Chapitre 17 Polynômes

Dans ce cours, $\mathbf{K}$ représente $\mathbf{R}$ ou $\mathbf{C}$ et n désignera un entier naturel.

17.1 Culture : la vraie définition des polynômes

17.1.1 Définition et opérations

Définition 17.1 - Polynôme.

On appelle **polynôme à coefficients dans $\mathbf{K}$** toute suite $(a_i)_{i\in\mathbf{N}}$ d'éléments de $\mathbf{K}$ nulle au-delà d'un certain rang, c'est-à-dire telle qu'il existe $N \in \mathbf{N}$ tel que pour tout $i \geqslant N$, $a_i = 0$.
Si P est un tel polynôme, on note $P = (a_i)_{i\in\mathbf{N}} = (a_0, a_1, \dots, a_N, 0, 0, \dots)$. Les nombres a_i sont appelés les **coefficients** du polynôme P.
Par définition, deux polynômes $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ sont **égaux** si, et seulement si, les suites $(a_i)_{i\in\mathbf{N}}$ et $(b_i)_{i\in\mathbf{N}}$ sont les mêmes, autrement dit, si, et seulement si, tous leurs coefficients sont égaux :

$$P = Q \iff \forall i \in \mathbf{N},\ a_i = b_i.$$

L'ensemble des polynômes, pour l'instant noté $\mathcal{P}_\mathbf{K}$, est donc un sous-ensemble de l'ensemble $\mathbf{K}^\mathbf{N}$ des suites à coefficients dans $\mathbf{K}$:

$$\mathcal{P}_\mathbf{K} = \left\{(a_i)_{i\in\mathbf{N}} \in \mathbf{K}^\mathbf{N} \mid \exists N \in \mathbb{N},\ \forall i > N,\ a_i = 0\right\}.$$

▻ **Addition interne**
L'addition sur l'ensemble des polynômes est définie de la même façon que celle sur l'ensemble $\mathbf{K}^\mathbf{N}$ des suites d'éléments de $\mathbf{K}$: la somme des deux polynômes $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ est définie par

$$P + Q = (a_i + b_i)_{i\in\mathbf{N}}.$$

Si la suite $(a_i)_{i\in\mathbf{N}}$ est nulle au-delà du rang N_p et la suite $(b_i)_{i\in\mathbf{N}}$ nulle au-delà du rang N_q, alors la suite $(a_i + b_i)$ est nulle au delà du rang $\max(N_p, N_q)$ donc $P + Q$ est bien un polynôme.

▻ **Multiplication par un élément de K (produit externe)**
Cette opération est aussi la même que celle définie sur $\mathbf{K}^\mathbf{N}$: le produit d'un polynôme $P = (a_i)_{i\in\mathbf{N}}$ par un *scalaire* $\lambda \in \mathbf{K}$ est défini par

$$\lambda \cdot P = (\lambda a_i)_{i\in\mathbf{N}}.$$

Si la suite $(a_i)_{i\in\mathbf{N}}$ est nulle au-delà du rang N, alors la suite $(\lambda a_i)_{i\in\mathbf{N}}$ est nulle aussi au-delà du rang N donc $\lambda \cdot P$ est bien un polynôme.

▻ **Multiplication interne (produit de Cauchy de deux polynômes)**
Cette multiplication n'est pas définie comme celle de deux suites numériques quelconques.
Le produit des deux polynômes $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ est défini par

$$P \times Q = (c_i)_{i\in\mathbf{N}} \qquad \text{où} \quad \forall i \in \mathbf{N}, \quad c_i = \sum_{k=0}^{i} a_k b_{i-k} = \sum_{\substack{k,\ell\geqslant 0\\ k+\ell=i}} a_k b_\ell.$$

Si la suite $(a_i)_{i\in\mathbf{N}}$ est nulle au-delà du rang N_p et si la suite $(b_i)_{i\in\mathbf{N}}$ est nulle au delà du rang N_q, alors la suite $(c_i)_{i\in\mathbf{N}}$ est nulle au delà du rang $N_p + N_q$. En effet, si $i > N_p + N_q$, alors

$$c_i = \sum_{k=0}^{N_p} a_k \underbrace{b_{i-k}}_{\substack{=0\\ \text{car } i-k>N_q}} + \sum_{k=N_p+1}^{i} \underbrace{a_k}_{=0} b_{i-k} = 0$$

donc $P \times Q$ est bien un polynôme et la multiplication ainsi définie est une opération interne sur $\mathcal{P}_{\mathbb{K}}$ (qui n'est pas le produit « classique » des deux suites $(a_i)_{i\in\mathbf{N}}$ et $(b_i)_{i\in\mathbf{N}}$).

- On peut vérifier que :
  - ▷ l'addition est une opération associative : pour P, Q, R des polynômes, $(P+Q)+R = P+(Q+R)$.
  - ▷ l'addition est une opération commutative : pour P, Q des polynômes, $P+Q = Q+P$.
  - ▷ le polynôme nul 0 est l'élément neutre de l'addition : pour P un polynômes, $P+0 = 0+P = P$.
  - ▷ tout polynôme $P = (a_i)_{i\in\mathbf{N}}$ possède un opposé noté $-P$ et l'on a $-P = (-a_i)_{i\in\mathbf{N}} = -1\cdot P$.

  On dit que : $(\mathcal{P}_{\mathbf{K}}, +)$ est un groupe commutatif.
- On vérifie aussi facilement que :
  - ▷ $\forall \alpha, \beta \in \mathbf{K},\ \forall P \in \mathcal{P}_{\mathbf{K}},\ (\alpha+\beta)\cdot P = \alpha\cdot P + \beta\cdot P$,
  - ▷ $\forall \alpha \in \mathbf{K},\ \forall P, Q \in \mathcal{P}_{\mathbf{K}},\ \alpha\cdot(P+Q) = \alpha\cdot P + \alpha\cdot Q$,
  - ▷ $\forall \alpha, \beta \in \mathbf{K},\ \forall P \in \mathcal{P}_{\mathbf{K}},\ \alpha\cdot(\beta\cdot P) = (\alpha\beta)\cdot P$,
  - ▷ $\forall P \in \mathcal{P}_{\mathbf{K}},\ 1\cdot P = P$.

  Ces quatre propriétés de la multiplication externe, combinées avec le fait que $(\mathcal{P}_{\mathbf{K}}, +)$ est un groupe commutatif, confèrent à $(\mathcal{P}_{\mathbf{K}}, +, \cdot)$ une structure d'espace vectoriel.
- On vérifie aussi que :
  - ▷ la multiplication interne est associative : pour P, Q, R des polynômes, $(P\times Q)\times R = P\times(Q\times R)$.
  - ▷ la multiplication interne est commutative : pour P, Q des polynômes, $P\times Q = Q\times P$.
  - ▷ le polynôme unité $1 = (1, 0, 0, \dots)$ est l'élément neutre de la multiplication : pour P un polynômes, $P\times 1 = 1\times P = P$.
  - ▷ la multiplication interne est distributive par rapport à l'addition : pour tous polynômes P, Q et R, on a $(P+Q)\times R = P\times R + Q\times R$ et $P\times(Q+R) = P\times Q + P\times R$.

  Ces propriétés, combinées avec le fait que $(\mathcal{P}_{\mathbf{K}}, +)$ soit un groupe commutatif, confère à $(\mathcal{P}, +, \times)$ une structure d'anneau commutatif.

  Comme dans n'importe quel anneau commutatif, on a $P\times 0 = 0\times P = 0$ pour tout polynôme P, la notation P^0 désigne le polynôme 1 (unité pour la multiplication) et l'on a $P\times 1 = 1\times P = P$, et pour tout $n \in \mathbb{N}^*$, P^n désigne le polynôme $\underbrace{P\times P\times \dots P}_{n \text{ facteurs}}$.

17.1.2 Indéterminée

On note X le polynôme $X = (0, 1, 0, 0, \dots) = (v_i)_{i\in\mathbf{N}}$.

- ▷ X^0 est le polynôme unité : $X^0 = 1 = (1, 0, 0, \dots)$.
- ▷ $X^1 = X = (0, 1, 0, 0, \dots)$.
- ▷ Déterminons X^2.

  On sait que $X^2 = X\times X = (c_i)_{i\in\mathbf{N}}$ où, pour tout $i \in \mathbf{N}$, $c_i = \sum_{k=0}^{i} v_k v_{i-k}$.

  $c_0 = v_0v_0 = 0$, $\quad c_1 = v_0v_1 + v_1v_0 = 0$, $\quad c_2 = v_0v_2 + v_1v_1 + v_2v_0 = 0+1+0 = 1$ et comme la suite définissant X est nulle au dela du rang 1, on sait qu'au dela du rang $1+1=2$ (cf définition du produit interne plus haut) les termes de la suite X^2 sont nuls.

  Ainsi, $X^2 = (0, 0, 1, 0, 0, \dots)$.
- ▷ Par récurrence, on peut montrer que pour tout $i \in \mathbb{N}$, X^i est le polynôme $(0, 0, \dots, 0, 1, 0, 0, \dots)$ où le 1 est en position i (en commençant la numérotation à 0 comme dans Python).

Soit $P = (a_i)_{i\in\mathbf{N}}$ un polynôme. On sait qu'il existe $n \in \mathbf{N}$ tel que $\forall i > n,\ a_i = 0$. Alors

$$\begin{aligned} P &= (a_0, a_1, \dots, a_n, 0, 0, \dots) \\ &= a_0.(1, 0, 0, \dots) + a_1.(0, 1, 0, \dots) + \dots + a_n(0, 0, \dots, 0, 1, 0, \dots) \\ &= a_0X^0 + a_1X^1 + a_2X^2 + \dots + a_nX^n \end{aligned}$$

17.2 Vocabulaire général

17.2.1 Polynôme, opérations

Définition 17.2 - Polynôme, indéterminée, coefficients.

Un polynôme est une expression de la forme $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, où n est un entier naturel, $a_0, a_1, \ldots, a_n \in \mathbf{K}$ sont les **coefficients** de P et X est l'**indéterminée**. Cette forme est appelée **forme développée réduite** du polynôme.
L'ensemble des polynômes d'indéterminée X à coefficients dans $\mathbf{K}$ est noté $\mathbf{K}[X]$.

ATTENTION

L'indéterminée est un objet à part entière. En particulier, ça n'est pas un nombre ! On n'écrira donc jamais « on pose $X = 5$ », cela n'a aucun sens, de même que « soit $X \in \mathbf{R}$ » (on n'a pas besoin d'introduire l'indéterminée quand on manipule des polynômes).

Remarque 17.3. On convient que $X^0 = 1$ et $X^1 = X$, de sorte que $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k$.

Définition 17.4 - Monôme, polynôme constant, polynôme nul.

On appelle **monôme** un polynôme de la forme $P = a_kX^k$, où $k \in \mathbf{N}$ et $a_k \in \mathbf{K}$.
On appelle **polynôme constant** un polynôme de la forme $P = a_0$, où $a_0 \in \mathbf{K}$.
On appelle **polynôme nul** le polynôme dont tous les coefficients sont nuls : $P = 0$.

Définition 17.5 - Égalité de polynômes, identification des coefficients.

Soit $P = \sum_{k=0}^{p} a_kX^k$ et $Q = \sum_{k=0}^{q} b_kX^k$ deux polynômes à coefficients dans $\mathbf{K}$. Quitte à rajouter des coefficients nuls, on peut écrire P et Q sous la forme $P = \sum_{k=0}^{n} a_kX^k$ et $Q = \sum_{k=0}^{n} b_kX^k$ où $n = \max(p, q)$. On a :

$$P = Q \iff \forall k \in [\![0, n]\!], \quad a_k = b_k.$$

Quand on utilise cette équivalence, on dit qu'on **identifie** les coefficients des deux polynômes.

Exercice d'application 17.6. Déterminer $(a, b, c) \in \mathbf{R}^3$ tel que $X^2 + X + 1 = a(X-1)^2 + b(X-1) + c$.

➥

Définition 17.7 - Opérations sur les polynômes.

Considérons $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$ deux polynômes à coefficients dans $\mathbf{K}$. Soit $\lambda \in \mathbf{K}$.

1. **Somme de deux polynômes**. Quitte à rajouter des coefficients nuls, on peut écrire P et Q sous la forme $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ où $n = \max(p, q)$. Alors, on définit la somme de P et Q par
$$P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k.$$
2. **Multiplication externe d'un polynôme par un scalaire de $\mathbf{K}$**. On a
$$\lambda P = \sum_{k=0}^{p} (\lambda a_k) X^k.$$
3. **Produit de deux polynômes**. On a
$$P \times Q = \sum_{k=0}^{p+q} c_k X^k \quad \text{où} \quad \forall k \in \mathbf{N},\ c_k = \sum_{\substack{j,\ell \in \mathbf{N} \\ j+\ell=k}} a_j b_\ell = \sum_{\ell=0}^{k} a_\ell b_{k-\ell}.$$

On peut vérifier que l'addition se « comporte bien » :

- l'addition est une opération associative (pour tous $P, Q, R \in \mathbf{K}[X]$, $(P+Q)+R = P+(Q+R)$) et commutative (pour tous $P, Q \in \mathbf{K}[X]$, $P+Q = Q+P$) ;
- le polynôme nul 0 est l'élément neutre de l'addition (pour tout $P \in \mathbf{K}[X]$, $0+P = P+0$) ;
- tout polynôme P possède un opposé noté $-P$ (pour tout $P \in \mathbf{K}[X]$, $P+(-P) = 0$) et l'on a $-P = (-1) \times P$.

On vérifie aussi facilement que c'est le cas pour le produit externe :

- $\forall \alpha, \beta \in \mathbf{K},\ \forall P \in \mathbf{K}[X],\ (\alpha+\beta) \cdot P = \alpha \cdot P + \beta \cdot P$;
- $\forall \alpha \in \mathbf{K},\ \forall P, Q \in \mathbf{K}[X],\ \alpha \cdot (P+Q) = \alpha \cdot P + \alpha \cdot Q$;
- $\forall \alpha, \beta \in \mathbf{K},\ \forall P \in \mathbf{K}[X],\ \alpha \cdot (\beta \cdot P) = (\alpha\beta) \cdot P$;
- $\forall P \in \mathbf{K}[X],\ 1 \cdot P = P$.

Enfin, les règles usuelles sur les produits sont valables pour les polynômes :

- la multiplication interne est associative (pour tous $P, Q, R \in \mathbf{K}[X]$, $(P \times Q) \times R = P \times (Q \times R)$) ;
- la multiplication interne est commutative (pour tous $P, Q \in \mathbf{K}[X]$, $P \times Q = Q \times P$). En effet, posons $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{k=0}^{q} b_k X^k$. Notons $PQ = \sum_{k=0}^{p+q} c_k X^k$ et $QP = \sum_{k=0}^{p+q} d_k X^k$. On a, par définition du produit, pour tout $i \in [\![0, p+q]\!]$,
$$c_i = \sum_{k=0}^{i} a_k b_{i-k} \underset{k'=i-k}{=} \sum_{k'=0}^{i} a_{i-k'} b_{k'} = \sum_{k'=0}^{i} b_{k'} a_{i-k'} = d_i$$
donc $P \times Q = Q \times P$.
- le polynôme unité $P = 1$ est élément neutre pour la multiplication interne (pour tout $P \in \mathbf{K}[X]$, $1 \times P = P$).
- la multiplication interne est distributive par rapport à l'addition : pour tous polynômes P, Q et R, on a $(P+Q) \times R = P \times R + Q \times R$ et $P \times (Q+R) = P \times Q + P \times R$.

Exemple 17.8. **1.** $(X^5 + 2X - i) + (X^3 - X^2 - X + i) = X^5 + X^3 - X^2 + X$.

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

3. $(X+1) \cdot (-iX^2 + X + 2) = -iX^3 + (1-i)X^2 + 3X + 2$.

Exercice d'application 17.9. Soit $P = X^2+1$ et $Q = X^3+X-2$. Donner la forme développée réduite de $-2P+3Q$ et de PQ.

➥

Définition 17.10 - Composition de polynômes.

Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes de $\mathbf{K}[X]$. On définit le **polynôme composé** $P \circ Q$, noté aussi $P(Q)$, par :

$$P \circ Q = P(Q) = \sum_{k=0}^{n} a_k Q^k.$$

Exemple 17.11. Si $P = X^2 + 2X - 1$ et $Q = X + 3$, alors

$$P \circ Q = (X+3)^2 + 2(X+3) - 1 = X^2 + 6X + 9 + 2X + 6 - 1 = X^2 + 8X + 14$$

et

$$Q \circ P = (X^2 + 2X - 1) + 3 = X^2 + 2X + 2.$$

Exemple 17.12 (☕). Soit $A = \sum_{k=0}^{n} a_k X^k$. On dit que A est un **polynôme pair** si $A(X) = A(-X)$. Montrons que si A est pair, alors tous les coefficients d'indice impair de A sont nuls.

On a

$$\sum_{k=0}^{n} a_k X^k = A(X) = A(-X) = \sum_{k=0}^{n} a_k (-X)^k.$$

donc, par identification, pour tout $k \in [\![0, n]\!]$, $a_k = (-1)^k a_k$. En particulier, pour tout $p \in \mathbf{N}$ tel que $2p+1 \in [\![0, n]\!]$, $a_{2p+1} = -a_{2p+1}$, donc $a_{2p+1} = 0$.

Remarque 17.13. Dans le cas particulier où $Q = X$, le polynôme $P \circ Q = P(Q) = P(X)$ est égal à P. On peut donc aussi bien utiliser la notation $P(X)$ que la notation P pour désigner le polynôme P.

Proposition 17.14 - Formule du binôme de Newton.

Soit $P, Q \in \mathbf{K}[X]$. Alors pour tout $n \in \mathbf{N}$,

$$(P+Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^{n-k} Q^k = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}.$$

Démonstration.
Identique à celle du chapitre sur les sommes. □

17.2.2 Degré d'un polynôme

Définition 17.15 - Degré d'un polynôme.

1. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul de $\mathbf{K}[X]$. L'ensemble $\{i \in [\![0,n]\!] \mid a_i \neq 0\}$ possède un plus grand élément d. Le nombre entier d est appelé le **degré** du polynôme P et noté $\deg(P)$. Le coefficient a_d est appelé le **coefficient dominant** de P.
2. Par convention, le degré du polynôme nul est $-\infty$ (et il ne possède pas de coefficient dominant).

En particulier, le degré est un élément de $\mathbf{N} \cup \{-\infty\}$.

Démonstration.
Si P est un polynôme non nul, $\{i \in \mathbf{N} \mid a_i \neq 0\}$ est une partie non vide de $\mathbf{N}$ (car P est supposé non nul), donc il possède un plus grand élément. □

Exemple 17.16. Le degré de $3X^5 - X + 1$ est 5 et son coefficient dominant est 3. Le degré de X est 1 et son coefficient dominant est 1. Le degré de 3 est 0 et son coefficient dominant est 3. Le degré de 0 est $-\infty$ et il ne possède pas de coefficient dominant.

Exercice d'application 17.17. Soit $n \in \mathbf{N}^\star$. Déterminer le degré et le coefficient dominant de $P = (X^2+1)^n - (X^2-1)^n$.

➥

Définition 17.18 - Polynôme unitaire.

Un polynôme non nul est dit **unitaire** si son coefficient dominant vaut 1.

Proposition 17.19 - Degré et opérations.

Soit P et Q deux polynômes de $\mathbf{K}[X]$ et $\lambda \in \mathbf{K}$ un scalaire non nul.

1. **(a)** $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$.
   (b) Si $\deg(P) \neq \deg(Q)$ alors $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$.
   (c) Si P et Q ne sont pas nuls, si $\deg(P) = \deg(Q)$ et que les coefficients dominants de P et Q ne sont pas opposés, alors $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big) = \deg(P) = \deg(Q)$.
2. $\deg(P \times Q) = \deg(P) + \deg(Q)$.
3. $\deg(\lambda P) = \deg(P)$ si $\lambda \neq 0$.

(toutes les opérations ont lieu dans $\mathbf{N} \cup \{-\infty\}$.)

Démonstration.

Exemple 17.20. Soit $P = 3X^2 + X + 1$, $Q = -X^3 + 1$ et $R = X^3 + X^2 + 1$. Alors, $\deg(P) = 2$, $\deg(Q) = 3$ et $\deg(R) = 3$. De plus, $P + Q = -X^3 + 3X^2 + X + 2$, $Q + R = X^2 + 2$ et $P \times Q = -3X^5 - X^4 - X^3 + 3X^2 + X + 1$. On constate que $\deg(P+Q) = 3 = \max\big(\deg(P), \deg(Q)\big)$, $\deg(Q+R) = 2 < \max\big(\deg(P), \deg(Q)\big)$ et $\deg(P \times Q) = 5 = \deg(P) + \deg(Q)$.

Remarque 17.21. Pour tout $P \in \mathbf{K}[X]$, $\deg(P \times 0) = \deg(P) + \deg(0) = \deg(P) - \infty = -\infty$, donc la convention $\deg(0) = -\infty$ est bien pratique pour que la formule du degré d'un produit soit vraie pour tous les polynômes !

Remarque 17.22. Soit P et Q tels que $P \times Q = 1$. Alors $P \neq 0$ et $Q \neq 0$ donc $\deg(P) \geqslant 0$ et $\deg(Q) \geqslant 0$. Or $0 = \deg(P \times Q) = \deg(P) + \deg(Q)$ donc $\deg(P) = \deg(Q) = 0$. Donc P et Q sont des polynômes constants non nuls. Donc si un polynôme P possède un inverse pour la multiplication, alors P est un polynôme constant non nul. Réciproquement, tout polynôme constant non nul possède un inverse pour la multiplication (si $P = a$ où $a \in \mathbf{K}$ et $a \neq 0$, alors $P \times \dfrac{1}{a} = 1$). Les polynômes **inversibles** sont donc les polynômes constants non nuls.

Cela signifie qu'un objet comme $\dfrac{1}{X^2 + 3X + 9}$ n'est pas un polynôme.

Proposition 17.23 - Degré d'une composée.

Soit P et Q deux polynômes de $\mathbf{K}[X]$. Si $\deg(Q) \geqslant 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Démonstration.

Méthode 17.24. *Résolution d'équations dont l'inconnue est un polynôme*

Si on cherche un ensemble de polynômes vérifiant une certaine contrainte, l'utilisation du degré peut permettre de restreindre le champ de recherche (dans un raisonnement par analyse-synthèse par exemple). Si on connaît le degré du polynôme cherché (ou une majoration du degré), on peut introduire des coefficients !

Exercice d'application 17.25. Déterminer les couples (A, B) de polynômes tels que $B^2 = X \times A^2$.

➥

Exercice d'application 17.26. Déterminer les polynômes $P \in \mathbf{R}[X]$ vérifiant $P \circ P = P$.

➥

Théorème 17.27 - Produit nul de polynômes.

Soit $A, B \in \mathbf{K}[X]$.

$$AB = 0 \iff A = 0 \text{ ou } B = 0.$$

Démonstration.

Remarque 17.28. En particulier, le produit de deux polynômes non nul est non nul.

Exercice d'application 17.29. Soit $(P,Q,R) \in \mathbf{K}[X]^3$. Montrer que $PR = PQ \iff P = 0$ ou $R = Q$.

➥

Notation 17.30. Soit $n \in \mathbf{N}$. On note $\mathbf{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$ de degré inférieur ou égal à n :

$$\mathbf{K}_n[X] = \{P \in \mathbf{K}[X] \mid \deg(P) \leqslant n\} = \left\{ \sum_{k=0}^{n} a_k X^k \ : \ (a_0, a_1, \dots, a_n) \in \mathbf{K}^{n+1} \right\}.$$

Puisque $\deg(0) = -\infty$, on a $0 \in \mathbf{K}_n[X]$.

Exemple 17.31. Les polynômes de degré 0 sont les polynômes constants non nuls. Les polynômes de $\mathbf{K}_0[X]$ sont tous les polynômes constants.

ATTENTION

L'ensemble des trinômes n'est pas $\mathbf{K}_2[X]$. L'ensemble $\mathbf{K}_2[X]$ est constitué des polynômes constants (de degré 0 ou $-\infty$), des polynômes affines (de degré 1) et des trinômes (de degré 2).

Proposition 17.32 - Stabilité de $\mathbf{K}_n[X]$ par somme et par produit externe.

Soit n un entier naturel. L'ensemble $\mathbf{K}_n[X]$ est stable par addition et multiplication externe par un scalaire, autrement dit :

$$\forall P, Q \in \mathbf{K}_n[X],\ \forall \lambda \in \mathbf{K}, \quad P + Q \in \mathbf{K}_n[X] \text{ et } \lambda P \in \mathbf{K}_n[X].$$

Démonstration.
Soit P et Q deux polynômes de $\mathbf{K}_n[X]$ et $\lambda \in \mathbf{K}$. On a :

$$\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big) \leqslant n$$

donc $P + Q \in \mathbf{K}_n[X]$. De plus, si $\lambda \neq 0$, $\deg(\lambda P) = n$ et si $\lambda = 0$, $\deg(\lambda P) = -\infty$. Dans tous les cas, $\lambda P \in \mathbf{K}_n[X]$. □

Remarque 17.33. $\mathbf{K}_n[X]$ n'est pas stable par produit en général. Il est stable par produit si et seulement si $n = 0$.

17.2.3 Fonctions polynomiales

Définition 17.34 - Fonction polynomiale.

1. On appelle **fonction polynomiale** sur $\mathbf{K}$ toute application f de $\mathbf{K}$ dans $\mathbf{K}$ telle qu'il existe un entier n et des éléments $a_0, \dots, a_n$ de $\mathbf{K}$ tels que

$$\forall x \in \mathbf{K}, \quad f(x) = \sum_{i=0}^{n} a_i x^i.$$

2. Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme à coefficient dans $\mathbf{K}$. On appelle **fonction polynomiale associée à** P la fonction $\widetilde{P} : x \longmapsto \sum_{i=0}^{n} a_i x^i$.

Remarque 17.35. Si f est une fonction polynomiale, il existe un polynôme P de $\mathbf{K}[X]$ telle que $f = \widetilde{P}$. Nous verrons plus loin que le polynôme P est unique (car on utilise $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$).

Dans toute la suite, si P désigne un polynôme, $\widetilde{P}$ sera sa fonction polynomiale associée.

Définition 17.36 - Évaluation d'un polynôme en un nombre.

On dit qu'on **évalue** un polynôme $P \in \mathbf{K}[X]$ en $x_0 \in \mathbf{K}$ lorsqu'on calcule $\widetilde{P}(x_0)$.

ATTENTION

X n'est pas un nombre (nous l'avons déjà dit !). On n'écrira donc pas « posons $X = 1$ » mais plutôt « on évalue le polynôme en 1 ».

17.2.4 Méthode algorithmique de Hörner pour l'évaluation des polynômes

Dans ce paragraphe, on s'intéresse à l'évaluation d'un polynôme P en un point a. Par exemple, si $P = 10X^4 - 7X^3 + 5X^2 + 3X - 13$ et que l'on veut évaluer P en $a = 2$, la méthode naïve consiste à calculer

$$\widetilde{P}(2) = 10 \times 2 \times 2 \times 2 \times 2 - 7 \times 2 \times 2 \times 2 + 5 \times 2 \times 2 + 3 \times 2 - 13 = 117$$

ce qui nécessite 10 multiplications et 4 additions/soustractions. En généralisant cette méthode à un polynôme quelconque, on arrive à une complexité en $\mathrm{O}(n^2)$ où n est le degré du polynôme. La fonction suivante permet d'évaluer un polynôme en un point avec cette méthode, où les coefficient du polynôme P sont stockés dans une liste L (selon le degré décroissant).

Script Python

```
def eval_naive(P: list, a: float) -> float:
    degre = len(P)-1
    valeur = P[degre]
    for i in range(degre):
        valeur = valeur + P[degre-i-1] * a**(i+1)
    return valeur
```

On peut l'utiliser pour vérifier le calcul précédent :

Console

```
>>> L = [10, -7, 5, 3, -13]
>>> eval_naive(L, 2)
117
```

La **méthode de Hörner** permet de réduire le nombre de calculs nécessaires. On peut réécrire le calcul précédent de la manière suivante :

$$\widetilde{P}(2) = (((10 \times 2 - 7) \times 2 + 5) \times 2 + 3) \times 2 - 13.$$

Ici, il n'y a que 4 multiplications et 4 additions. On peut généraliser cette idée à un polynôme de degré n et on obtient alors un calcul qui ne nécessite que n additions et n multiplications (donc une complexité en $\mathrm{O}(n)$, ce qui est nettement mieux !).

Script Python

```
def horner(P: list, a: float) -> float:
    degre = len(P)-1
    valeur = P[0]
    for i in range(1, degre+1):
        valeur = valeur*a + P[i]
    return valeur
```

On peut vérifier que l'algorithme fonctionne sur l'exemple étudié avant :

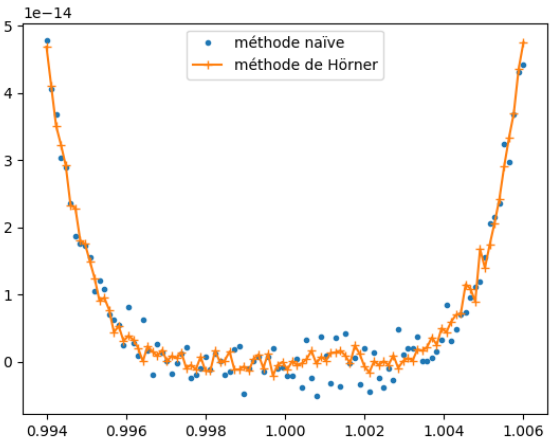
CONSOLE

```
>>> L = [10, -7, 5, 3, -13]
>>> horner(L, 2)
117
```

Outre l'intérêt de rapidité, la méthode de Hörner génère moins d'erreurs de calcul. On représente ci-après le graphe de la fonction $x \longmapsto (1-x)^6$ obtenu avec la méthode naïve et la méthode de Hörner. Aucune des deux méthodes ne donne une représentation correcte (on devrait voir apparaître une courbe ressemblant à une parabole), mais la méthode de Hörner est plus proche de la réalité.

SCRIPT PYTHON

```
P = [1, -6, 15, -20, 15, -6, 1]
n_points = 100
x = np.linspace(0.994, 1.006,
   n_points)
y_naive = np.zeros(n_points)
y_horner = np.zeros(n_points)
for k in range(n_points):
    y_naive[k] = eval_naive(P, x[k])
    y_horner[k] = horner(P, x[k])
plt.plot(x, y_naive, '.', label='
   méthode naïve')
plt.plot(x, y_horner, '-+', label='
   méthode de Hörner')
plt.legend()
plt.show()
```



17.2.5 Dérivées

Définition 17.37 - Dérivée formelle.

Pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ de $\mathbf{K}[X]$, on définit son **polynôme dérivé** P' par

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

ATTENTION

Le polynôme dérivé est une construction abstraite et n'a donc aucun rapport avec le taux d'accroissement !

Proposition 17.38 - Opérations sur la dérivation polynomiale.

Soit $P, Q \in \mathbf{K}[X]$ et $\lambda \in \mathbf{K}$.

1. $(\lambda P + Q)' = \lambda P' + Q'$; **2.** $(PQ)' = P'Q + PQ'$; **3.** $(P \circ Q)' = Q' \times (P' \circ Q)$.

Démonstration.

Notons $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ (quitte à choisir des coefficients nuls).

1. $\lambda P+Q=\sum_{k=0}^{n}(\lambda a_k+b_k)X^k$, donc

$$\begin{aligned}(\lambda P+Q)'&=\sum_{k=1}^{n}k(\lambda a_k+b_k)X^{k-1} && \text{d'après la définition de la dérivée}\\ &=\lambda\sum_{k=1}^{n}a_kX^{k-1}+\sum_{k=1}^{n}b_kX^{k-1} && \text{par linéarité de la somme}\\ &=\lambda P'+Q' && \text{d'après la définition de la dérivée}\end{aligned}$$

2. Le coefficient de degré k de $(PQ)'$ vaut $(k+1)\sum_{i=0}^{k+1}a_ib_{k+1-i}$ et celui de $P'Q+PQ'$ vaut $\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j}+\sum_{k=0}^{k}a_i(k-i+1)b_{k-i+1}$. Ces coefficients sont égaux car :

$$\begin{aligned}\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j}+\sum_{k=0}^{k}a_i(k-i+1)b_{k-i+1}&\sum_{i=1}^{k+1}ia_ib_{k+1-i}+\sum_{i=0}^{k}a_i(k-i+1)b_{k-i+1} && \text{avec } i=j+1\\ &=\sum_{i=0}^{k+1}ia_ib_{k+1-i}+\sum_{i=0}^{k+1}a_k(k-i+1)b_{k-i+1}b_{k-i+1}\\ &=\sum_{i=0}^{k+1}(ia_ib_{k+1-i}+a_i(k-i+1)b_{k+1-i})\\ &=(k+1)\sum_{i=0}^{k+1}a_ib_{k+1-i}.\end{aligned}$$

3. Par définition, $P\circ Q=\sum_{k=0}^{n}a_kQ^k$, donc par récurrence avec le point **1.**, $(P\circ Q)'=\sum_{k=0}^{n}a_k(Q^k)'$. Puis, par récurrence à partir du point **2.**, $(Q^k)'=kQ'Q^{k-1}$ pour tout $k\in\mathbf{N}$. Ainsi, $(P\circ Q)'=\sum_{k=1}^{n}a_k\times kQ'Q^{k-1}=Q'\times(P'\circ Q)$. □

On peut itérer le processus de dérivation. Soit $P\in\mathbf{K}[X]$, $\ell\in\mathbf{N}$. Comme dans le cas des fonctions, on utilise alors les notations P'', P''' et $P^{(\ell)}$ pour désigner respectivement les dérivées seconde, troisième et ℓ-ième de P. Plus précisément, on convient que $P^{(0)}=P$ et

$$\forall\ell\in\mathbf{N},\quad P^{(\ell+1)}=\left(P^{(\ell)}\right)'=\left(P'\right)^{(\ell)}.$$

La dérivée ℓ-ième est encore linéaire :

$$\forall\ell\in\mathbf{N},\ \forall P,Q\in\mathbf{K}[X],\quad(\lambda P+Q)^{(\ell)}=\lambda P^{(\ell)}+Q^{(\ell)}.$$

On peut aussi généraliser la formule de dérivation d'un produit.

Proposition 17.39 - Formule de Leibniz.

Pour tous polynômes P et Q de $\mathbf{K}[X]$ et tout entier naturel n, on a

$$(P\times Q)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}.$$

Démonstration.

Proposition 17.40 - Degré du polynôme dérivé, du polynôme dérivé ℓ fois.

Soit $P \in \mathbf{K}[X]$. On a

$$\deg(P') = \begin{cases} \deg(P) - 1 & \text{si} \quad \deg(P) \geqslant 1 \\ -\infty & \text{si} \quad \deg(P) < 1 \end{cases}$$

Plus généralement, si $\ell \in \mathbf{N}$,

$$\deg\left(P^{(\ell)}\right) = \begin{cases} \deg(P) - \ell & \text{si} \quad \deg(P) \geqslant \ell \\ -\infty & \text{si} \quad \deg(P) < \ell \end{cases}$$

Démonstration.

Notons $d = \deg(P)$ et $P = \sum_{k=0}^{d} a_k X^k$.

- Si $d \leqslant 0$, $P' = 0$ d'où $\deg(P) = -\infty$. Supposons $d \geqslant 1$. On a $P' = \sum_{k=1}^{d} k a_k X^{k-1} = d a_d X^{d-1} + \dots$ avec $d a_d \neq 0$, donc $\deg(P') = d - 1$.
- ◦ Si $P \neq 0$, le résultat est clair. Pour tout $\ell \in [\![0, \deg(P)]\!]$, on note H_ℓ : « $\deg(P^{(\ell)}) = \deg(P) - \ell$ » (remarque : on a distingué le cas $P = 0$ pour que l'écriture $[\![0, \deg(P)]\!]$ ait un sens).
  On a $P^{(0)} = P$, donc H_0 est vraie. Soit $\ell \in [\![0, \deg(P) - 1]\!]$ tel que H_ℓ soit vraie. Le polynôme $\deg(P^{(\ell)})$ a pour degré $\deg(P) - \ell \geqslant 1$ donc il n'est pas constant et l'on a

$$\deg(P^{(\ell+1)}) = \deg\left(\left(P^{\ell}\right)'\right) = \deg(P^{(\ell)}) - 1 = \deg(P) - (\ell + 1)$$

donc la propriété $H_{\ell+1}$ est vraie.
Le principe de récurrence finie assure que le résultat est vrai pour tout $\ell \in [\![0, \deg(P)]\!]$.

- En particulier, H_d assure que $P^{(\deg(P))}$ est un polynôme constant donc d'après le premier point, les dérivées suivantes de P sont toutes nulles. □

Exercice d'application 17.41. Donner les dérivées successives de $P = X^3 + X + 1$.

➥

Proposition 17.42 - Dérivée ℓ-ième de $(X-a)^n$.

Soit $n \in \mathbf{N}$, $\ell \in \mathbf{N}$, $a \in \mathbf{K}$.

$$((X-a)^n)^{(\ell)} = \begin{cases} n(n-1)\cdots(n-\ell+1)(X-a)^{n-\ell} = \dfrac{n!}{(n-\ell)!}(X-a)^{n-\ell} & \text{si} \quad \ell \in [\![0,n]\!] \\ 0 & \text{si} \quad \ell \geqslant n+1 \end{cases}$$

Démonstration.

Exemple 17.43. Si $P = \sum_{k=0}^{n} a_k X^k$, alors $P'' = \sum_{k=2}^{n} k(k-1)a_k X^{k-2}$.

Remarque 17.44 (*Lien avec la fonction polynomiale*). La formule donnée pour dériver un polynôme P permet de remarquer que, lorsque $\mathbf{K} = \mathbf{R}$, la fonction polynomiale associée à P' est la dérivée de la fonction polynomiale associée à P :

$$\forall x \in \mathbf{R}, \quad \widetilde{P'}(x) = \left(\widetilde{P}\right)'(x).$$

Il n'est donc pas surprenant que la dérivée d'un polynôme respecte les mêmes règles que la dérivée d'une fonction.

17.2.6 Formule de Taylor

Théorème 17.45 - Formule de Taylor polynomiale.

Soit $n \in \mathbf{N}$, $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{K}_n[X]$ (il est important de noter que n est le degré du polynôme ici).

1. Formule de Taylor en 0. $P = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(0)}{k!} X^k$.
2. Formule de Taylor en $a \in \mathbf{K}$. $P = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(a)}{k!} (X-a)^k$.

Démonstration.

Corollaire 17.46 - Expression des coefficients d'un polynôme en fonction des dérivées.

Soit $n \in \mathbf{N}$, $P = \sum_{k=0}^{n} a_k X^k \in \mathbf{K}[X]$,

$$\forall\, k \in [\![0, n]\!], \quad a_k = \frac{\widetilde{P}^{(k)}(0)}{k!}.$$

Démonstration.
Ce résultat est obtenu dans la démonstration précédente (point **1.**). On peut aussi le déduire de la proposition précédente en identifiant les coefficients des polynômes $P = \sum_{k=0}^{n} a_k X^k$ et $P = \sum_{k=0}^{n} \frac{\widetilde{P}^{(k)}(0)}{k!} X^k$. □

17.3 Arithmétique des polynômes

17.3.1 Diviseurs et multiples

Définition 17.47 - Diviseur, multiple.

Soit A et B deux polynômes. On dit que A est un **diviseur** de B ou que A **divise** B ou encore que B est un **multiple** de A si et seulement si il existe un polynôme K tel que $B = KA$.
On note alors $A \mid B$.

Exemple 17.48 (♥).
1. Pour tout $A \in \mathbf{K}[X]$, $1 \mid A$ et $A \mid 0$.
2. Si $0 \mid A$, alors $A = 0$.
3. Si $\lambda \in \mathbf{K}^\star$, alors $\lambda \mid A$.

Exercice d'application 17.49. Montrer que $X - 1$ et $2X^2 - 2$ divisent $X^2 - 1$.

➥

Exercice d'application 17.50. Montrer que pour tout $(a, n) \in \mathbf{K} \times \mathbf{N}^\star$, $X - a \mid X^n - a^n$.

➥

Proposition 17.51 - Principales propriétés de la divisibilité.

Soit $A, B, C, D \in \mathbf{K}[X]$.
1. **Réflexivité**. $A \mid A$.
2. **Transitivité**. Si $A \mid B$ et si $B \mid C$, alors $A \mid C$.
3. $A \mid B$ et $B \mid A$ si et seulement s'il existe $\lambda \in \mathbf{K}^\star$ tel que $A = \lambda B$.
4. **Combinaisons linéaires**. Si $D \mid A$ et $D \mid B$, alors $D \mid (AU + BV)$ pour tous $U, V \in \mathbf{K}[X]$.
5. **Produit**. Si $A \mid B$ et $C \mid D$, alors $AC \mid BD$. En particulier, $A^k \mid B^k$ pour tout $k \in \mathbf{N}$.

Démonstration.

Proposition 17.52 - Lien entre divisibilité et degré.

Soit P, Q deux polynômes avec $Q \neq 0$. Si $P \mid Q$, alors $\deg(P) \leqslant \deg(Q)$.

Démonstration.

Exemple 17.53. Le polynôme $X^3 - X + 1$ ne peut pas diviser $X + 1$ car $\deg(X^3 - X + 1) > \deg(X + 1)$.

17.3.2 Division euclidienne de deux polynômes

Lemme 17.54 - Diminuer le degré d'un polynôme.

Soit $A, B \in \mathbf{K}[X]$ deux polynômes non nuls. Notons $n = \deg(A)$, $d = \deg(B)$ et supposons $n \geqslant d$. Posons $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{d} b_k X^k$.
Alors le polynôme $A_1 = A - \dfrac{a_n}{b_d} X^{n-d} B$ est de degré strictement inférieur à celui de A.

Démonstration.
Les polynômes A et $-\dfrac{a_n}{b_d} X^{n-d} B$ sont de même degré. De plus, le coefficient dominant de A est a_n et celui de $-\dfrac{a_n}{b_d} X^{n-d} B$ est $-a_n$, donc $\deg\left(A - \dfrac{a_n}{b_d} X^{n-d} B\right) < \deg(A)$. □

Exemple 17.55. Considérons $A = X^4 + 3X^2 - 5X + 1$ et $B = X^2 - 3X$.

1. $A_1 = A - X^2 B = (X^4 - 3X^2 - 5X + 1) - X^2(X^2 - 3X) = 3X^3 + 3X^2 - 5X + 1$.
2. On peut itérer le processus : $A_2 = A_1 - 3XB = 3X^3 + 3X^2 - 5X + 1 - 3X(X^2 - 3X) = 12X^2 - 5X + 1$.
3. Poursuivons : $A_3 = A_2 - 12B = 12X^2 - 5X + 1 - 12(X^2 - 3X) = 31X + 1$.

On ne peut plus continuer. En résumé, on a obtenu $A - (X^2 + 3X + 12)B = 31X + 1$, c'est-à-dire

$$A = (X^2 + 3X + 12)B + (31X + 1).$$

Théorème 17.56 - Division euclidienne.

Soit $A, B \in \mathbf{K}[X]$ avec $B \neq 0$.
Il existe un unique couple $(Q, R) \in \mathbf{K}[X]^2$ tel que $A = QB + R$ et $\deg(R) < \deg(B)$.
Cette écriture est la **division euclidienne** de A par B, avec Q le **quotient** et R le **reste**.

Démonstration.

Exemple 17.57. La démonstration assure que si $\deg(A) < \deg(B)$, la division euclidienne de A par B est immédiate puisqu'on a $A = 0 \times B + A$ (le quotient est le polynôme nul et le reste est A). Par exemple, le quotient de la division euclidienne de X par X^2+1 est 0 et le reste est 0, puisque $X = 0 \times (X^2+1) + X$.

La démonstration est constructive : elle donne une méthode pour obtenir la division euclidienne d'un polynôme par un autre. Dans l'Exemple 17.55, la méthode est mise en place. En pratique, on pose la division euclidienne (comme on le fait pour des entiers !) pour gagner de la place.

Méthode 17.58. *Poser une division euclidienne*

On peut poser la division en faisant disparaître les monômes de plus haut degré successivement. Par exemple, considérons $A = X^4 + 3X^2 - 5X + 1$ et $B = X^2 - 3X$ et détaillons le calcul (qui a déjà été fait dans l'Exemple 17.55).

1. On soustrait à A un multiple de B de sorte que X^4 disparaisse.

$$\begin{array}{rrr|l} X^4 & +3X^2 & -5X+1 & X^2-3X \\ \cline{4-4} -X^4+3X^3 & & & X^2 \\ \cline{1-1} 3X^3 & +3X^2 & & \end{array}$$

On note $A_1 = 3X^3 + 3X^2$ le nouveau polynôme obtenu.

2. On soustrait à A_1 un multiple de B de sorte que $3X^3$ disparaisse.

$$\begin{array}{rrr|l} X^4 & +3X^2 & -5X+1 & X^2-3X \\ \cline{4-4} -X^4+3X^3 & & & X^2+3X \\ \cline{1-1} 3X^3 & +3X^2 & & \\ -3X^3 & +9X^2 & & \\ \cline{2-2} & 12X^2 & -5X & \end{array}$$

On note $A_2 = 12X^2 - 5X$ le nouveau polynôme obtenu.

3. On soustrait à A_2 un multiple de B de sorte que $12X^2$ disparaisse.

$$\begin{array}{rrr|l} X^4 & +3X^2 & -5X+1 & X^2-3X \\ \cline{4-4} -X^4+3X^3 & & & X^2+3X+12 \\ \cline{1-1} 3X^3 & +3X^2 & & \\ -3X^3 & +9X^2 & & \\ \cline{2-2} & 12X^2 & -5X & \\ & -12X^2 & +36X & \\ \cline{3-3} & & 31X+1 & \end{array}$$

▪ Le reste est de degré 1 donc on ne peut plus poursuivre. Finalement, $A = B(X^2+3X+12)+(31X+1)$.

Exemple 17.59. **1.** Effectuons la division euclidienne de $A = 2X^4 - 3X^2 + 5$ par $B = X^2 - 2X + 3$.

$$\begin{array}{rrr|l}
2X^4 & -3X^2 & +5 & X^2-2X+3 \\
\cline{4-4}
-2X^4+4X^3-6X^2 & & & 2X^2+4X-1 \\
\cline{1-3}
4X^3-9X^2 & & & \\
-4X^3+8X^2-12X & & & \\
\cline{1-3}
-X^2-12X+5 & & & \\
X^2-2X+3 & & & \\
\cline{1-3}
-14X+8 & & &
\end{array}$$

2. Effectuons la division euclidienne de $A = 2X^5 + 5X^3 + 6X + 2$ et $B = X^2 + X + 2$.

$$\begin{array}{rrrr|l}
2X^5 & +5X^3 & +6X+2 & & X^2+X+2 \\
\cline{5-5}
-2X^5-2X^4-4X^3 & & & & 2X^3-2X^2+3X+1 \\
\cline{1-3}
-2X^4+X^3 & & & & \\
2X^4+2X^3+4X^2 & & & & \\
\cline{1-3}
3X^3+4X^2+6X & & & & \\
-3X^3-3X^2-6X & & & & \\
\cline{1-3}
X^2 & +2 & & & \\
-X^2-X-2 & & & & \\
\cline{1-3}
-X & & & &
\end{array}$$

Exercice d'application 17.60. Dans chaque cas, poser la division euclidienne de A par B.

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

➥

Remarque 17.61. Soit $A, B \in \mathbf{R}[X]$. S'il existe $Q, R \in \mathbf{C}[X]$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$, alors $Q, R \in \mathbf{R}[X]$. En particulier, si $A \mid B$ dans $\mathbf{C}[X]$ et $A, B \in \mathbf{R}[X]$, alors $A \mid B$ dans $\mathbf{R}[X]$.

Proposition 17.62 - Lien entre divisibilité et reste par la division euclidienne.

Soit $A, B \in \mathbf{K}[X]$ avec $B \neq 0$. Notons R le reste de la division euclidienne de A par B.

$$B \mid A \iff R = 0.$$

Démonstration.
Via le théorème de la division euclidienne, il existe $Q, R \in \mathbf{K}[X]$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$.

$$R = 0 \iff A = BQ \iff B \mid A.$$

□

Exercice d'application 17.63. Montrer que $X^3 + 7X^2 - 9X + 1$ est divisible par $X - 1$.

➥

17.4 Racines d'un polynôme

17.4.1 Définitions

Définition 17.64 - Racine d'un polynôme.

Soit $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$. On dit que α est une **racine** de P lorsque $(X - \alpha) \mid P$.

Proposition 17.65 - Évaluation d'un polynôme en une racine.

Soit $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$. Le reste de la division euclidienne de P par $(X - \alpha)$ est $\widetilde{P}(\alpha)$. En particulier, α est racine de P si et seulement si $\widetilde{P}(\alpha) = 0$.

Démonstration.

Définition 17.66 - Multiplicité d'une racine.

Soit $P \in \mathbf{K}[X]\setminus\{0\}$, $\alpha \in \mathbf{K}$, $n \in \mathbf{N}^\star$. On dit que α est une racine de **multiplicité** n de P lorsque les deux conditions suivantes sont satisfaites :

(a) $(X-\alpha)^n \mid P$;

(b) $(X-\alpha)^{n+1}$ ne divise pas P.

Cela équivaut à dire qu'il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-\alpha)^n Q$ et $\widetilde{Q}(\alpha) \neq 0$.

Démonstration.
Supposons que α est racine de P de multiplicité n. Puisque $(X-\alpha)^n \mid P$, on obtient qu'il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-\alpha)^n Q$. De plus, $X-\alpha$ ne divise pas Q puisque $(X-\alpha)^{n+1}(\alpha)$ ni divise pas P, ainsi $\widetilde{Q}(\alpha) \neq 0$.
La réciproque est laissée en exercice. □

Définition 17.67 - Racine simple, multiple, double, triple.

Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$. On dit que α est une racine

- **simple** lorsque α est une racine de multiplicité 1 de P.
- **multiple** lorsque α est une racine de multiplicité supérieure ou égale à 2 de P. Plus particulièrement, si une racine de multiplicité 2 (resp. 3) est dite **racine double** (resp. **triple**).

Exemple 17.68.

1. Soit $(a,b,c) \in \mathbf{K}^\star \times \mathbf{K}^2$. $P = aX^2+bX+c$ a une racine double si et seulement si $b^2-4ac = 0$.

2. Soit $P = 2X^4-7X^3+6X^2+X-2$. On a $\widetilde{P}(1) = 0$, donc 1 est racine de P et, après division euclidienne, $P = (X-1)(2X^3-5X^2+X+2)$. Or 1 est racine de $2X^3-5X^2+X+2$, donc on obtient via une division euclidienne $P = (X-1)^2(2X^2-3X-2)$. Enfin, 1 n'est pas racine de $2X^2-3X-2$. En résumé, $(X-1)^2 \mid P$ et $(X-1)^3$ ne divise pas P, donc 1 est racine double de P.

Proposition 17.69 - Caractérisation de la multiplicité à l'aide des dérivées.

Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$, $n \in \mathbf{N}^\star$. α est une racine de multiplicité n de P si et seulement si

$$\widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = \ldots = \widetilde{P}^{(n-1)}(\alpha) = 0 \quad \text{et} \quad \widetilde{P}^{(n)}(\alpha) \neq 0.$$

Démonstration.

Remarque 17.70. Soit $P \in \mathbf{K}[X]$, $\alpha \in \mathbf{K}$, $n \in \mathbf{N}^\star$. α est une racine de multiplicité au moins n si et seulement si

$$(X-\alpha)^n \mid P \quad \text{ou} \quad \widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = ... = \widetilde{P}^{(n-1)}(\alpha) = 0.$$

Exemple 17.71. Considérons $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$. On a $\widetilde{P}(1) = \widetilde{P'}(1) = \widetilde{P''}(1) = 0$. Donc 1 est racine de P de multiplicité au moins 3. Notons que puisque $\widetilde{P^{(3)}}(1) = 6$, 1 est racine de multiplicité 3.

17.4.2 Factorisation d'un polynôme

Proposition 17.72 - Caractérisation de plusieurs racines multiples.

Soit $r \in \mathbf{N}^\star$, $P \in \mathbf{K}[X]$, $\alpha_1, ..., \alpha_r \in \mathbf{K}$ des scalaires deux à deux distincts et $m_1, ..., m_r \in \mathbf{N}^\star$. Les assertions suivantes sont équivalentes.

(i) pour tout $i \in [\![1, r]\!]$, α_i est racine de P de multiplicité au moins m_i ;

(ii) $\prod_{k=1}^{r} (X-\alpha_k)^{m_k} \mid P$.

Démonstration.

- **(i) $\Longrightarrow$ (ii)**. Pour tout $r \in \mathbf{N}^\star$, on pose H_r : « pour tout $\alpha_1, \ldots, \alpha_r \in \mathbf{K}$, si $\alpha_1, ..., \alpha_r$ sont des racines distinctes de multiplicités respectives au moins égales à $m_1, \ldots, m_r$, alors $\prod_{k=1}^{r} (X-\alpha_k)^{m_k} \mid P$ ».

  Soit α_1 une racine de multiplicité au moins m_1 de P. Alors $(X-\alpha_1)^{m_1}$ divise P par définition de la multiplicité, donc H_1 est vraie.

Soit $r \in \mathbf{N}^\star$ tel que H_r soit vraie. Soit $\alpha_1, ..., \alpha_{r+1}$ des racines distinctes de P de multiplicités respectives au moins égales à $m_1, ..., m_{r+1}$. Via H_r, il existe $Q \in \mathbf{K}[X]$ tel que $P = \prod_{k=1}^{r}(X-\alpha_k)^{m_k} Q$. Alors

$$\widetilde{P}(\alpha_{r+1}) = \underbrace{\prod_{k=1}^{r}(\alpha_{r+1}-\alpha_k)^{m_k}}_{\neq 0 \text{ car les racines sont distinctes}} \widetilde{Q}(\alpha_{r+1}).$$

Or $\widetilde{P}(\alpha_{r+1}) = 0$ car α_{r+1} est racine de P, donc $\widetilde{Q}(\alpha_{r+1}) = 0$, ce qui montre que α_{r+1} est une racine de Q. Notons m l'ordre de multiplicité de α_{r+1} en tant que racine de Q. On sait alors qu'il existe $Q_1 \in \mathbf{K}[X]$ tel que

$$Q = (X-\alpha_{r+1})^m Q_1 \quad \text{et} \quad \widetilde{Q_1}(\alpha_{r+1}) \neq 0.$$

Ensuite,

$$P = (X-a_{r+1})^m \underbrace{Q_1 \prod_{k=1}^{r}(X-\alpha_k)^{m_k}}_{=Q_2}.$$

Or $\widetilde{Q_2}(\alpha_{r+1}) = \widetilde{Q_1}(\alpha_{r+1}) \times \prod_{k=1}^{r}(\alpha_{r+1}-\alpha_k)^{m_k} \neq 0$. Ainsi α_{r+1} est racine de P d'ordre de multiplicité exactement m. Par suite, $m_{r+1} \leqslant m$ (puisque m_{r+1} est inférieure ou égale à la multiplicité par définition), donc $(X-\alpha_{r+1})^{m_{r+1}} \mid (X-\alpha_{r+1})^m$, puis par produit

$$\prod_{k=1}^{r+1}(X-\alpha_k)^{m_k} \mid (X-\alpha_{r+1})^r \prod_{k=1}^{m}(X-\alpha_k)^{m_k}$$

donc en particulier $\prod_{k=1}^{r+1}(X-\alpha_k)^{m_k} \mid P$, ce qui prouve que H_{r+1} est vraie.
Le principe de récurrence permet de conclure.

- **(ii) $\Longrightarrow$ (i)**. Puisque $(X-\alpha_1)^{m_1} \dots (X-\alpha_r)^{m_r}$ divise P, on a en particulier que pour tout $i \in [\![1, r]\!]$, $(X-\alpha_i)^{m_i}$ divise P. On conclut avec la Remarque 17.70. □

Lemme 17.73 - Divisibilité et égalité de degrés.

Soit $A, B \in \mathbf{K}[X]$. Si $A \mid B$ et $\deg(A) = \deg(B)$, alors $A = \lambda B$ où λ est le coefficient dominant de A divisé par celui de B.

Démonstration.

Exercice d'application 17.74. Montrer que $X^n - 1 = \prod_{k=1}^{n}(X - \mathrm{e}^{2ik\pi/n})$.

➥

On peut généraliser la méthode développée dans l'exemple précédent. On obtient alors le corollaire suivant.

Corollaire 17.75 - Lien entre nombre de racines et degré.

Soit $P \in \mathbf{K}[X]$ un polynôme non nul et $\alpha_1, ..., \alpha_r$ des racines de P de multiplicités respectives $m_1, ..., m_r \in \mathbf{N}^\star$ où $r \in \mathbf{N}^\star$.

1. La somme des multiplicités des racines est inférieure ou égale au degré :
$$m_1 + ... + m_r \leqslant \deg(P).$$
En particulier, un polynôme a au plus $\deg(P)$ racines distinctes.
2. Si $m_1 + ... + m_r = \deg(P)$, alors
   - $\alpha_1, ..., \alpha_r$ sont les racines de P (il n'y en a pas d'autres).
   - $P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$ où λ est le coefficient dominant de P.

Démonstration. **1.** La proposition précédente assure que $\prod_{k=1}^{r}(X-\alpha_k)^{m_k} \mid P$, donc comme $P \neq 0$, $\deg\left(\prod_{k=1}^{r}(X-\alpha_k)^{m_k}\right) \leqslant \deg(P)$, puis en utilisant la formule donnant le degré d'un produit, $\sum_{k=1}^{r} m_k \leqslant \deg(P)$.

2. Si $\alpha \notin \{\alpha_1, \ldots, \alpha_r\}$ était racine, sa multiplicité serait au moins égale à 1 donc la somme des multiplicités dépasserait $\deg(P)$, ce qui est impossible d'après le point précédent.
Avec $\prod_{k=1}^{r}(X-\alpha_k)^{m_k} \mid P$ et $\deg\left(\prod_{k=1}^{r}(X-\alpha_k)^{m_k}\right) = \deg(P)$, on conclut avec le lemme précédent que $P = \lambda \prod_{k=1}^{r}(X-\alpha_k)^{m_k}$. □

Exemple 17.76. $P = 2X^4 - 7X^3 + 6X^2 + X - 2$ possède une racine double (1) et deux racines simples (2 et $\frac{1}{2}$). Ainsi le nombre de racines de P comptées avec multiplicité est 4. De plus, puisque le coefficient de P est 2, on obtient
$$P = 2(X-1)^2(X-2)\left(X - \frac{1}{2}\right).$$

Le corollaire assure en particulier qu'un polynôme de degré $n \geqslant 0$ a au plus n racines distinctes. On en déduit le corollaire suivant, très important en pratique car il permet d'identifier deux fonctions polynomiales égales sur une partie infinie.

Corollaire 17.77 - Caractérisation du polynôme nul avec ses racines.

Soit $n \in \mathbf{N}$. Si P est de degré au plus n et possède $n+1$ racines, alors $P = 0$. En particulier, un polynôme ayant une infinité de racines est nécessairement nul. On en déduit aussi que si $P, Q \in \mathbf{K}[X]$ coïncident sur une partie infinie de $\mathbf{K}$, alors $P = Q$.

Démonstration.

Corollaire 17.78 - Identification entre polynôme et fonction polynomiale.

L'application $\Phi : \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathcal{P}(\mathbf{K}) \\ P & \longmapsto & \widetilde{P} \end{array}$ est bijective, où $\mathcal{P}(\mathbf{K})$ est l'ensemble des fonctions polynomiales de $\mathbf{K}$ à valeurs dans $\mathbf{K}$.

Démonstration.

Remarque 17.79. On retrouve ce qui a été dit dans la Remarque 17.35 : si f est une fonction polynomiale, il existe une unique polynôme P tel que $f = \widetilde{P}$.

Définition 17.80 - Polynôme scindé.

Soit $P \in \mathbf{K}[X]$ non nul. On dit que P est **scindé** sur $\mathbf{K}$ si et seulement si

$$\exists \alpha_1, ..., \alpha_r \in \mathbf{K},\ \exists m_1, ..., m_r \in \mathbf{N}^\star,\ \exists \lambda \in \mathbf{K}, \quad P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k}.$$

Autrement dit, P est scindé sur $\mathbf{K}$ si et seulement P est produit de polynômes de degré 1 à coefficients dans $\mathbf{K}$.

Proposition 17.81 - Caractérisation des polynômes scindés.

Soit $P \in \mathbf{K}[X]$ non constant. P est scindé si et seulement si il possède $\deg(P)$ racines comptées avec leur multiplicité.

Démonstration.

Exemple 17.82. **1.** $2X^4 - 7X^3 + 6X^2 + X - 2 = 2(X-1)^2(X-2)\left(X - \frac{1}{2}\right)$ est scindé sur $\mathbf{R}$.

2. $X^2 + 1 = (X - i)(X + i)$ est scindé sur $\mathbf{C}$, mais par sur $\mathbf{R}$ car ce polynôme n'a pas de racines réelles.

3. Soit $n \in \mathbf{N}^\star$. $X^n - 1 = \prod_{k=1}^{n}(X - \mathrm{e}^{i\frac{2k\pi}{n}})$ est scindé sur $\mathbf{C}$.

Proposition 17.83 - Lien entre racines et divisibilité.

Soit A et B deux polynômes avec A scindé. Alors toutes les racines de A sont des racines de B avec une multiplicité au moins égale si et seulement si $A \mid B$.

Démonstration.

Exemple 17.84. Les racines de $X^4 - 1$ sont les racines 4-ièmes de l'unité. Elles sont aussi racines 12-ièmes donc $X^4 - 1$ divise $X^{12} - 1$.

17.5 Factorisation dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$

17.5.1 Polynômes irréductibles

Tout le cours d'arithmétique dans $\mathbf{K}[X]$ évolue en parallèle avec le cours d'arithmétique dans $\mathbf{Z}$. Ceci tient entre autres dans le fait qu'il existe dans $\mathbf{Z}$ (muni des opérations + et $\times$) et dans $\mathbf{K}[X]$ (muni des opérations + et $\times$) une division euclidienne. Le théorème fondamental de l'arithmétique dans $\mathbf{Z}$ dit que tout entier n supérieur ou égal à 2 se décompose, de manière unique à l'ordre près des facteurs, en un produit de nombres premiers. Les nombres premiers dans $\mathbf{N}^\star$ ont leur analogue dans $\mathbf{K}[X]$: les polynômes irréductibles sur $\mathbf{K}$. De même que, dans $\mathbf{N}^\star$, le nombre 1 ne fait pas partie de la liste des nombres premiers pour assurer l'unicité de la décomposition, un polynôme de degré 0 ne fera pas partie de la liste des polynômes irréductibles sur $\mathbf{K}[X]$ pour assurer l'unicité de la décomposition dans $\mathbf{K}[X]$.

Définition 17.85 - Polynôme irréductible.

Soit $P \in \mathbf{K}[X]$. On dit que P est **irréductible** si et seulement si les deux points suivants sont vérifiés.

(a) $\deg(P) \geqslant 1$;

(b) les seuls diviseurs de P sont les constantes ou les multiples de P :

$$\forall Q \in \mathbf{K}[X], \quad Q \mid P \iff \exists \lambda \in \mathbf{K}^\star,\ Q = \lambda \text{ ou } Q = \lambda P.$$

Exemple 17.86. On a $X^2 + 1 = (X - i)(X + i)$ dans $\mathbf{C}[X]$, donc $X - i \mid X^2 + 1$ ce qui montre que $X^2 + 1$ n'est pas irréductible dans $\mathbf{C}[X]$.

Montrons que $X^2 + 1$ est irréductible dans $\mathbf{R}[X]$. Soit $P \in \mathbf{R}[X] \setminus \{0\}$ tel que $P \mid X^2 + 1$. Alors $\deg(P) \leqslant \deg(X^2 + 1)$, puis $\deg(P) \in \{0, 1, 2\}$.
Supposons $\deg(P) = 1$. Alors il existe $(a, b) \in \mathbf{R}^\star \times \mathbf{R}$ tel que $P = aX + b$. Puisque $aX + b \mid X^2 + 1$, on obtient que $-\frac{b}{a}$ est une racine de $X^2 + 1$, ce qui est absurde.
Donc les seuls diviseurs de P dans $\mathbf{R}[X]$ sont de degré 0 ou $2 = \deg(P)$, ce qui entraîne que P est irréductible.

ATTENTION

Un polynôme qui n'a pas de racine dans $\mathbf{K}$ n'est pas nécessairement irréductible sur $\mathbf{K}$. Considérons par exemple le polynôme $P = X^4+X^2+1 \in \mathbf{R}[X]$. P n'a pas de racine sur $\mathbf{R}$ puisque pour tout x réel, $\tilde{P}(x) = x^4+x^2+1 > 0$. Pourtant,

$$P = X^4 + 2X^2 + 1 - X^2 = (X^2+1)^2 - X^2 = (X^2+X+1)(X^2-X+1),$$

et le polynôme n'est pas irréductible sur $\mathbf{R}$.

Proposition 17.87 - Non irréductibilité des polynômes avec racine.

Soit $P \in \mathbf{K}[X]$. Si $\deg(P) \geqslant 2$ et si P possède une racine $\alpha \in \mathbf{K}$, alors P n'est pas irréductible sur $\mathbf{K}$.

Démonstration.

Théorème 17.88 - Irréductibilité des polynômes de degré 1.

Les polynômes de degré 1 sont irréductibles sur $\mathbf{K}$.

Démonstration.

17.5.2 Décomposition dans $\mathbf{C}[X]$

Commençons par présenter le « théorème fondamental de l'algèbre ».

Théorème 17.89 - Théorème de D'Alembert-Gauss.

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

Démonstration.
Admis (difficile). □

Par exemple, l'équation $z^6 + z^4 + 1 = 0$ admet au moins une solution dans $\mathbf{C}$. On note que le théorème ne fournit aucun procédé pour l'obtenir et de fait, personne au monde ne sait donner la valeur exacte d'une solution. Au degré 2, on dispose de formule fournissant les solutions en fonction des coefficients de l'équation (avec le discriminant). Une telle formule existence encore au degré 3 (formules de Cardan, qui contient entre autres des racines carrées et des racines cubiques) et au degré 4 (formules de Ferrari). Mais il a été démontré qu'il n'est plus possible d'obtenir de telles formules pour les équations quelconques de degré supérieur ou égal à 5.

Théorème 17.90 - Polynômes irréductibles de $\mathbf{C}[X]$.

Les polynômes irréductibles de $\mathbf{C}[X]$ sont les polynômes de degré 1.

Démonstration.

Théorème 17.91 - Décomposition des polynômes à coefficients dans C.

Soit $P \in \mathbf{C}[X]$ un polynôme non constant. P se décompose de manière unique, à l'ordre près des facteurs, en produit de polynômes irréductibles de $\mathbf{C}[X]$:

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k},$$

avec

- λ le coefficient dominant de P ;
- $\alpha_1, \alpha_2, \ldots, \alpha_r$ les racines complexes distinctes de P de multiplicités respectives $m_1, m_2, \ldots, m_r$.

En particulier, tout polynôme de $\mathbf{C}[X]$ est scindé.

Démonstration.

Exemple 17.92. On a donné précédemment la décomposition de $X^n - 1 = \prod_{k=1}^{n} (X - \mathrm{e}^{2ik\pi/n})$. En particulier,

1. $X^3 - 1 = (X-1)(X-j)(X-j^2)$, où $j = \mathrm{e}^{2i\pi/3}$;
2. $X^4 - 1 = (X-1)(X-i)(X+1)(X+i)$.

Exemple 17.93. Factorisons dans $\mathbf{C}[X]$ le polynôme $X^4 + 1$.

Cherchons les racines de $X^4 + 1$. Soit $z \in \mathbf{C}$.

$$z^4 = -1 \iff z^4 = \mathrm{e}^{i\pi} \iff \exists k \in [\![0, 3]\!], \quad z = \mathrm{e}^{i(2k+1)\pi/4}.$$

Ainsi

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

Exercice d'application 17.94. Factoriser dans $\mathbf{C}[X]$ le polynôme $P = X^3 - X^2 + 4X - 4$.

➥

Exercice d'application 17.95. Factoriser dans $\mathbf{C}[X]$ le polynôme $3X^6 + 3X^3 + 3$.

➥

17.5.3 Polynôme conjugué

Définition 17.96 - Polynôme conjugué.

Soit $P \in \mathbf{C}[X]$ dont on note n le degré. Il existe $(a_0, ..., a_n) \in \mathbf{C}^{n+1}$ tel que $P = \sum_{k=0}^{n} a_k X^k$.

On appelle **polynôme conjugué** de P et on note $\overline{P}$ le polynôme $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$.

Il s'agit d'une « conjugaison formelle » (on a conjugué les coefficients). Les propriétés usuelles de cette conjugaison formelle sont données ci-après.

Proposition 17.97 - Opérations et conjugaison.

Soit $A, B \in \mathbf{C}[X]$, $\lambda \in \mathbf{C}$, $z \in \mathbf{C}$.

1. $\overline{A+B} = \overline{A} + \overline{B}$.
2. $\overline{\lambda \cdot A} = \overline{\lambda} \cdot \overline{A}$.
3. $\overline{A \times B} = \overline{A} \times \overline{B}$.
4. $\overline{(\overline{A})} = A$.
5. $A \in \mathbf{R}[X] \iff \overline{A} = A$.
6. $\forall z \in \mathbf{C},\ \overline{(\widetilde{A}(z))} = \widetilde{(\overline{A})}(\overline{z})$.

Démonstration.

Proposition 17.98 - Les racines complexes d'un polynôme réel sont conjuguées.

Soit $P \in \mathbf{R}[X]$ de degré supérieur ou égal à 1. Soit $z \in \mathbf{C}$.
Si z est une racine de P alors $\overline{z}$ est racine de P avec même ordre de multiplicité.

Démonstration.

17.5.4 Factorisation dans $\mathbf{R}[X]$

Théorème 17.99 - Polynômes irréductibles de $\mathbf{R}[X]$.

Les polynômes irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racines réelles.

Démonstration.

Exemple 17.100. Soit $\theta \in \mathbf{R}$. Soit $A = X^2 - 2\cos(\theta)X + 1$. Cherchons à factoriser A.

Cherchons pour commencer les racines de P. On peut utiliser le discriminant ou l'astuce suivante :

$$X^2 - 2\cos\theta X + 1 = (X - \cos\theta)^2 + \sin^2\theta = (X - \cos\theta - i\sin\theta)(X - \cos\theta + i\sin\theta) = (X - \mathrm{e}^{i\theta})(X - \mathrm{e}^{-i\theta}).$$

- Si $\theta \notin \pi\mathbf{Z}$, les racines de A ne sont pas réelles donc $A = X^2 - 2\cos\theta X + 1$ est irréductible.
- Si $\theta \in 2\pi\mathbf{Z}$, $A = X^2 - 2X + 1 = (X-1)^2$.
- Si $\theta \in \pi + 2\pi\mathbf{Z}$, $A = X^2 + 2X + 1 = (X+1)^2$.

Théorème 17.101 - Décomposition des polynômes à coefficients dans R.

Tout polynôme P de $\mathbf{R}[X]$ de degré supérieur ou égal à 1 se décompose de manière unique, à l'ordre près des facteurs, en produit de polynômes irréductibles :

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k} \prod_{k=1}^{s} (X^2 - 2\,\mathfrak{Re}(\omega_k)X + \mid \omega_k \mid^2)^{n_k},$$

où

- λ le coefficient dominant de P ;
- pour tout $k \in [\![1, r]\!]$, α_k est une racine réelle de P de multiplicité m_k (il y a exactement r racines réelles) ;
- pour tout $k \in [\![1, s]\!]$, ω_k, $\overline{\omega_k}$ sont des racines complexes non réelles de P, de multiplicité n_k (il y a exactement $2s$ racines complexes).

Démonstration.

Exemple 17.102. Factorisons dans $\mathbf{R}[X]$, $X^4 + 1$.

- *Méthode 1.* On utilise la décomposition obtenue dans $\mathbf{C}[X]$,

$$X^4 + 1 = (X - \mathrm{e}^{i\frac{\pi}{4}})(X - \mathrm{e}^{-i\frac{\pi}{4}})(X - \mathrm{e}^{i\frac{5\pi}{4}})(X - \mathrm{e}^{-i\frac{5\pi}{4}}) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

- *Méthode 2.* Moins calculatoire, mais plus astucieuse.

$$X^4 + 1 = (X^2)^2 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

Exemple 17.103. Soit $n \in \mathbf{N}^\star$. Déterminons la factorisation dans $\mathbf{R}[X]$ de $X^n - 1$.

On a obtenu la décomposition dans $\mathbf{C}[X]$ suivante :

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{i\frac{2k\pi}{n}}\right).$$

- Si n est pair, alors il existe $k \in \mathbf{Z}$ tel que $n = 2k$ et, en regroupant les termes complexes conjugués,

$$\begin{aligned} X^{2k} - 1 &= (X-1)(X+1) \prod_{p=1}^{k-1} \left(X - \mathrm{e}^{i\frac{2p\pi}{n}}\right)\left(X - \mathrm{e}^{-i\frac{2p\pi}{n}}\right) \\ &= (X-1)(X+1) \prod_{p=1}^{k-1} \left(X^2 - 2\cos\left(\frac{p\pi}{n}\right)X + 1\right). \end{aligned}$$

- Si n est impair, alors il existe $k \in \mathbf{Z}$ tel que $n = 2k+1$ et de même qu'avant,

$$\begin{aligned} X^{2k+1} - 1 &= (X-1) \prod_{p=1}^{k} \left(X - \mathrm{e}^{i\frac{2p\pi}{n}}\right)\left(X - \mathrm{e}^{-i\frac{2p\pi}{n}}\right) \\ &= (X-1) \prod_{p=1}^{k} \left(X^2 - 2\cos\left(\frac{p\pi}{n}\right)X + 1\right). \end{aligned}$$

Exercice d'application 17.104. Décomposer $P = X^4 - 2X^3 + 2X^2 - 2X + 1$ dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$.

➥

Exercice d'application 17.105. Factoriser X^6+X^3+1 dans $\mathbf{R}[X]$ à partir de la décomposition dans $\mathbf{C}[X]$ donnée ci-après :

$$X^6+X^3+1=(X-\mathrm{e}^{i\frac{2\pi}{9}})(X-\mathrm{e}^{-i\frac{2\pi}{9}})(X-\mathrm{e}^{i\frac{2\pi}{8}})(X-\mathrm{e}^{-i\frac{8\pi}{9}})(X-\mathrm{e}^{i\frac{14\pi}{9}})(X-\mathrm{e}^{-i\frac{14\pi}{9}}).$$

➥

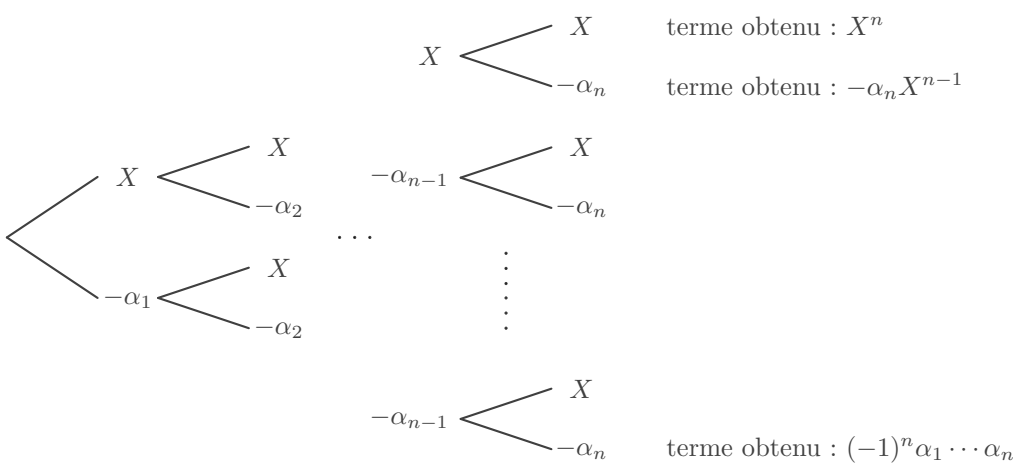
17.6 Relations coefficients-racines

Proposition 17.106 - Relations coefficients-racines ou de Viète.

Soit $P\in\mathbf{K}[X]$ un polynôme scindé. Notons $n=\deg(P)$, $P=\sum_{k=0}^{n}a_kX^k$ et $\alpha_1,...,\alpha_n$ les racines de P. Alors

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

Démonstration.
En développant $\lambda(X-\alpha_1)\cdots(X-\alpha_n)$ (où $\lambda\in\mathbf{C}$ est le coefficient dominant de P), on obtient que



$$P = \lambda(X^n + (-\alpha_1 - \alpha_2 - \cdots - \alpha_n)X^{n-1} + \cdots + (-\alpha_1)(-\alpha_2)\dots(-\alpha_n)$$

En identifiant, on obtient :

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

□

Exemple 17.107. Soit $n \in \mathbf{N}^\star$. $X^n - 1 = \prod_{k=0}^{n-1}(X - \mathrm{e}^{2ik\pi/n})$. Les relations coefficients-racines s'écrivent

$$\sum_{k=0}^{n-1} \mathrm{e}^{2ik\pi/n} = -\frac{0}{1} = 0 \quad \text{et} \quad \prod_{k=0}^{n-1} \mathrm{e}^{2ik\pi/n} = (-1)^{n+1}.$$

17.7 Compléments sur les décompositions en éléments simples

Nous avons déjà vu dans des chapitres précédents que les fonctions du type $x \longmapsto \dfrac{px+q}{ax^2+bx+c}$ peuvent se mettre sous des formes plus simples facilitant les calculs de primitives ou de dérivées n-ièmes. Nous allons généraliser cela à d'autres fonctions.

17.7.1 Théorème de décomposition en éléments simples

Théorème 17.108 - Décomposition en éléments simples.

Soit A et B deux polynômes dans $\mathbf{K}[X]$. On suppose que B non nul, scindé et à racines simples. Notons $\alpha_1, \alpha_2, \dots, \alpha_k$ les racines de B. Soit la **fonction rationnelle**

$$\begin{array}{rccc} f: & \mathbf{R}\backslash\{\alpha_1,\dots,\alpha_k\} & \longrightarrow & \mathbf{K} \\ & t & \longmapsto & \dfrac{A(t)}{B(t)} \end{array}$$

Alors il existe un unique polynôme $E \in \mathbf{K}[X]$ et un unique k-uplet $(a_1, a_2, \dots, a_k) \in \mathbf{K}^k$ tel que

$$\forall t \in \mathbf{R}\backslash\{\alpha_1,\dots,\alpha_k\}, \quad f(t) = E(t) + \frac{a_1}{t-\alpha_1} + \frac{a_2}{t-\alpha_2} + \cdots + \frac{a_k}{t-\alpha_k}.$$

E est alors appelé la **partie entière** de $\dfrac{A}{B}$ et c'est le quotient de la division euclidienne de A par B.
L'écriture complète est appelée **la décomposition en éléments simples** de f

Démonstration.
Admis. □

Méthode 17.109. *Obtenir la décomposition en éléments simples*

Lorsque l'on doit trouver une décomposition en éléments simples, on commence par déterminer la division euclidienne de A par B : $A = BE + R$. On arrive alors à une écriture de la forme

$$f(t) = E(t) + \frac{R(t)}{B(t)}.$$

Pour trouver les coefficients a_i, on joue ensuite sur la double écriture de f. D'après le Théorème 17.108, on sait qu'il existe des scalaires $a_1, \dots, a_k$ tels que :

$$\forall t \in \mathbf{R}\backslash\{\alpha_1,\dots,\alpha_k\}, \quad \frac{R(t)}{(t-\alpha_1)(t-\alpha_2)\dots(t-\alpha_k)} = \frac{a_1}{t-\alpha_1} + \frac{a_2}{t-\alpha_2} + \cdots + \frac{a_k}{t-\alpha_k}.$$

En multipliant cette ligne par $(t-\alpha_1)$, on a

$$\frac{R(t)}{(t-\alpha_2)\dots(t-\alpha_k)} = a_1 + \frac{a_2(t-\alpha_1)}{t-\alpha_2} + \dots + \frac{a_k(t-\alpha_1)}{t-\alpha_k}.$$

En passant à la limite quand t tend vers α_1, on en déduit :

$$\frac{R(\alpha_1)}{(\alpha_1-\alpha_2)\dots(\alpha_1-\alpha_k)} = a_1.$$

En reproduisant ce schéma, on peut déterminer tous les coefficients.

Exercice d'application 17.110. Déterminer la décomposition en éléments simples de $f : t \longmapsto \dfrac{t^5+t^4+t^3+t^2+t+1}{t^3-t}$.

➥

Exemple 17.111. Déterminons la décomposition en éléments simples de $f : t \longmapsto \dfrac{t^5}{(t^2+4)(t+1)}$.

On commence par effectuer la division euclidienne de X^5 par $(X^2+4)(X+1) = X^3+X^2+4X+4$. On obtient $X^5 = (X^3+X^2+4X+4)(X^2-X-3)+(3X^2+16X+12)$. On remarque également que le polynôme $(X^2+4)(X+1)$ se décompose en $(X-2i)(X+2i)(X+1)$ et est donc scindé à racines simples. Ainsi, d'après le Théorème 17.108, il existe des uniques complexes a, b, c tels que pour tout $t \in \mathbf{R}\setminus\{-1\}$,

$$f(t) = -3-t+t^2+\frac{3t^2+16t+12}{(t^2+4)(t+1)} = -3-t+t^2+\frac{a}{t+1}+\frac{b}{t-2i}+\frac{c}{t+2i}.$$

On a donc, pour tout $t \in \mathbf{R}\setminus\{-1\}$,

$$\frac{3t^2+16t+12}{(t+2i)(t-2i)(t+1)} = \frac{a}{t+1}+\frac{b}{t-2i}+\frac{c}{t+2i} \tag{17.1}$$

Comme précédemment, en multipliant (17.1) par $t+1$ et faisant tendre t vers -1, on obtient $a = \dfrac{-1}{5}$.

Pour le pôle $2i$, on va utiliser la même technique. ATTENTION, cela revient à dire que la variable t est complexe (puisqu'on la fait tendre vers $2i$), ce qui n'est pas du tout justifié par le cours de cette année. On évitera donc de faire cela sur une copie : c'est un calcul à faire au brouillon.

On obtient ainsi (après simplification) $b = \dfrac{8}{5} - \dfrac{16}{5}i$.

On pourrait procéder de la même façon pour obtenir c, mais il est plus efficace de remarquer que comme f est à dénominateur et numérateur réels, on a pour tout $t \in \mathbf{R}\setminus\{-1\}$, $f(t) = \overline{f(t)}$ et donc

$$\overline{\frac{a}{t+1}+\frac{b}{t-2i}+\frac{c}{t+2i}} = \frac{a}{t+1}+\frac{b}{t-2i}+\frac{c}{t+2i}$$

$$\frac{a}{t+1}+\frac{\overline{b}}{t+2i}+\frac{\overline{c}}{t-2i} = \frac{a}{t+1}+\frac{b}{t-2i}+\frac{c}{t+2i}.$$

Par unicité des coefficients a, b, c, on en déduit que $c = \overline{b}$.

Finalement, pour tout $t \in \mathbf{R}\backslash\{-1\}$,

$$f(t) = -3 - t + t^2 + \frac{1}{5}\left(\frac{-1}{t+1} + \frac{8-16i}{t-2i} + \frac{8+16i}{t+2i}\right).$$

Exemple 17.112. Déterminons la décomposition en éléments simples de $f : t \longmapsto \dfrac{t^3+t+1}{(t^3-1)(t+1)}$.

Pas besoin ici de division euclidienne, car le numérateur est déjà de degré strictement inférieur au dénominateur. On factorise simplement $(X^3-1)(X+1)$ en $(X-1)(X-j)(X+j)(X+1)$ qui est scindé à racines simples. Ainsi, d'après le Théorème 17.108, il existe des uniques complexes a, b, c, d tels que pour tout $t \in \mathbf{R}\backslash\{1,-1\}$, on ait

$$\frac{t^3+t+1}{(t^3-1)(t+1)} = \frac{a}{t+1} + \frac{b}{t-1} + \frac{c}{t-j} + \frac{d}{t+j} \tag{17.2}$$

À nouveau, en multipliant (17.2) par $t+1$ et faisant tendre t vers -1, on obtient $a = \dfrac{3}{2}$. En multipliant (17.2) par $t-1$ et faisant tendre t vers 1, on obtient $b = \dfrac{1}{2}$ (on n'oublie pas que $t^3-1 = (t-1)(t^2+t+1)$).

Pour les racines complexes j et $\overline{j}$, on utilise la même technique que dans l'exemple précédent pour remarquer que $c = \overline{d}$. On détermine alors c AU BROUILLON par la même astuce pas très légale que précédemment. On trouve $c = \dfrac{2j-4j^2}{12}$ et donc $d = \dfrac{4j-2j^2}{12}$. Finalement, pour tout $t \in \mathbf{R}\backslash\{1,-1\}$,

$$f(t) = \frac{3}{2(t+1)} + \frac{1}{2(t-1)} + \frac{2j-4j^2}{12(t-j)} + \frac{4j-2j^2}{12(t+j)}.$$

17.7.2 Pour aller plus loin : les fractions rationnelles (hors-programme)

Définition 17.113 - Fraction rationnelle.

Une **fraction rationnelle** à coefficients dans $\mathbf{K}$ d'indéterminée X est une expression de la forme $\dfrac{P}{Q}$ où P et Q sont des polynômes de $\mathbf{K}[X]$ et Q est non nul.
On note $\mathbf{K}(X)$ l'ensemble de ces fractions rationnelles.

Les opérations classiques (addition,multiplication par une constante,multiplication) dans $\mathbf{K}[X]$ s'effectuent « naturellement » en combinant les règles de calcul sur les fractions et les polynômes.

Exemple 17.114.

$$\begin{aligned}
\frac{X}{2X^2+1} - X \times \frac{3X^2-X}{2+X} &= \frac{X}{2X^2+1} - \frac{3X^3-X^2}{2+X} \\
&= \frac{X(3X^3-X^2) - (3X^3-X^2)(2X^2+1)}{(2+X)(2X^2+1)} \\
&= \frac{3X^4 - X^3 - 6X^5 + 4X^4 - 3X^3 + X^2}{4X^2+2+2X^3+X} \\
&= \frac{-6X^5 + 7X^4 - 4X^3 + X^2}{2X^3+4X^2+X+2}
\end{aligned}$$

Tout comme les polynômes, les fractions rationnelles sont des objets purement formels. En particulier ce ne sont pas des fonctions, et X ne désigne pas un réel ou un complexe, mais l'indéterminée.

Définition 17.115 - Forme irréductible, pôle.

Une fraction rationnelle $\frac{P}{Q}$ est dite sous **forme irréductible** lorsque P et Q n'ont aucun facteur irréductible en commun et que Q est unitaire.
Dans ce cas, les racines de Q sont appelés les **pôles** de la fraction $\frac{P}{Q}$, et leur multiplicité en tant que racine de Q est appelée leur multiplicité en temps que pôle de $\frac{P}{Q}$.

Exemple 17.116. $F = \dfrac{X^2+2X}{2X^3-2X}$ n'est pas sous forme irréductible, mais est égale à $\dfrac{\frac{1}{2}(X+2)}{X^2-1} = \dfrac{\frac{1}{2}(X+2)}{(X+1)(X-1)}$ qui est irréductible car son dénominateur et son numérateur sont sous forme factorisée et n'ont manifestement pas de facteurs irréductibles communs.

Ainsi, F a deux pôles simples : 1 et -1.

0 est une racine de $2X^3-2X$, mais n'est pas un pôle de F, car la simplification par X fait apparaître que ce n'était qu'une illusion.

Théorème 17.117 - Décomposition en éléments simples - version étendue.

Si $F = \dfrac{P}{Q}$ est une fraction rationnelle **sous forme irréductible** telle que Q soit scindé. Notons $\alpha_1, \alpha_2, \dots, \alpha_n$ les racines de Q et $k_1, k_2, \dots, k_n$ leurs multiplicités respectives.
Alors, il existe un unique polynôme $E \in \mathbf{K}[X]$ et des uniques coefficients $a_{i,j}$ dans $\mathbf{K}$ tels que

$$F(X) = E(X) + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \frac{a_{i,j}}{(X-\alpha_i)^j}.$$

Dans ce cas E est le quotient de la division euclidienne de P par Q.
Cette écriture est appelée **décomposition en éléments simples** de F.

Ce théorème s'applique dans $\mathbf{C}[X]$ à toutes les fractions rationnelles (puisque tous les polynômes sont scindés dans $\mathbf{C}[X]$) et dans $\mathbf{R}[X]$ aux fractions rationnelles dont le dénominateur n'a pas de facteur irréductible de degré 2.

Lorsque le dénominateur a un facteur irréductible de degré 2, il existe aussi une décompositions en éléments simples, mais celle-ci est plus compliquée.

Remarque 17.118. Ce paragraphe n'est pas au programme, donc si vous tombez sur une forme de ce type, la forme de la décomposition sera précisée (par contre, on peut vous demandez de trouver les coefficients $a_{i,j}$, donc la suite est intéressante !).

Exemple 17.119. Déterminons la décomposition en éléments simples de $F = \dfrac{2X^5+X^4+3X+2}{X^4-2X^2+1}$.

La division euclidienne de $2X^5+X^4+3X+2$ par X^4-2X^2+1 donne

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

Donc

$$F = 1+2X+\frac{1+X+2X^2+4X^3}{(X-1)^2(X+1)^2}.$$

$X^4-2X^2+1 = (X^2-1)^2 = (X-1)^2(X+1)^2$, donc le théorème précédent indique que cette fraction rationnelle peut se mettre sous la forme

$$\frac{1+X+2X^2+4X^3}{(X-1)^2(X+1)^2} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{X+1} + \frac{d}{(X+1)^2}.$$

avec $(a,b,c,d) \in \mathbf{R}^4$. En multipliant par $(X-1)^2$, on obtient

$$\frac{1+X+2X^2+4X^3}{(X+1)^2} = a(X-1)+b+\frac{c(X-1)^2}{X+1}+\frac{d(X-1)^2}{(X+1)^2}.$$

En évaluant en 1, obtient $b=2$. De même, avec $(X+1)^2$, on obtient $d=\dfrac{-1}{2}$.

En revanche, cette méthode ne permet pas de déterminer a et c.

D'autres méthodes plus efficaces existent, mais, à défaut, on peut tout mettre au même dénominateur :

$$\frac{1+X+2X^2+4X^3}{X^4-2X^2+1} = \frac{a(X-1)(X+1)^2+2(X+1)^2+c(X+1)(X-1)^2+\frac{-1}{2}(X-1)^2}{X^4-2X^2+1}.$$

puis

$$1+X+2X^2+4X^3 = a(X-1)(X+1)^2+2(X+1)^2+c(X+1)(X-1)^2+\frac{-1}{2}(X-1)^2$$

En identifiant les coefficients de degré 0 et 3, on obtient

$$\begin{cases} a+c &= 4 \\ -a+2+c+-1/2 &= 1 \end{cases}, \text{ donc } \begin{cases} a+c &= 4 \\ -a+c &= -1/2 \end{cases} \text{ et ainsi } \begin{cases} c &= 7/4 \\ a &= 9/4 \end{cases}$$ On a donc pour conclure que

$$F = 1+2X+\frac{9/4}{X-1}+\frac{2}{(X-1)^2}+\frac{7/4}{X+1}+\frac{-1/2}{(X+1)^2}.$$

Questions de cours

1. Donner le résultat qui permet l'identification des coefficients de polynômes.
2. Donner les formules permettant de calculer la somme et le produit de deux polynômes.
3. Énoncer la formule du binôme de Newton pour les polynômes.
4. Définir le degré d'un polynôme (sans oublier le cas du polynôme nul !).
5. Donner la définition de polynôme unitaire.
6. Donner l'inégalité pour le degré d'une somme ainsi que le cas d'égalité. Donner les formules pour le degré d'un produit de polynômes, du produit d'un polynôme par un constante et d'une composée de polynômes.
7. Donner la définition de polynôme dérivé.
8. Donner la formule de Leibniz pour les polynômes.
9. Donner la formule permettant de calculer $\deg(P^{(\ell)})$, où $P \in \mathbf{K}[X]$ et $\ell \in \mathbf{N}$.
10. Donner les formules de Taylor pour les polynômes, en 0 et en $a \in \mathbf{K}$.
11. Définir la notion de multiple (resp. diviseur) d'un polynôme.
12. Énoncer le théorème de division euclidienne pour les polynômes.
13. Définir la notion de racine d'un polynôme.
14. Définir la notion de multiplicité d'une racine d'un polynôme.
15. Donner la caractérisation de la multiplicité d'une racine d'un polynôme à l'aide des dérivées.
16. Combien de racines, comptées avec multiplicité, un polynôme peut-il avoir au plus ?
17. Donner la définition de polynôme scindé.
18. Donner la définition de polynôme irréductible.
19. Donner les polynômes irréductibles dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$.
20. Énoncer le théorème de D'Alembert-Gauss.
21. Donner les formules de factorisation dans $\mathbf{C}[X]$ et dans $\mathbf{R}[X]$.
22. Quand on peut-on affirmer que les racines d'un polynôme sont conjuguées l'une de l'autre ?
23. Énoncer les relations coefficients-racines (ou de Viète).