre pour $+$ est $0_{K[K]}$ et le neutre pour $\times$ et $1X^0 = 1$.
2) La composition $\circ$ est associative et distributive à droite par rapport à l'addition et la multiplication c'est-à-dire pour tout $(P, Q, R) \in (\mathbb{K}[X])^3$,

$$(P \circ Q) \circ R = P \circ (Q \circ R), \quad (PQ) \circ R = (P \circ R) \times (Q \circ R), \quad (P + Q) \circ R = (P \circ R) + (Q \circ R).$$

Remarques

- **Espace vectoriel**. On verra que $(\mathbb{K}[X], +, \cdot)$ est un espace vectoriel.
- **Pas de distributivité à gauche**. $X^2 \circ (X + X) \neq X^2 \circ X + X^2 \circ X$.
- **Notation**. Parfois on note $P(X)$ au lieu de P, $P(-X)$ au lieu de $P \circ (-X)$, $P(X^2)$ au lieu de $P \circ X^2$...

Exercice. Soit $P \in \mathbb{K}[X]$ un polynôme pair c'est-à-dire $P(-X) = P(X)$.
Montrer qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = Q(X^2)$.

I.3 Degré et opérations

Théorème (Opérations, degré et coefficient dominant)

Soient $(P, Q) \in (\mathbb{K}[X])^2$ et $\lambda \in \mathbb{K}$.

1) $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ **avec égalité si** $\deg P \neq \deg Q$ **ou** $\begin{cases} \deg P = \deg Q \\ \mathrm{CD}(P) \neq -\mathrm{CD}(Q) \end{cases}$

2) $\deg(\lambda P) = \begin{cases} \deg P & \text{si } \lambda \neq 0 \\ -\infty & \text{si } \lambda = 0 \end{cases}$

3) $\deg(PQ) = \deg P + \deg Q$ et $\mathrm{CD}(PQ) = \mathrm{CD}(P)\mathrm{CD}(Q)$

4) Si Q non nul, $\deg(P \circ Q) = \deg Q \deg P$ et $\mathrm{CD}(P \circ Q) = \mathrm{CD}(P)(\mathrm{CD}(Q))^{\deg P}$.

Remarques

Le degré et ces opérations sont souvent utilisées lorsque l'on cherche des polynômes vérifiant une propriété.

Exercice.

1) Déterminer les polynômes $P \in \mathbb{K}[X]$ vérifiant $P \circ P = P$.

2) Déterminer les polynômes $P \in \mathbb{K}[X]$ vérifiant $X^2 P = P(X^2)$.

3) On pose (P_n) la suite de polynômes vérifiant : $P_0 = 1$ et : $\forall n \in \mathbb{N}$, $P_{n+1} = 3XP_n + X$. Déterminer le degré de P_n et le coefficient dominant de P_n.

Théorème (Propriétés de l'anneau $\mathbb{K}[X]$)

1) $\mathbb{K}[X]$ **est intègre.** Soit $(P, Q) \in (\mathbb{K}[X])^3$, $PQ = 0_{\mathbb{K}[X]} \Rightarrow P = 0_{\mathbb{K}[X]}$ ou $Q = 0_{\mathbb{K}[X]}$.

2) **Simplification**. Soit $(P, Q, R) \in (\mathbb{K}[X])^3$, $PQ = PR$ et $P \neq 0_{\mathbb{K}[X]} \Rightarrow Q = R$.

3) **Eléments inversibles**. Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

II Arithmétique dans $\mathbb{K}[X]$

II.1 Multiples et diviseurs

Définition (Multiples - Diviseurs)

Soit $(A, B) \in (\mathbb{K}[X])^2$.
On dit que B **divise** A, noté $B|A$ ou que A **est un multiple de** B s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.

Exemple $X + 1$ divise $X^2 - 1$. Pour tout $n \in \mathbb{N}$, $X - 1$ divise $X^n - 1$.

Propriétés (Propriétés de la divisibilité)

Soient $(P, Q, R, A, B) \in (\mathbb{K}[X])^5$, $(\lambda, \mu) \in \mathbb{K}^2$.

1) **Relation** | La relation | sur $\mathbb{K}[X]$ est réflexive, transitive
2) **Polynômes associés**.

$$(P|Q \quad \text{et} \quad Q|P) \iff \exists \lambda \in \mathbb{K} \setminus \{0\} \,/\, Q = \lambda P.$$

Les polynômes P et Q sont dits associés.

3) **Combinaison linéaire**. Si $P|A$ et $P|B$ alors $P|\lambda A + \mu B$.
4) **Produit**. Si $P|A$ et $Q|B$ alors $PQ|AB$. En particulier, si $n \in \mathbb{N}^*$ et $P|A$ alors $P^n|A^n$.

II.2 Division euclidienne

Théorème (Division euclidienne)

Soit $(A, B) \in (\mathbb{K}[X])^2$ tel que $B \neq 0$.

Il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que $\begin{cases} A = BQ + R \\ \deg R < \deg B \end{cases}$.

Q est appelé le **quotient** et R le **reste**.

Remarques (Caractérisation de la divisibilité par le reste nul)

A est divisible par B si et seulement si le reste de la division euclidienne de A par B est nul.

✎ Méthode pratique ✎ (Déterminer quotient et reste de division euclidienne)

1) **Méthode 1**. On pose la division euclidienne (comme en primaire).
2) **Méthode 2**. On "force" la factorisation de A par B, le terme correctif est le reste.
3) **Méthode 3**. On réarrange A pour l'écrire sous forme $A = BQ + R$ avec $\deg R < \deg B$.

Exercice.

1) Déterminer le reste et le quotient de la division euclidienne de $X^4 + X^2 + X + 2$ par $X^2 - X + 1$.
2) Déterminer le reste et le quotient de la division euclidienne de $X^3 - X + 9$ par $X + 2$.
3) Déterminer le reste et le quotient de la division euclidienne de X^n par $X - 1$.

II.3 PGCD-PPCM

Définition (PPCM-PGCD)

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec A ou B non nul.

- On appelle PGCD de A et B tout diviseur commun à A et B de degré maximal.
  On notera $A \wedge B$ le seul PGCD de A et B unitaire.
- On appelle PPCM de A et B tout multiple commun à A et B de degré minimal.
  On notera $A \vee B$ le seul PPCM de A et B unitaire.

Remarques (PGCD et PPCM de deux polynômes)

On peut définir les PPCM et PGCD de n polynômes : $P_1 \wedge \cdots \wedge P_n$ et $P_1 \vee \cdots \vee P_n$.

Théorème (Propriété d'Euclide)

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec B non nul.
Si $A = BQ + R$ est la division euclidienne de A par B, alors pour $D \in \mathbb{K}[X]$,

$$[D|A \text{ et } D|B] \Leftrightarrow [D|B \text{ et } D|R].$$

Par conséquent, LES PGCD de A et B sont LES PGCD de B et R.

✎ Méthode pratique ✎ (Algorithme d'Euclide : calcul du PGCD)

On souhaite déterminer le PGCD de deux polynômes A et B non nuls.
L'algorithme repose sur la propriété d'Euclide, il consiste à définir les polynômes successifs R_0, R_1,... de la manière suivante:

- au départ $R_0 = A$ et $R_1 = B$
- ensuite si $R_1 \neq 0$, on définit R_2 le reste de la division euclidienne de R_0 par R_1 ($\deg R_2 < \deg R_1$)
- ...
- on répète le procédé, tant que $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} ($\deg R_{k+2} < \deg R_{k+1}$)

La suite $(\deg R_k)$ est strictement décroissante, d'entiers naturels, donc il existe $N \in \mathbb{N}^*$ tel que $R_{N+1} = 0$ et $R_N \neq 0$.
D'après le principe d'Euclide R_N est un PGCD de A et B.

Exercice. Déterminer le PGCD de $A = X^3 + 3X^2 - X - 3$ et $B = X^2 - 3X + 2$.

Propriétés (Propriétés des PGCD et PPCM)

1) Les diviseurs communs à deux polynômes sont les diviseurs d'un PGCD.
2) Les multiples communs à deux polynômes sont les multiples d'un PPCM.
3) Les PGCD (resp. PPCM) de deux polynômes sont des polynômes associés.
4) Les lois $\wedge$ et $\vee$ sont associatives.

Propriétés (Une formule)

Soient A et B deux polynômes unitaires dont l'un est non nul. Alors: $(A \wedge B) \times (A \vee B) = AB$.

Théorème (Relation de Bezout)

1) Soient A et B deux polynômes non nuls et D UN PGCD de A et B.
Alors il existe $(U, V) \in (\mathbb{K}[X])^2$ tel que: $AU + BV = D$.
On dit que (U, V) est **un couple de Bezout** associé à A et B.
2) **Généralisation**. Soient $A_1, \ldots, A_n$, des polynômes non nuls et D un PGCD des polynômes $A_1, \ldots, A_n$.
Alors, il existe $(U_1, \ldots, U_n) \in (\mathbb{K}[X])^n$ tel que: $A_1U_1 + \cdots + A_nU_n = D$.

Exercice. Déterminer un couple de Bezout lorsque $A = X^2 - 1$ et $B = X^2 - 3X + 2$.

✎ Méthode pratique ✎ (Algorithme d'Euclide étendu pour trouver un couple de Bezout)

On peut adapter l'algorithme d'Euclide étendu de $\mathbb{Z}$ en présentant les calculs dans un tableau.
Soient A et B deux polynômes non nuls.

1) On applique l'algorithme d'Euclide à A et B on construit alors une suite de restes (R_n) et une suite de quotients (Q_n) qui vérifient donc :

$$R_n = Q_{n+1}R_{n+1} + R_{n+2} \qquad R_0 = a \qquad R_1 = b.$$

Un PGCD de A et B est le dernier reste non nul noté R_N.

2) On détermine des suites (U_n) et (V_n) telles que $R_n = U_nA + V_nB$ pour $0 \leqslant n \leqslant N$.
Les suites (U_n) et (V_n) définies par $\begin{cases}(U_0, V_0) = (1, 0)\\(U_1, V_1) = (0, 1)\end{cases}$ et $\begin{cases}U_{n+2} = U_n - Q_{n+1}V_{n+1}\\V_{n+2} = V_n - Q_{n+1}V_{n+1}\end{cases}$ conviennent (ce que l'on prouve par récurrence).

3) On déduit alors: $A \wedge B = R_N = U_NA + V_NB$ et donc (U_N, V_N) est un couple de Bezout de A et B.

4) On présente les calculs dans un tableau :

	$R_0 = A$	$R_1 = B$	R_2	$\dots$	R_n	$\dots$	$A \wedge B$
Q_k		Q_1	Q_2	$\dots$	Q_n	$\dots$	
U_k	1	0	U_2	$\dots$	U_n	$\dots$	U_N
V_k	0	1	V_2	$\dots$	V_n	$\dots$	V_N

Exercice. Déterminer UN couple de Bezout pour $A = X^3 + 3X^2 - X - 3$ et $X^2 - 3X + 2$.

II.4 Polynômes premiers entre eux

Définition (Polynômes premiers entre eux)

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec A ou B non nul.
On dit que A et B sont **premiers entre eux** si $A \wedge B = 1$.
Autrement dit, A et B sont premiers entre eux si A et B n'ont pas d'autres diviseurs communs que les polynômes constants non nuls.

Exercice. Montrer que lorsque $a \neq b$ les polynômes $X - a$ et $X - b$ sont premiers entre eux.

Théorème (Théorème de Bezout)

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec A et B non nul.
Alors :

$$A \wedge B = 1 \quad \Leftrightarrow \quad \exists (U, V) \in (\mathbb{K}[X])^2 \ / \ AU + BV = 1.$$

Exercice. Montrer que lorsque $a \neq b$ les polynômes $X - a$ et $X - b$ sont premiers entre eux.

✎ Méthode pratique ✎ (Comment prouver que deux polynômes sont premiers entre eux)

- On peut montrer que le PCGD unitaire vaut 1, par exemple avec l'algorithme d'Euclide.
- On peut montrer qu'un diviseur commun divise nécessairement 1.
- On peut utiliser le théorème de Bezout.

Exercice. Soit $(A, B, C) \in (\mathbb{K}[X])^3$, A, B et C non nuls.

1) Montrer que si A et B sont premiers entre eux, alors les diviseurs de A sont premiers avec B.

2) On suppose $\begin{cases}A \wedge B = 1\\A \wedge C = 1\end{cases}$. Montrer que $A \wedge BC = 1$.
En déduire que pour tout $(p, q) \in (\mathbb{N}^*)^2$, $A^p \wedge B^q = 1$.

3) Soit $(p,q) \in \mathbb{N}^2$. Montrer que lorsque $a \neq b$ les polynômes $(X-a)^p$ et $(X-b)^q$ sont premiers entre eux.

Théorème (Théorème de Gauss)

Soient A, B et C trois polynômes non nuls.

$$\text{Si} \quad \begin{cases} A \text{ divise } BC \\ A \wedge B = 1 \end{cases} \quad \text{alors} \quad A \text{ divise } C.$$

Corollaire

Soient A, B et C trois polynômes non nuls.

$$\text{Si} \quad \begin{cases} A \text{ divise } C \\ B \text{ divise } C \\ A \wedge B = 1 \end{cases} \quad \text{alors} \quad AB \text{ divise } C.$$

Définition (n polynômes premiers entre eux)

Soient $(a_1, \dots, a_n) \in (\mathbb{K}[X])^n$.

1) On dit que $A_1, \dots, A_n$ sont **premiers entre eux dans leur ensemble** si $A_1 \wedge \cdots A_n = 1$.
2) On dit que $A_1, \dots, A_n$ sont **premiers entre eux 2 à 2** si pour tout $(i,j) \in [\![1,n]\!]^2$, $A_i \wedge A_j = 1$.

III Fonction polynomiale. Racines d'un polynôme.

III.1 Fonction polynomiale.

Définition (Fonction polynomiale)

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

La fonction polynomiale associée à P est la fonction $\begin{array}{rccc} \widetilde{P} : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \sum_{k=0}^{n} a_k x^k \end{array}$.

⚠ **Attention** ⚠ Il convient de bien distinguer polynôme et fonction polynomiale associée. Ce ne sont mathématiquement pas les mêmes objets. Si $P = X^2 + 1$, on peut **évaluer** P en 2 en calculant $\widetilde{P}(2) = 5$.

Théorème (Opérations sur les fonctions polynomiales)

Soient $(P,Q) \in (\mathbb{K}[X])^2$ et $\lambda \in \mathbb{K}$. Alors

$$\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}, \qquad \widetilde{PQ} = \widetilde{P}\widetilde{Q}, \qquad \widetilde{\lambda P} = \lambda \widetilde{P}, \qquad \widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}.$$

☞ **Explication** ☜ Cela signifie que les lois sur $\mathbb{K}[X]$ correspondent à celles sur $\mathbb{K}^{\mathbb{K}}$.

✎ Méthode pratique ✎ (Algorithme de Horner)

La méthode de Horner d'évaluation polynomiale est basée sur la réécriture de $P = \sum_{k=0}^{n} a_k X^k$ sous forme :

$$P(X) = a_0 + X[a_1 + X[a_2 + X[\ldots + X[a_n]]]].$$

Pour le calcul de $P(\alpha)$ où $\alpha \in \mathbb{K}$, on peut mettre en oeuvre l'algorithme de Horner en dressant le tableau :

Coefficients de P	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
Calculs intermédiaires = ...	a_n	$a_n\alpha + a_{n-1}$	$(a_n\alpha + a_{n-1})\alpha + a_{n-2}$	$\ldots$	A	$\widetilde{P}(\alpha) = A\alpha + a_0$
... coefficients de Q	q_{n-1}	q_{n-2}	q_{n-3}	$\ldots$	q_0	Reste

On part donc du coeur du parenthésage. On part de a_n, on multiplie par α, on ajoute a_{n-1}, on multiplie par α, on ajoute a_{n-2},.....on ajoutera enfin a_0.

Application : le tableau ci-dessus donne les coefficients du polynôme $Q = \sum_{k=0}^{n-1} q_k X^k$ quotient de la division euclidienne de P par $X - \alpha$ et le reste.

Exemple On pose $P = 2X^3 - 4X^2 + 5X - 7$. Mettre en oeuvre l'algorithme d'Euclide pour évaluer $\widetilde{P}(2)$ et déterminer le quotient de la division euclidienne de P par $X - 2$.

III.2 Racines d'un polynôme

Théorème-Définition (Racines et multiplicité)

Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

- $\widetilde{P}(\alpha) = 0$ si et seulement si $X - \alpha$ divise P. On dit dans ce cas que α est **racine (ou zéro)** de P.
- Si α est racine de P, **l'ordre de multiplicité** de la racine est le plus grand entier $m \in \mathbb{N}^*$ tel que $(X - \alpha)^m$ divise P c'est-à-dire :

  $$(X - \alpha)^m | P \qquad \text{et} \qquad (X - \alpha)^{m+1} \not| P.$$

  On dit que α est de multiplicité m.
  De manière équivalente α est une racine de P de multiplicité m s'il existe $Q \in \mathbb{K}[X]$ tel que

  $$P = (X - \alpha)^m Q \qquad \text{et} \qquad Q(\alpha) \neq 0.$$

Exemple Le polynôme $P = (X-1)^3 X^2 (X+2)$ possède trois racines **comptées sans leur multiplicité** : 1 (de multiplicité 3), 0 (de multiplicité 2), -2 (de multiplicité 1). Le polynôme P possède 6 racines **comptées avec leur multiplicité**.

Remarques

- α est racine de P d'ordre de multiplicité au moins m si $(X - \alpha)^m$ divise P.
- α est une racine **multiple** de P si son ordre de multiplicité est supérieur ou égal à 2.
- Une racine d'ordre 1/2/3 est dite racine **simple/double/triple**.

Théorème (Factorisation par $(X-\alpha_1)^{m_1}\cdots(X-\alpha_k)^{m_k}$)

Soit $P \in \mathbb{K}[X]$.

1) Soit $(\alpha_1, \ldots, \alpha_k) \in \mathbb{C}^k$ des racines distinctes de P de multiplicités respectives $m_1, \ldots, m_k \in \mathbb{N}^*$, alors:

$$\prod_{i=1}^{k}(X-\alpha_i)^{m_i} \quad \text{divise} \quad P.$$

2) Si de plus, $m_1 + \cdots + m_k = n = \deg P$, alors:

$$P = \lambda \prod_{i=1}^{k}(X-\alpha_i)^{m_i} \qquad \text{où } \lambda \in \mathbb{K}^* \text{ est le coefficient dominant de } P.$$

Dans ce cas, on dit que le polynôme est scindé sur $\mathbb{K}$. Autrement dit P est scindé $\boxed{\text{sur } \mathbb{K}}$ s'il admet n racines $\boxed{\text{dans } \mathbb{K}}$ comptées avec multiplicité.

⚠ **Attention** ⚠ La précision scindée $\boxed{\text{sur } \mathbb{K}}$ est essentielle. Un polynôme peut être scindé sur $\mathbb{C}$ sans pour autant l'être sur $\mathbb{R}$. Par exemple $X^2+1 = (X-\mathrm{i})(X+\mathrm{i})$ est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$.
En revanche: "scindé sur $\mathbb{R}$" $\Rightarrow$ "scindé sur $\mathbb{C}$" car $\mathbb{R} \subset \mathbb{C}$.

✎ **Méthode pratique** ✎ **(Déterminer le reste de la division euclidienne à l'aide des racines)**

On peut dans certains cas déterminer le reste de la division eucldienne de A par B (sans déterminer le quotient).

- On pose Q et R les quotient et reste : $(*)$ $\quad A = BQ + R \qquad$ où $\qquad \deg R < \deg B$.
- On évalue la relation $(*)$ en les racines α de B :

$$\widetilde{A}(\alpha) = \widetilde{B}(\alpha)\widetilde{Q}(\alpha) + \widetilde{R}(\alpha) \qquad \text{qui donne} \qquad (**)\ \widetilde{A}(\alpha) = \widetilde{R}(\alpha)$$

- On pose alors les coefficients de R, il y en a autant que le degré de B. Les relations $(**)$ donnent alors un système donc les inconnues sont les coefficients de R.

Cette méthode s'applique plutôt dans le cas où $\deg B$ est petit, dans ce cas il y a peu de coefficients de R à déterminer.

Exercice.

1) Déterminer le reste de la division euclidienne de X^n par $X-1$.
2) Déterminer le reste de la division euclidienne de $X^{200}+X+2$ par X^2-1.
3) Déterminer le reste de la division euclidienne de $X^{200}+X+2$ par X^2+1. *La proposition suivante peut être utile.*

Proposition

Soient $P \in \boxed{\mathbb{R}}[X]$ et $\alpha \in \mathbb{C}$. Alors :

$$\alpha \text{ racine de } P \Leftrightarrow \overline{\alpha} \text{ racine de } P.$$

Dans ce cas les racines complexes conjuguées α et $\overline{\alpha}$ ont même multiplicité.

Exercice. Montrer que X^2+X+1 divise X^4+X^2+1.

Théorème (Lien entre nombre de racines et degré)

1) Soit $n \in \mathbb{N}$. Tout polynôme **non nul** de degré inférieur ou égal à n possède au plus n racines **comptées avec leur multiplicité**.
2) Soit $n \in \mathbb{N}$. Un polynôme de degré inférieur ou égal à n possèdant au moins $n+1$ racines **comptées avec leur multiplicité** est nul.
3) Seul le polynôme nul possède une infinité de racines.

Exercice.

1) Soit P un polynôme de $\mathbb{R}[X]$ tel que pour tout $k \in \mathbb{N}$, $\widetilde{P}(k)=0$. Montrer que P est le polynôme nul.
2) Soient P et Q deux polynômes de $\mathbb{C}[X]$ tel que $P(X^2)=Q(X^2)$. Montrer que $P=Q$.

⚠ **Attention** ⚠ Un polynôme de $\mathbb{K}[X]$ de degré $n \in \mathbb{N}$ n'a pas forcément n racines dans $\mathbb{K}$, comptées avec leur multiplicité. Par exemple X^2+1 n'a aucune racine dans $\mathbb{R}$. En revanche quand $\mathbb{K}=\mathbb{C}$, c'est le cas, on le verra plus loin (théorème de d'Alembert).

Proposition (Identification polynôme-fonction polynomiale)

L'application $\begin{array}{rccc}\Psi : & \mathbb{K}[X] & \to & \mathcal{P} \\ & P & \mapsto & \widetilde{P}\end{array}$ est une bijection.
En particulier, si deux fonction polynomiales sont égales alors les polynômes associés le sont aussi ce qui justifie l'identification du polynôme P avec sa fonction polynomiale $\widetilde{P}$ et donc cela justifie de pouvoir écrire $P(\alpha)$ au lieu de $\widetilde{P}(\alpha)$.
On peut montrer mieux : cette application est un isomorphisme d'espaces vectoriels et un isomorphismes d'anneaux.

⚠ **Attention** ⚠ Ce résultat est faux dans d'autres corps, en particulier les corps finis. Contre-exemple :

III.3 Polynômes d'interpolation de Lagrange

Objectif : soient $n \in \mathbb{N}^*$, $x_0, \dots, x_n$ des éléments de $\mathbb{K}$ deux à deux distincts et $y_0, \dots, y_n$ des éléments de $\mathbb{K}$.
On cherche un polynôme P tel que : $\forall i \in [\![0,n]\!]$, $P(x_i)=y_i$ (c'est le problème de l'interpolation).

On cherche tout d'abord, pour $i \in [\![0,n]\!]$ les polynômes L_i de degré n vérifiant :

$$L_i(x_i)=1 \qquad \forall j \in [\![0,n]\!],\ j \neq i, \qquad L_i(x_j)=0.$$

Définition (Bases de Lagrange)

On appelle polynômes interpolateurs de Lagrange aux abscisses $x_0, \dots, x_n$ les polynômes $L_0, \dots, L_n$ définis par :

$$\forall i \in [\![0,n]\!], \qquad L_i =$$

Théorème (Interpolation de Lagrange)

Soient $n \in \mathbb{N}^*$, $x_0, \dots, x_n$ des éléments de $\mathbb{K}$ deux à deux distincts et $y_0, \dots, y_n$ des éléments de $\mathbb{K}$.

1) Il existe un **unique** polynôme $P \in \mathbb{K}[X]$ de degré **au plus** n tel que : $\forall i \in [\![0, n]\!]$, $P(x_i) = y_i$, il est défini par :

$$P = \sum_{i=0}^{n} y_i L_i =$$

2) Les polynômes $Q \in \mathbb{K}[X]$ vérifiant : $\forall i \in [\![0, n]\!]$, $Q(x_i) = y_i$, sont les polynômes :

$$Q = P + \prod_{i=0}^{n} (X - x_i) \times S$$

où $S \in \mathbb{K}[X]$ et P le polynôme défini dans 1).

IV Dérivation

IV.1 Polynome dérivé

Définition (Polynôme dérivé)

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

1) Le **polynôme dérivé** de P est défini par $P' = \sum_{k=0}^{n} k a_k X^{k-1} = \sum_{\boxed{k=1}}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k$.

2) Pour $k \in \mathbb{N}$, on note $P^{(k)}$, les dérivées successives de P définies par récurrence par $\begin{cases} P^{(0)} = P \\ \forall k \in \mathbb{N}^*, \quad P^{(k)} = (P^{(k-1)})' \end{cases}$.

Exemples

1) Si $P = X^3 + 2X^2 + X + 1$ alors $P' = 3X^2 + 4X + 1$, $P'' = 6X + 4$, $P''' = 6$, $P^{(k)} = 0$ pour tout $k \geqslant 4$.

2) Si $P = \sum_{k=0}^{n} a_k X^k$ alors $P^{(n)} = n! a_n$ et $P^{(k)} = 0$ pour tout $k \geqslant n + 1$.

Exercice. Calculer les dérivées successives de X^n.

Exercice. Déterminer les polynômes P de $\mathbb{C}[X]$ vérifiant $P'^2 = P$.

☞ **Explication** ☜ Cette définition est purement formelle. Jusqu'alors on connaissait la notion de dérivée de fonction ici on introduit la dérivée de polynôme. Évidemment, ces deux notions coincident si l'on considère la dérivée d'un polynôme et la dérivée de la fonction polynomiale associée i.e. $\widetilde{P'} = \widetilde{P}'$. De sorte que les règles de dérivation des opérations sur les polynômes sont les mêmes que pour les fonctions.

Théorème (Opérations et dérivation de polynômes)

Soient $(P,Q) \in (\mathbb{K}[X])^2$, $m \in \mathbb{N}$ et $\lambda \in \mathbb{R}$ alors:

1) $\deg P^{(m)} = \deg P - m$ si $m \leqslant \deg P$ et $P^{(m)} = 0$ sinon
2) $(P+Q)^{(m)} = P^{(m)} + Q^{(m)}$
3) $(PQ)' = P'Q + PQ'$ et $(PQ)^{(m)} = \sum_{i=0}^{m} \binom{m}{i} P^{(i)} Q^{(m-i)}$ (formule de Leibniz)
4) $(\lambda P)' = \lambda P'$
5) $(P \circ Q)' = (P' \circ Q)Q'$.

IV.2 Formule de Taylor

Théorème (Formule de Taylor pour les polynômes)

Soient $P \in \mathbb{K}_n[X]$ et $\alpha \in \mathbb{K}$. Alors:

$$P(X) = P(\alpha) + P'(\alpha)(X-\alpha) + P''(\alpha)\frac{(X-\alpha)^2}{2!} + \cdots + P^{(n)}(\alpha)\frac{(X-\alpha)^n}{n!} = \sum_{k=0}^{n} P^{(k)}(\alpha)\frac{(X-\alpha)^k}{k!}$$

Exercice. Déterminer le reste et le quotient de la division euclidienne de $P \in \mathbb{K}$ par $(X-1)^k$. On exprimera le reste et le quotient à l'aide des dérivées successives de P.

Théorème (Caractérisation de la multiplicité à l'aide des dérivées)

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$. Alors:

$$\begin{cases} \alpha \text{ est racine de } P \text{ d'ordre} \\ \text{de multiplicité } m \geqslant 1 \end{cases} \iff \begin{cases} P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0 \\ P^{(m)}(\alpha) \neq 0 \end{cases}.$$

Exemples

1) Soit $P = X^3 - X^2 + 2X + 4$. Montrer que -1 est racine d'ordre de multiplicité 1.
2) Soit $P = 2X^3 - 7X^2 + 4X + 4$. Montrer que 2 est racine d'ordre de multiplicité 2.

Exercice.

1) Montrer que pour tout $n \in \mathbb{N}$, $(X+1)^2$ divise $(X+2)^n - nX - n - 1$.
2) Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Donner une caractérisation de "α est une racine multiple de P".
3) Soit $P \in \mathbb{K}[X]$. Donner une caractérisation de "P admet une racine multiple".

Remarques

Soient $P \in \boxed{\mathbb{R}}[X]$ et $\alpha \in \mathbb{C}$. On peut montrer que :

$$\alpha \text{ racine de } P \text{ de multiplicité } m \Leftrightarrow \overline{\alpha} \text{ racine de } P \text{ de multiplicité } m.$$

V Factorisation de polynômes

V.1 Polynômes irréductibles de $\mathbb{R}[X]$ et de $\mathbb{C}[X]$

Définition (Polynôme irréductible)

Soit $P \in \mathbb{K}[X]$. P est **irréductible** sur $\mathbb{K}$ si $\deg P \geqslant 1$ et si les seuls diviseurs de P dans $\mathbb{K}[X]$ sont:

- les polynômes constants non nuls
- les polynômes associés à P, λP où $\lambda \in \mathbb{K}^*$.

Remarques

- La notion de polynôme irréductible est l'analogue pour les polynômes de la notion de nombre premier pour les entiers. Il existe d'ailleurs des résultats de décomposition de polynômes en produit de polynômes irréductibles analogues au théorème fondamental de l'arithmétique dans $\mathbb{Z}$.
- On dira donc qu'un polynôme est réductible (n'est pas irréductible) s'il s'écrit comme le produit de deux polyômes de de degré $\geqslant 1$.

Exemple $X^2 + 1$ est réductible sur $\mathbb{C}$ (car divisible par $X - \mathrm{i}$ et $X + \mathrm{i}$) mais irréductible sur $\mathbb{R}$.

Théorème (de d'Alembert-Gauss où Théorème fondamental de l'algèbre)

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

Preuve - Admis. □

Corollaire

1) Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.
2) Tout polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}$, possède exactement n racines dans $\mathbb{C}$ comptées avec leur multiplicité.

⚠ **Attention** ⚠ Le résultat est faux dans $\mathbb{R}$. Contre-exemple :

Exercice. Montrer que deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racine commune.

Théorème (Polynômes irréductibles et décomposition dans $\mathbb{C}[X]$)

1) **Les polynômes irréductibles de** $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
2) **Décomposition primaire dans** $\mathbb{C}[X]$ Tout polynôme de $\mathbb{C}[X]$ s'écrit de façon unique (à l'ordre près) sous la forme :
$$P = \lambda(X - \alpha_1) \cdots (X - \alpha_n)$$
où les α_i sont complexes et $\lambda \in \mathbb{C}$ est le coefficient dominant de P.

Exercice.

1) **Résultat à connaître.** Donner la décomposition primaire (décomposition en produit de polynômes irréductibles) dans $\mathbb{C}[X]$ de $X^n - 1$.

2) Donner la décomposition primaire (décomposition en produit de polynômes irréductibles) dans $\mathbb{C}[X]$ de $X^4 + 16$.

Corollaire (Caractérisation de la divisibilité dans $\mathbb{C}[X]$ aves les racines)

Soient deux polynômes A et B de $\mathbb{C}[X]$ avec B non nul. Alors :

$$B|A \Leftrightarrow \text{ LES racines de } B \text{ sont DES racines de } A \text{ d'ordre de multiplicité inférieur.}$$

Théorème (Polynômes irréductibles et décomposition dans $\mathbb{R}[X]$)

1) **Les polynômes irréductibles de** $\mathbb{R}[X]$ sont:
   - les polynômes de degré 1
   - les polynômes de degré 2 dont le discriminant est < 0 (pas de racine réelle).
2) Tout polynôme de $\mathbb{R}[X]$ s'écrit de façon unique (à l'ordre près) sous la forme :
$$P = \lambda(X - \alpha_1)\cdots(X - \alpha_n)(X^2 + r_1X + s_1)\cdots(X^2 + r_pX + s_p)$$
où les α_i, r_i et s_i sont réels et $\lambda \in \mathbb{R}$ est le coefficient dominant de P et les polynômes de degré 2 sont de discriminant négatif.

⚠ **Attention** ⚠ Un polynôme peut n'admettre aucune racine réelle et pourtant être réductible dans $\mathbb{R}[X]$. Contre-exemple :

Exercice.

1) Montrer que tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine réelle.

2) Factoriser dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ le polynôme $X^4 + 16$.

3) Factoriser dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme $X^{2n} - 1$.

✎ **Méthode pratique** ✎ **(Décomposition primaire dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$)**

- Pour obtenir la décomposition de P dans $\mathbb{C}[X]$:
  - ▶ **Méthode 1** : on détermine les racines de P et leur multiplicité
  - ▶ **Méthode 2** : on factorise grâce à des formules de factorisation (identité remarquables...) jusqu'à obtenir un produit de polynômes de degré 1.
- Pour obtenir la décomposition de P dans $\mathbb{R}[X]$:
  - ▶ **Méthode 1** : on décompose dans $\mathbb{C}[X]$ et on regroupe les paires de racines complexes conjugués en utilisant la relation
$$(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha^2|.$$
  - ▶ **Méthode 2** : on factorise grâce à des formules de factorisation (identité remarquables...) jusqu'à obtenir un produit de polynômes de degré 1 et de degré 2 de discriminant < 0.

VI Relations coefficients-racines

Théorème (Relations coefficients-racines - Formules de Viète)

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}^*$ scindé sur $\mathbb{K}$ de racines $\alpha_1, \dots, \alpha_n$ comptées avec leur multiplicité (donc non nécessairement distinctes). On pose pour $k \in [\![1, n]\!]$:

$$\sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k},$$

appelées **fonctions symétriques élémentaires des racines** i.e.

$$\sigma_1 = \sum_{1 \leqslant i_1 \leqslant n} \alpha_{i_1} = \alpha_1 + \cdots + \alpha_n \qquad \text{(somme)}$$

$$\sigma_2 = \sum_{1 \leqslant i_1 < i_2 \leqslant n} \alpha_{i_1}\alpha_{i_2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n \qquad \text{(somme des produits 2 à 2)}$$

$$\sigma_3 = \sum_{1 \leqslant i_1 < i_2 < i_3 \leqslant n} \alpha_{i_1}\alpha_{i_2}\alpha_{i_3} = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_3\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n \qquad \text{(somme des produits 3 à 3)}$$

$$\dots\dots$$

$$\sigma_n = \alpha_1\alpha_2 \cdots \alpha_n \qquad \text{(produit)}.$$

Alors pour tout $k \in [\![1, n]\!]$, $\sigma_k = (-1)^k \dfrac{a_{n-k}}{a_n}$.

Réciproquement, si les valeurs des fonctions symétriques élémentaires sont connues, alors $\alpha_1, \dots, \alpha_n$ sont racines du polynôme

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n \sigma_n.$$

☞ **Explication** ☜ D'après ce théorème, quelque soit le degré du polynôme, on dispose toujours de relations entre coefficients et racines. Ces relations de par leur forme ne permettent pas a priori d'exprimer les racines en fonction des coefficients (ou l'inverse). Cela dit on sait (depuis la première) que dans le cas d'un polynôme de degré 2, on sait exprimer les racines en fonction des coefficients, les fameuses formules $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. Pour les degrés 3 et 4 il existe aussi des formules permettant d'exprimer les racines en fonction des coefficients (formules de Cardan pour le degré 3 et de Ferrari pour le degré 4). En revanche, pour le degré 5 et plus, il est démontré qu'il n'existe pas de telles formules (théorie de Galois, compliqué...). Ces relations sont donc un pis aller, elles n'expriment pas racines en fonction des coefficients mais relient racines aux coefficients.

Exercice.

1) Déterminer $(\alpha_1, \alpha_2) \in \mathbb{R}^2$ tels que $\begin{cases} \alpha_1 + \alpha_2 = \dfrac{8}{3} \\ \alpha_1\alpha_2 = \dfrac{4}{3} \end{cases}$.

2) Soit $P = X^3 + X^2 + 1$ et $\alpha_1, \alpha_2, \alpha_3$ les racines de P dans $\mathbb{C}$. Calculer $S = \sum_{i=1}^{3} \alpha_i^2$ et $T = \sum_{i=1}^{3} \dfrac{1}{\alpha_i^2}$.

3) Résoudre le système $\begin{cases} a + b + c = 1 \\ a^2 + b^2 + c^2 = 3 \\ a^3 + b^3 + c^3 = 1 \end{cases}$.