Chapitre 15

Polynômes

Dans ce cours, $\mathbf{K}$ représente $\mathbf{R}$ ou $\mathbf{C}$ et l'expression « au-delà du rang N » signifie « à partir du rang $N+1$ inclus ».

1. Définitions, opérations, indéterminée, degré

Définition 1.

Soit $u \in \mathbf{K}^{\mathbf{N}}$. On dit que u est **presque nulle** si u est nulle au delà d'un certain rang, *i.e.* s'il existe $N \in \mathbf{N}$ tel que, pour tout $i > N$, $u_i = 0$.

Définition 2.

On appelle **polynôme** à coefficients dans $\mathbf{K}$ toute suite $(a_i)_{i\in\mathbf{N}}$ presque nulle d'éléments de $\mathbf{K}$. Les nombres a_i sont appelés **coefficients** du polynôme.
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 $\mathbf{K}$:

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

1.1. Opérations et propriétés des opérations

On peut définir plusieurs opérations sur l'ensemble des polynômes. L'addition est définie de la même façon que celle sur l'ensemble $\mathbf{K}^{\mathbf{N}}$ des suites d'éléments de $\mathbf{K}$:

Définition 3.

La **somme** des deux polynômes $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ est définie par

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

Dans la définition précédente, 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.

On peut également définir le produit par un élément de $\mathbf{K}$ (produit externe) de la même façon que sur $\mathbf{K}^{\mathbf{N}}$:

Définition 4.

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.

Enfin, on peut définir le produit de deux polynômes (produit interne). Cette multiplication n'est pas définie comme celle de deux suites numériques quelconques.

Définition 5 - Produit de Cauchy.

Le **produit** des deux polynômes $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ est défini par

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

Cette opération est appelée **produit de Cauchy**.

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 opération interne sur $\mathcal{P}_{\mathbf{K}}$ (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 et commutative,
  - le polynôme nul 0 est l'élément neutre de l'addition,
  - 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 a par ailleurs :
  - la multiplication interne (produit de Cauchy) est associative,
  - la multiplication interne est commutative : soit $P = (a_i)_{i\in\mathbf{N}}$ et $Q = (b_i)_{i\in\mathbf{N}}$ deux polynômes ; on pose $P \times Q = (c_i)_{i\in\mathbf{N}}$ et $Q \times P = (d_i)_{i\in\mathbf{N}}$, alors pour tout $i \in \mathbf{N}$,

    $$c_i = \sum_{k=0}^{i} a_k b_{i-k} \underset{k'=i-k}{=} \sum_{k'=0}^{i} a_{i-k'} b_{k'} = \sum_{k'=0}^{i} b_{k'} a_{i-k'} = d_i$$

    donc $P \times Q = Q \times P$.
  - le polynôme unité $1 = (1, 0, 0, \dots) = (u_i)_{i\in\mathbf{N}}$ est élément neutre pour la multiplication interne.
  - 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 $P \times (Q+R) = P \times Q + P \times R$.

  Enfin, la multiplication externe est associative et commutative, distributive par rapport à l'addition, d'élément neutre le polynôme unité $1 = (1, 0, 0, \dots)$.
  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.

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 $n \in \mathbf{N}^\star$, P^n désigne le polynôme $\underbrace{P \times P \times \dots P}_{n \text{ facteurs}}$.

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 $i \in \mathbf{N}$, $c_i = \sum_{k=0}^{i} v_k v_{i-k}$.

  $c_0 = v_0 v_0 = 0$, $\quad c_1 = v_0 v_1 + v_1 v_0 = 0$, $\quad c_2 = v_0 v_2 + v_1 v_1 + v_2 v_0 = 0 + 1 + 0 = 1$ et comme la suite définissant X est nulle au delà du rang 1, on sait qu'au delà du rang $1+1=2$ (cf définition du produit interne plus haut) les termes au delà du rang 1 de la suite X^2 sont nuls.
  Ainsi, $X^2 = (0, 0, 1, 0, 0, \dots)$.
- Par récurrence, on peut montrer que pour tout $i \in \mathbf{N}$, 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 en Python).

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

Alors

$$\begin{aligned} P &= (a_0, a_1, \dots, a_n, 0, 0, \dots) \\ &= a_0 \cdot (1, 0, 0, \dots) + a_1 \cdot (0, 1, 0, \dots) + \dots + a_n \cdot (0, 0, \dots, 0, 1, 0, \dots) \\ &= a_0 X^0 + a_1 X^1 + a_2 X^2 + \dots + a_n X^n \end{aligned}$$

Proposition 6.

Tout polynôme P à coefficients dans $\mathbf{K}$ peut s'écrire sous la forme

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$$

où $n \in \mathbf{N}$ et $(a_0, \ldots, a_n) \in \mathbf{K}^{n+1}$. Le polynôme X est appelé l'**indéterminée** du polynôme P. On dit que P est un polynôme à une indéterminée.

⚠ **Attention** ⚠**.** X est le polynôme (0,1,0..) et n'est pas un nombre.

On n'écrira donc JAMAIS : « je pose $X = 5$... » car ÇA N'A AUCUN SENS.

Notation 7. L'ensemble des polynômes à coefficients dans $\mathbf{K}$ d'indéterminée X est noté $\mathbf{K}[X]$.

Définition 8.

On appelle **monôme** tout polynôme de la forme a_iX^i où $i \in \mathbf{N}$ et $a_i \in \mathbf{K}$.
Les polynômes de la forme a_0 sont appelés les **polynômes constants**.

On peut réécrire les opérations définies précédemment. Soit $p, q \in \mathbf{N}$, $P = a_0 + a_1X + \cdots + a_pX^p$ et $Q = b_0 + b_1X + \cdots + b_qX^q$.

- Quitte à rajouter des coefficients nuls, on peut écrire P et Q sous la forme

  $$P = a_0 + a_1X + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i \quad \text{et} \quad Q = b_0 + b_1X + \cdots + b_nX^n = \sum_{i=0}^{n} b_iX^i$$

  où $n = \max(p, q)$. Alors

  $$\begin{aligned} P + Q &= (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n \\ &= \sum_{i=0}^{n} (a_i + b_i)X^i \end{aligned}$$

- Pour tout $\lambda \in \mathbf{K}$,

  $$\begin{aligned} \lambda \cdot P &= (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n \\ &= \sum_{i=0}^{n} \lambda a_iX^i \end{aligned}$$

- $$P \times Q = \sum_{i=0}^{p+q} \Big(\sum_{\substack{k+\ell=i \\ k\in\{0,\ldots,p\} \\ \ell\in\{0,\ldots,q\}}} a_kb_\ell \Big) X^k.$$

On dit que :

1. $(\mathbf{K}[X], +)$ est un groupe abélien,
2. $(\mathbf{K}[X], +, \times)$ est un anneau commutatif,
3. $(\mathbf{K}[X], +, \cdot)$ est un espace vectoriel.

Exemple 9.

$$\begin{aligned} &(X^5 + 2X - i) + (X^3 - X^2 - X + i) = X^5 + X^3 - X^2 + X, \\ &(3X^3 - 4X + 1) + (-3X^3 + X^2 + 1) = X^2 - 4X + 2, \\ &(X + 1) \cdot (-iX^2 + X + 2) = -iX^3 + (1 - i)X^2 + 3X + 2. \end{aligned}$$

1.3. Composition des polynômes

Définition 10.

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 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

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

Exercice d'application 12. Soit $A \in \mathbf{K}[X]$. On dit que A est un **polynôme pair** si $A(X) = A(-X)$. Montrer que si A est pair , alors il existe $B \in \mathbf{K}[X]$ tel que $A = B(X^2)$.

$\hookrightarrow$ Soit $A \in \mathbf{K}[X]$. Notons $a_0, ..., a_n \in \mathbf{K}$ les coefficients de A. 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 (puisque deux polynômes sont égaux si et seulement si tous leurs coefficients sont égaux), pour tout $k \in [\![0, n]\!]$, $a_k = (-1)^k a_k$. En particulier, pour tout $p \in \left[\!\left[0, \left\lfloor \frac{n-1}{2} \right\rfloor\right]\!\right]$, $a_{2p+1} = -a_{2p+1}$, donc $a_{2p+1} = 0$, donc en posant $B = \sum_{p=0}^{\lfloor n/2 \rfloor} a_{2p} X^p$. Ainsi $A = B(X^2)$.

Remarque 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.

1.4. Degré d'un polynôme

Définition 14.

Soit $P = (a_i)_{i \in \mathbf{N}}$ un polynôme non nul de $\mathbf{K}[X]$. L'ensemble $\{ i \in \mathbf{N} \mid a_i \neq 0 \}$ possède un plus grand élément d. Le nombre entier d est appelé le **degré** du polynôme P et noté $\deg(P)$.
Par convention, le degré du polynôme nul est $-\infty$.

Démonstration.
Soit $P = (a_i)_{i \in \mathbf{N}}$ un polynôme non nul de $\mathbf{K}[X]$.

$\{ i \in \mathbf{N} \mid a_i \neq 0 \}$ est un sous-ensemble de $\mathbf{N}$ non vide (car P est supposé non nul) et majoré (car la suite $(a_i)_{i \in \mathbf{N}}$ est nulle au-delà d'un certain rang), donc il possède un plus grand élément. □

Exemple 15. $\deg(3X^5 - X + 1) = 5$.

Remarque 16. Les polynômes de degré 0 sont les polynômes constants non nuls.

Proposition 17.

- Si un polynôme P s'écrit $P = \sum_{i=0}^{n} a_i X^i$, alors son degré est inférieur ou égal à n.
- Tout polynôme $P = \sum_{i=0}^{d} a_i X^i$ où $a_d \neq 0$ est de degré d.

Définition 18.

- Tout polynôme P non nul de degré $d \geqslant 0$ s'écrit de manière unique sous la forme $P = \sum_{i=0}^{d} a_i X^i$ où $(a_0, a_1, \dots, a_d) \in \mathbf{K}^{d+1}$ et $a_d \neq 0$. Le coefficient a_d est appelé le **coefficient dominant** de P.
- Un polynôme non nul est **unitaire** si son coefficient dominant vaut 1.

Proposition 19.

Soit P et Q deux polynômes de $\mathbf{K}[X]$ et $\lambda \in \mathbf{K}^\star$.

1. $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$.
   De plus, on peut préciser que si $\deg(P) \neq \deg(Q)$ alors $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$.
   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. $\deg(\lambda P) = \deg(P)$ si $\lambda \neq 0$.
3. $\deg(P \times Q) = \deg(P) + \deg(Q)$.

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

Démonstration.
Soit P et Q deux polynômes de degrés respectifs d et d' où $d, d' \in \mathbf{N} \cup \{-\infty\}$.

1. - Si $P = 0$, alors $P + Q = Q$ donc $\deg(P+Q) = \deg(Q) = \max\big(\deg(P), \deg(Q)\big)$.
   - Si $Q = 0$, alors $P + Q = P$ donc $\deg(P+Q) = \deg(P) = \max\big(\deg(P), \deg(Q)\big)$.
   - Supposons maintenant que $P \neq 0$ et $Q \neq 0$. Donc P et Q s'écrivent $P = \sum_{i=0}^{d} a_i X^i$ et $Q = \sum_{i=0}^{d'} b_i X^i$ où $a_0, \dots, a_d, b_0, \dots, b_{d'} \in \mathbf{K}$ et $a_d \neq 0$ et $b_{d'} \neq 0$.
     - Cas où $d < d'$: on a
     $$P + Q = \sum_{i=0}^{d} (a_i + b_i) X^i + \sum_{i=d+1}^{d'} b_i X^i = \sum_{i=0}^{d'} s_i X^i$$
     où pour tout $i \in [\![0, d']\!]$, $s_i = \begin{cases} a_i + b_i & \text{si } i \leqslant d \\ b_i & \text{si } i > d \end{cases}$. Puisque $s_{d'} = b_{d'} \neq 0$, le polynôme $P + Q$ est de degré d' donc $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$.
     - De même, si $d' < d$ alors le polynôme $P + Q$ est de degré d donc $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$.

- Cas où $d = d'$. On a $P+Q = \sum_{i=0}^{d} (a_i+b_i)X^i$. Si $a_d + b_d \neq 0$, alors $\deg(P+Q) = \deg(d) = \max\big(\deg(P), \deg(Q)\big)$ et sinon, $\deg(P+Q) < \deg(d)$ donc $\deg(P+Q) < \max\big(\deg(P), \deg(Q)\big)$.

Dans tous les cas, on constate que $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$.

2. Notons a_n le coefficient dominant de P. Alors le coefficient dominant de λP est λa_n et $\deg(\lambda P) = \deg(P)$.
3.
   - Si $P = 0$ ou $Q = 0$, alors $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$, et $P \times Q = 0$ donc
   $$\deg(P \times Q) = -\infty = \deg(P) + \deg(Q).$$
   - On suppose que $P \neq 0$ et $Q \neq 0$. Alors P et Q s'écrivent $P = \sum_{i=0}^{d} a_i X^i$ et $Q = \sum_{i=0}^{d'} b_i X^i$ où $a_0, \ldots, a_d, b_0, \ldots, b_{d'} \in \mathbf{K}$ et $a_d \neq 0$ et $b_{d'} \neq 0$. On a
   $$P \times Q = \sum_{i=0}^{d+d'} \Big(\sum_{\substack{k+\ell=i \\ k\in\{0,\ldots,d\} \\ \ell\in\{0,\ldots,d'\}}} a_k b_\ell \Big) X^k..$$
   Dans la somme précédente, le coefficient devant $X^{d+d'}$ est $a_d b_{d'}$ qui n'est pas nul. Donc
   $$\deg(P \times Q) = d + d' = \deg(P) + \deg(Q).$$

□

Exemple 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 21. 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 $P \times \frac{1}{a} = 1$). Les polynômes **inversibles** sont donc les polynômes constants non nuls.

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

Exercice d'application 22. Soit $n \in \mathbf{N}^\star$. Déterminer le degré et le coefficient dominant de $P = (X^2+1)^n - (X^2-1)^n$.

↪ On obtient $\deg(P) \leqslant 2n$. En utilisant la formule du binôme de Newton, on observe que :
- le coefficient en X^{2n} est nul ;
- le coefficient en X^{2n-1} est nul (P est pair, donc il n'apparaît que des puissances paires de X dans P) ;
- le coefficient en X^{2n-2} est
$$nX^{2n-2} - (-nX^{2n-2}) = 2nX^{2n-2}.$$

Donc $\deg(P) = 2n - 2$ et le coefficient dominant de P est $2n$.

◇◇

Remarque technique 23. 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).

Exercice d'application 24. Déterminer les couples (A, B) de polynômes tels que $B^2 = X \times A^2$.

$\hookrightarrow$ *Analyse.* On suppose qu'il existe un couple (A,B) solution. On a $\deg(B^2) = \deg(XA^2)$, donc $2\deg(B) = 1 + 2\deg(A)$. Or $\deg(A), \deg(B) \in \mathbf{N} \cup \{-\infty\}$. Si $(\deg(A), \deg(B)) \in \mathbf{N}^2$, l'égalité est impossible, donc $A = 0$ ou $B = 0$. Dans tous les cas, on obtient $A = B = 0$.
Synthèse. $0^2 = X \times 0^2$.
Conclusion. Ainsi l'unique couple solution est $(0,0)$.

Exercice d'application 25. Déterminer les polynômes $P \in \mathbf{R}[X]$ vérifiant $P \circ P = P$.

$\hookrightarrow$ *Analyse.* Soit $P \in \mathbf{R}[X]$ tel que $P \circ P = P$. Supposons $P \neq 0$, notons $n = \deg(P)$ et $P = \sum_{k=0}^{n} a_k X^k$, avec $a_k \neq 0$. Alors $P \circ P = \sum_{k=0}^{n} a_k P^k$. Le terme de plus au degré de ce dernier polynôme est $a_n^n X^{n^2}$ avec $a_n^n \neq 0$, d'où $\deg(P \circ P) = n^2$. Ainsi, $n^2 = n$ puis $n \in \{0,1\}$.
Synthèse.

- $P = 0$ est solution du problème.
- Soit $P \in \mathbf{R}[X]$ avec $\deg(P) = 0$. Il existe $a_0 \in \mathbf{R}^\star$ tel que $P = a_0$. Alors $P \circ P = a_0 = P$. Donc P est solution du problème.
- Soit $P \in \mathbf{R}[X]$ avec $\deg(P) = 1$. Il existe $(a_0, a_1) \in \mathbf{R} \times \mathbf{R}^\star$ tel que $P = a_0 + a_1 X$. Alors $P \circ P = a_0 + a_1(a_0 + a_1 X) = a_0(1 + a_1) + a_1^2 X$. Donc P est solution si et seulement si

$$\left\{ \begin{array}{rcl} a_0(1+a_1) & = & a_0 \\ a_1^2 & = & a_1 \end{array} \right. \iff \left\{ \begin{array}{rcl} a_0 & = & 0 \\ a_1 & = & 1 \end{array} \right.$$

  Dans ce cas seul X est solution.

Conclusion. L'ensemble des solutions est $\{0, X\} \cup \{\lambda \ : \ \lambda \in \mathbf{R}^\star\}$.

◇◇

Proposition 26.

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

Notation 27. Pour tout entier naturel n, on note $\mathbf{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n (autrement dit, $\mathbf{K}_n[X] = \{P \in \mathbf{K}[X] \mid \deg(P) \leqslant n\}$).

Exemple 28. $\mathbf{K}_2[X] = \{aX^2 + bX + c \mid (a,b,c) \in \mathbf{K}^3\}$. L'ensemble $\mathbf{K}_0[X]$ est l'ensemble des polynômes constants (y compris le polynôme nul).

Proposition 29.

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 sait que

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

et $\deg(\lambda P) \leqslant n$. □

Remarque 30. $\mathbf{K}_n[X]$ n'est pas stable par produit en général. Il est stable par produit si et seulement si $n = 0$.

Théorème 31.

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

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

Démonstration.
Si $A = 0$ ou $B = 0$, alors $AB = 0$.
Réciproquement, supposons que $AB = 0$. Alors $\deg(AB) = -\infty$, *i.e.* $\deg(A) + \deg(B) = -\infty$. Or $\deg(A), \deg(B) \in \mathbf{N} \cup \{-\infty\}$, donc $\deg(A) = -\infty$ ou $\deg(B) = -\infty$, *i.e.* $A = 0$ ou $B = 0$. □

Remarque 32. Le théorème précédente signifie que $(\mathbf{R}[X], +, \times)$ est un anneau intègre.

Exemple 33. Soit $(P, Q, R) \in \mathbf{K}[X]^3$. $PR = PQ \iff P = 0$ ou $R = Q$

1.5. Fonctions polynomiales

Définition 34.

- 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

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

- À tout polynôme $P = \sum_{i=0}^{n} a_i X^i$, on associe une fonction polynomiale que l'on note $\widetilde{P}$, définie par :

$$\begin{array}{rccc} \widetilde{P} : & \mathbf{K} & \longrightarrow & \mathbf{K} \\ & x & \longmapsto & \sum_{i=0}^{n} a_i x^i \end{array}$$

  Cette fonction polynomiale est la **fonction polynomiale associée** au polynôme P.

Remarque 35. Si f est une fonction polynomiale, il existe évidemment 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 $\mathbf{C}$).

Si l'on travaillait avec des polynômes à coefficients dans un autre *corps* que $\mathbf{R}$ ou $\mathbf{C}$, alors l'unicité n'aurait pas été assurée.

On distinguera dans tout ce cours un polynôme P de sa fonction polynomiale en notant cette dernière $\widetilde{P}$ (même nom que le polynôme avec un tilde). Il faut faire attention car cette notation n'est pas officielle (on utilise souvent le même nom pour le polynôme et sa fonction polynomiale, ce qui constitue un abus de langage toléré).

Proposition 36.

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

1. $\widetilde{\lambda A} = \lambda \widetilde{A}$.
2. $\widetilde{A + B} = \widetilde{A} + \widetilde{B}$.
3. $\widetilde{A \times B} = \widetilde{A} \times \widetilde{B}$.
4. $\widetilde{A \circ B} = \widetilde{A} \circ \widetilde{B}$.

Pour évaluer en x une fonction polynomiale $\tilde{P} : x \longmapsto \sum_{k=0}^{n} p_k X^k$, il suffit de faire n additions et n multiplications suivant le parenthésage ci-dessous (en commençant par la parenthèse la plus intérieure) :

$$P(x) = ((\cdots((p_n x + p_{n-1})x + p_{n-2})x + \cdots)x + p_1)x + p_0.$$

Cette méthode, appelée **algorithme de Hörner**, est la méthode la plus efficace pour évaluer une fonction polynomiale en un point x.

Exercice d'application 37. Évaluer $P = 2X^4 - X^3 + 3X^2 - 1$ en -2 grâce à l'algorithme de Hörner.

↪ On a $P = ((2X-1)X+3)X^2 - 1$, donc

$$\begin{aligned}\tilde{P}(-2) &= ((2\times(-2)-1)\times(-2)+3)\times(-2)^2 - 1\\ &= ((-5)\times(-2)+3)\times(-2)^2 - 1\\ &= 13\times(-2)^2 - 1\\ &= 52 - 1\\ &= 51\end{aligned}$$

On peut implémenter cet algorithme en Python. On choisit de stocker les coefficients du polynôme dans un tableau.

```
def horner(P, x):
    n = len(P)
    y = P[n-1]
    for k in range(1, n):
        y = y*x + P[n-k-1]
    return y
```

Exemple d'appel :

```
>>> horner([-1,0,3,-1,2], -2)
51
```

1.6. Dérivées

Définition 38.

Pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ où $n \in \mathbf{N}$, et $a_0, a_1, \ldots, a_n \in \mathbf{K}$, on définit son **polynôme dérivé** P' par

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

Le polynôme P' est défini de sorte que, lorsque $\mathbf{K} = \mathbf{R}$, la fonction polynôme associée à P' soit la dérivée de la fonction polynôme associée à P. La dérivation des polynômes possède donc les mêmes propriétés que la dérivation des fonctions, à savoir

$$(P+Q)' = P' + Q', \quad (\lambda P)' = \lambda P', \quad (P \circ Q)' = Q' \times P' \circ Q \quad \text{et} \quad (PQ)' = P'Q + PQ',$$

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

On peut évidemment itérer le processus de dérivation. 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, si $D : \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathbf{K}[X] \\ P & \longmapsto & P' \end{array}$, alors

$$P^{(\ell)} = (\underbrace{D \circ D \circ \cdots \circ D}_{\ell \text{ fois}})(P).$$

Par convention, on pose $P^{(0)} = P$.

On a alors,

$$(P+Q)^{(\ell)} = P^{(\ell)} + Q^{(\ell)}, \quad (\lambda P)^{(\ell)} = \lambda P^{(\ell)}.$$

pour tous $P, Q \in \mathbf{K}[X]$, $\lambda \in \mathbf{K}$, $\ell \in \mathbf{N}$.

Exemple 39. Si $P = \sum_{k=0}^{n} a_k X^k$, alors $P'' = \sum_{k=2}^{n} k(k-1)a_k X^{k-2}$.

Proposition 40.

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

$$\deg(P') = \begin{cases} \deg(P) - 1 & \text{si } P \text{ n'est pas constant,} \\ -\infty & \text{si } P \text{ est constant.} \end{cases}$$

Plus généralement, si P n'est pas nul, pour tout entier naturel $\ell \leqslant \deg(P)$, on a $\deg(P^{(\ell)}) = \deg(P) - \ell$ et pour tout entier naturel $\ell \geqslant \deg(P) + 1$, on a $P^{(\ell)} = 0$.

Démonstration.
Le premier point est évident avec la définition.

On suppose que P n'est pas nul.

Pour tout $\ell \in [\![0, \deg(P)]\!]$, on note $\mathcal{H}_\ell$ la propriété : $\deg(P^{(\ell)}) = \deg(P) - \ell$.

- $\mathcal{H}_0$ est clairement vérifiée.
- Soit $\ell \in [\![0; \deg(P) - 1]\!]$. On suppose que la propriété $\mathcal{H}_\ell$ est vraie. Le polynôme $P^{(\ell)}$ 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 $\mathcal{H}_{\ell+1}$ est vraie.

Le principe de récurrence finie assure que le résultat est vrai pour tout $\ell \in [\![0; \deg(P)]\!]$.

Le polynôme $P^{(\deg(P))}$ est un polynôme constant donc d'après le premier point, les dérivées suivantes de P sont toutes nulles.

□

Exemple 41.

$$P = X^3 + X + 1 \qquad P' = 3X^2 + 1 \qquad P^{(2)} = 6X \qquad P^{(3)} = 6 \quad \text{et} \quad \forall \ell \geqslant 4,\ P^{(\ell)} = 0.$$

Proposition 42.

Soit $n \in \mathbf{N}$. Pour tout $\ell \in [\![0; n]\!]$,

$$(X^n)^{(\ell)} = n(n-1)\dots(n-\ell+1)X^{n-\ell} = \frac{n!}{(n-l)!}X^{n-\ell}$$

et pour tout $\ell \geqslant n+1$, $(X^n)^{(\ell)} = 0$.

Démonstration.
La deuxième partie du résultat est évidente d'après la proposition précédente. Pour la première partie, on raisonne par récurrence finie : pour tout entier $\ell \in [\![0;n]\!]$, on note $\mathcal{P}_\ell$ la propriété : $(X^n)^{(\ell)} = n(n-1)\dots(n-\ell+1)X^{n-\ell} = \dfrac{n!}{(n-l)!}X^{n-\ell}$.

- La propriété $\mathcal{P}_0$ est vraie (facile).
- Soit $\ell \in [\![0;\underline{n-1}]\!]$. On suppose que la propriété $\mathcal{P}_\ell$ est vraie. Alors

$$(X^n)^{(\ell+1)} = \left((X^n)^{(\ell)}\right)' = \left(\frac{n!}{(n-\ell)!}X^{n-\ell}\right)' = \frac{n!}{(n-\ell)!}(n-\ell)X^{n-(\ell+1)} = \frac{n!}{(n-(\ell+1))!}X^{n-(\ell+1)}$$

ce qui prouve que $\mathcal{P}_{\ell+1}$ est vraie.

Par récurrence finie, on obtient que pour tout $\ell \in [\![0;n]\!]$, $(X^n)^{(\ell)} = n(n-1)\dots(n-\ell+1)X^{n-\ell} = \dfrac{n!}{(n-l)!}$. □

Proposition 43 - Formule de Leibniz.

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

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

Même démonstration que celle faite dans le chapitre « Dérivation des fonctions d'une variable réelle ».

1.7. Formule de Taylor

Théorème 44 - Formule de Taylor.

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

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

Démonstration. 1. Soit $\ell \in [\![0,n]\!]$.

$$P^{(\ell)} = \left(\sum_{k=0}^{n} a_k X^k\right)^{(\ell)} = \sum_{k=0}^{n} a_k \left(X^k\right)^{(\ell)} = \sum_{k=\ell}^{n} a_k \frac{k!}{(k-\ell)!} X^{k-\ell}$$

car $\left(X^k\right)^{(\ell)} = 0$ si $k<\ell$ et $\left(X^k\right)^{(\ell)} = \dfrac{k!}{(k-\ell)!}X^{k-\ell}$ si $k \geqslant \ell$. Ainsi,

$$\begin{aligned}\widetilde{P}^{(\ell)}(0) &= \sum_{k=\ell}^{n} a_k \frac{k!}{(k-\ell)!}\,0^{k-\ell} \\ &= a_\ell \frac{\ell!}{(\ell-\ell)!} \qquad \text{car } 0^{k-\ell} = \begin{cases} 0 & \text{si} \quad k-\ell>0 \\ 1 & \text{si} \quad k-\ell=0 \end{cases} \\ &= a_\ell\, \ell!\end{aligned}$$

Donc $a_\ell = \dfrac{\widetilde{P}^{(\ell)}(0)}{\ell!}$ et ensuite $P = \sum_{k=0}^{n} \dfrac{\widetilde{P}^{(k)}(0)}{k!} X^k$.

2. Soit $a \in \mathbf{K}$ et $Q = P(X+a)$. On peut démontrer par récurrence que pour tout $k \in [\![0, n]\!]$, $Q^{(k)} = P^{(k)}(X+a)$.
On applique ensuite la formule de Taylor en 0 à Q.

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

Or $P = Q(X-a)$ donc $P = \sum_{k=0}^{n} \dfrac{\widetilde{P}^{(k)}(a)}{k!} (X-a)^k$. □

Corollaire 45.

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

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

2. Arithmétique des polynômes

2.1. Diviseurs et multiples

Définition 46.

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 47.
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 $\lambda \mid A$.
4. $X - 1 \mid X^2 - 1$ car $X^2 - 1 = (X-1)(X+1)$.
5. $2X^2 - 2 \mid X^2 - 1$ car $X^2 - 1 = \dfrac{1}{2}(2X^2 - 2)$.

Exercice d'application 48. Montrer que pour tout $(a, n) \in \mathbf{K} \times \mathbf{N}^\star$, $X - a \mid X^n - a^n$.

↪ Soit $a \in \mathbf{K}$. On a

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

Proposition 49.

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

$$(P \mid Q \text{ et } Q \mid P) \iff \exists\, k \in \mathbf{K}^\star,\ P = kQ.$$

Démonstration.
Si $P \mid Q$ et $Q \mid P$, alors il existe K_1 et K_2 dans $\mathbf{K}[X]$ tels que $Q = K_1 P$ et $P = K_2 Q$. Donc $Q = K_1 K_2 Q$.

Si $Q = 0$, alors $P = K_2 Q = 0$ et la propriété est vraie.

Si $Q \neq 0$, alors $K_1 K_2 = 1$ et donc K_1 et K_2 sont des polynômes constants non-nuls, donc il existe $k \in \mathbf{K}^\star$ tel que $K_2 = k$ et $P = kQ$.

Le sens réciproque est évident. □

Si la condition de la proposition précédente est satisfaite, on dit que les polynômes P et Q sont **associés** .

Proposition 50.

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

1. Si $A \mid B$ et $B \mid C$, alors $A \mid C$.
2. Si $A \mid B$ et $A \mid C$, alors pour tout $(\lambda, \mu) \in \mathbf{K}^2$, $A \mid \lambda B + \mu C$.
3. Si $A \mid B$ et $C \mid D$, alors $AC \mid BD$.

Démonstration. 2. Supposons que $A \mid B$ et $A \mid C$. Soit $(\lambda, \mu) \in \mathbf{K}^2$. Il existe $P_1, P_2 \in \mathbf{K}[X]$ tels que $B = AP_1$ et $C = AP_2$. Ainsi,

$$A = \lambda B + \mu C = A(\underbrace{\lambda P_1 + \mu P_2}_{\in \mathbf{K}[X]}),$$

donc $A \mid \lambda B + \mu C$.
Les autres points sont laissés en exercice. □

Proposition 51.

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

Démonstration.
Si $P \mid Q$, alors il existe $K \in \mathbf{K}[X]$ tel que $PK = Q$. Donc $\deg(PK) = \deg(Q)$.

Donc $\deg(P) + \deg(K) = \deg(Q)$.

Comme Q est non-nul, K est non-nul donc $\deg(K) \leqslant 0$ et donc $\deg(P) \geqslant \deg(Q)$. □

2.2. Division euclidienne de deux polynômes

Théorème 52 - 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. • *Unicité.* Soit $(Q_1, R_1) \in \mathbf{K}[X]^2$ et $(Q_2, R_2) \in \mathbf{K}[X]^2$ tels que $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$. On a donc $BQ_1 + R_1 = BQ_2 + R_2$ d'où $B(Q_1 - Q_2) = R_2 - R_1$.
En prenant le degré de ces polynômes, on obtient :

$$\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) \leqslant \max(\deg(R_1), \deg(R_2)) < \deg(B).$$

Donc $\deg(B) + \deg(Q_1 - Q_2) < \deg(B)$ et donc $\deg(Q_1 - Q_2) < 0$. On en déduit que $Q_1 - Q_2$ est le polynôme nul et que $Q_1 = Q_2$
Comme $R_2 - R_1 = B(Q_1 - Q_2) = B \times 0 = 0$ on a aussi que $R_1 = R_2$.
Ainsi $(Q_1, R_1) = (Q_2, R_2)$.

- *Existence.* On fait une récurrence sur le degré. Posons, pour tout $n \in \mathbf{N}$, H_n : « pour tout polynôme A tel que $\deg(A) < n$, il existe $Q, R \in \mathbf{K}[X]$ tel que $A = BQ+R$ et $\deg(R) < \deg(B)$ ».
Notons $d = \deg(B)$. Puisque $B \neq 0$, $d \geqslant 0$. Soit $A \in \mathbf{K}[X]$ avec $\deg(A) < d$. alors $A = B \times 0 + A$. Ainsi H_k est vraie pour tout $k \leqslant d$.
Soit $n \geqslant d$ tel que H_n soit vraie. Soit $A \in \mathbf{K}[X]$ avec $\deg(A) < n+1$. Notons $A = \sum\limits_{k=0}^{n} a_k X^k$.
Notons b_d le coefficient dominant de B. Considérons
$$A_1 = A - \frac{a_n}{b_d} X^{n-d} \times B.$$
Le coefficient de X^n dans $\frac{a_n}{b_d} X^{n-d} \times B$ est $\frac{a_n}{b_d} \times b_d = a_n$. Ainsi $\deg(A_1) \leqslant n - 1 < n$. D'après H_n, il existe $Q_1, R_1 \in \mathbf{K}[X]$ tel que $A_1 = BQ_1 + R_1$ et $\deg(R_1) < \deg(B)$. Ainsi,
$$B\left(Q_1 + \frac{a_n}{b_d} X^{n-d}\right) + \underbrace{R_1}_{\deg(R_1)<\deg(B)}$$
ce qui prouve H_{n+1}.
Le principe de récurrence permet de conclure. □

$(\mathbf{K}[X], +, \times)$ est un anneau euclidien (*i.e.* un anneau sur lequel on peut définir une division euclidienne). Par conséquent, le théorème de Bézout, le lemme d'Euclide, la notion de PGCD et de PPCM existent aussi pour les polynômes.

◇◇

Remarque technique 53. En pratique, 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.

1. On soustrait à A un multiple de B de sorte que X^4 disparaisse.
$$\begin{array}{rrrrr|l}
X^4 & & +3X^2 & -5X & +1 & X^2 - 3X \\ \cline{6-6}
-X^4 & +3X^3 & & & & X^2 \\ \cline{1-2}
 & 3X^3 & +3X^2 & & &
\end{array}$$
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.
$$\begin{array}{rrrrr|l}
X^4 & & +3X^2 & -5X & +1 & X^2 - 3X \\ \cline{6-6}
-X^4 & +3X^3 & & & & X^2 + 3X \\ \cline{1-2}
 & 3X^3 & +3X^2 & & & \\
 & -3X^3 & +9X^2 & & & \\ \cline{2-3}
 & & 12X^2 & -5X & &
\end{array}$$
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.
$$\begin{array}{rrrrr|l}
X^4 & & +3X^2 & -5X & +1 & X^2 - 3X \\ \cline{6-6}
-X^4 & +3X^3 & & & & X^2 + 3X + 12 \\ \cline{1-2}
 & 3X^3 & +3X^2 & & & \\
 & -3X^3 & +9X^2 & & & \\ \cline{2-3}
 & & 12X^2 & -5X & & \\
 & & -12X^2 & +36X & & \\ \cline{3-4}
 & & & 31X & +1 &
\end{array}$$
Le reste est de degré 1 donc on ne peut plus poursuivre. Finalement, $A = B(X^2 + 3X + 12) + (31X + 1)$.

◇◇

Exemple 54. 1. Effectuons la division euclidienne de $A = X^3 + 3X + 2$ par $B = X^2 + X$.

$$\begin{array}{r|l}
X^3 + 3X^2 \qquad\qquad + 2 & X^2 + X \\ \cline{2-2}
- X^3 \;\; - X^2 \qquad\qquad\quad & X + 2 \\ \cline{1-1}
2X^2 \qquad\quad & \\
- 2X^2 - 2X \qquad & \\ \cline{1-1}
- 2X + 2 &
\end{array}$$

Donc $A = B(X + 2) - (2X + 2)$.

2. Effectuons la division euclidienne de $A = X^7 - 3X + 1$ par $B = X^2 + 1$.

$$\begin{array}{r|l}
X^7 \qquad\qquad\qquad - 3X + 1 & X^2 + 1 \\ \cline{2-2}
- X^7 - X^5 \qquad\qquad\qquad\quad & X^5 - X^3 + X \\ \cline{1-1}
- X^5 \qquad\qquad\qquad\quad & \\
X^5 + X^3 \qquad\qquad\quad & \\ \cline{1-1}
X^3 - 3X \qquad & \\
- X^3 \;\; - X \qquad & \\ \cline{1-1}
- 4X + 1 &
\end{array}$$

Donc $A = B(X^5 - X^3 + X) + (-4X + 1)$.

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

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

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

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

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

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

Exercice d'application 55. Soit $n \in \mathbf{N}$, $\theta \in \mathbf{R}$. Déterminer le reste de la division euclidienne de X^n par $X^2 - 2\cos(\theta)X + 1$.

$\hookrightarrow$ Par le théorème de la division euclidienne, il existe $(Q,R)\in\mathbf{R}[X]^2$ tel que

$$X^n=(X^2-2\cos(\theta)X+1)Q(X)+R(X)$$

avec $\deg(R)<2$. Ainsi il existe $(\lambda,\mu)\in\mathbf{R}^2$ tel que $R=\lambda X+\mu$. En évaluant X^n en $\mathrm{e}^{i\theta}$ et $\mathrm{e}^{-i\theta}$, on obtient

$$\left\{\begin{array}{rcl}\lambda\mathrm{e}^{i\theta}+\mu&=&\mathrm{e}^{in\theta}\\ \lambda\mathrm{e}^{-i\theta}+\mu&=&\mathrm{e}^{-in\theta}\end{array}\right.\iff\left\{\begin{array}{rcl}\lambda&=&\frac{\mathrm{e}^{-in\theta}}{\mathrm{e}^{2i\theta}-1}(\mathrm{e}^{2in\theta+i\theta}-\mathrm{e}^{i\theta})\\ \mu&=&-\frac{\mathrm{e}^{-in\theta}}{\mathrm{e}^{2i\theta}-1}(\mathrm{e}^{2in\theta}-\mathrm{e}^{2i\theta})\end{array}\right.$$

Finalement, $R=\frac{\sin(n\theta)}{\sin(\theta)}X-\frac{\sin((n-1)\theta)}{\sin(\theta)}$.

Remarque 56. 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 57.

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

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

3. Racines d'un polynôme

3.1. Définitions

Proposition 58.

Soit $P\in\mathbf{K}[X]$ et $\alpha\in\mathbf{K}$. Le reste de la division euclidienne de P par $(X-\alpha)$ est $\widetilde{P}(\alpha)$.

Démonstration.
Soit Q et R le quotient et le reste de la division euclidienne de P par $(X-\alpha)$.
On a $P=(X-\alpha)Q+R$ et $\deg(R)<\deg(X-\alpha)$. Or $\deg(X-\alpha)=1$, donc $\deg(R)<1$
Donc R est un polynôme constant, c'est-à-dire qu'il existe $\lambda\in\mathbf{K}$ tel que $R(X)=\lambda$.
On obtient $\widetilde{P}(\alpha)=(\alpha-\alpha)\widetilde{Q}(\alpha)+\widetilde{R}(\alpha)$ donc $\widetilde{P}(\alpha)=\lambda$ donc $R=\widetilde{P}(\alpha)$. □

Définition 59.

Soit $P\in\mathbf{K}[X]$ et $\alpha\in\mathbf{K}$.
On dit que α est une **racine** de P si et seulement si $(X-\alpha)\mid P$ (si et seulement si $\widetilde{P}(\alpha)=0$ d'après la proposition précédente).

Définition 60.

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 si et seulement si les deux conditions suivantes sont satisfaites :

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

Définition 61.

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

- **simple** si et seulement si α est une racine de multiplicité 1 de P.
- **multiple** si et seulement si α est une racine de multiplicité $\geqslant 2$ de P. Plus particulièrement, si une racine de multiplicité 2 (resp. 3) est dite **racine double** (resp. **triple**).

Exemple 62. 1. Soit $(a,b,c) \in \mathbf{K}^\star \times \mathbf{K}^2$. P 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 63.

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

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

Démonstration. • Sens direct. On suppose que α est une racine de multiplicité n de P, *i.e.* $(X-\alpha)^n \mid P$ et $(X-\alpha)^{n+1}$ de divise pas P.
Il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-\alpha)^n Q$ et $(X-\alpha)$ de divise pas Q. Ainsi, α n'est pas une racine de Q et donc $\widetilde{Q}(\alpha) \neq 0$.
Soit $\ell \in [\![0, n]\!]$.

$$P^{(\ell)} = [(X-\alpha)^n Q]^{(\ell)} = \sum_{k=0}^{\ell} \binom{n}{k} [(X-\alpha)^n]^{(k)} \, Q^{(\ell-k)} = \sum_{k=0}^{\ell} \binom{n}{k} \frac{n!}{(n-k)!} (X-\alpha)^{n-k} \, Q^{(\ell-k)}$$

car $k \leqslant \ell \leqslant n$. Ensuite,

$$\widetilde{P}^{(\ell)}(\alpha) = \sum_{k=0}^{\ell} \binom{n}{k} \frac{n!}{(n-k)!} (\alpha-\alpha)^{n-k} \, \widetilde{Q}^{(\ell-k)}(\alpha) = \sum_{k=0}^{\ell} \binom{n}{k} \frac{n!}{(n-k)!} 0^{n-k} \, \widetilde{Q}^{(\ell-k)}(\alpha).$$

◦ Si $\ell < n$, alors $\forall\, k \in [\![0, n]\!]$, $0^{n-k} = 0$ car $n - k \neq 0$ et donc $\widetilde{P}^{(\ell)} = 0$.

◦ Si $\ell = n$, alors

$$\begin{cases} \forall\, k \in [\![0, \ell-1]\!], \quad 0^{n-k} = 0 \\ 0^{n-\ell} = 0^0 = 1 \end{cases}$$

et donc $\widetilde{P}^{(\ell)}(\alpha) = \sum_{k=0}^{n-1} 0 + \binom{n}{n} \frac{n!}{(n-n)!} \widetilde{Q}^{(0)}(\alpha) = n! \, \widetilde{Q}(\alpha) \neq 0$.

• Sens réciproque. On suppose que $\widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = ... = \widetilde{P}^{(n-1)}(\alpha) = 0$ et $\widetilde{P}^{(n)} \neq 0$. On note d le degré de P.
On utilise la formule de Taylor :

$$P = \sum_{k=0}^{d} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^k = \sum_{k=0}^{n-1} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^k + \sum_{k=n}^{d} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^k.$$

On peut faire ce découpage car $n \leqslant d$ (puisque $P^{(n)} \neq 0$). Or

$$\sum_{k=0}^{n-1} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^k = 0$$

donc

$$P = \sum_{k=n}^{d} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^k$$

puis

$$P = (X-\alpha)^n \sum_{k=n}^{d} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (X-\alpha)^{k-n}$$

et on note $P = (X-\alpha)^n Q$. On vient de montrer que $(X-\alpha)^n \mid P$.
De plus,

$$\widetilde{Q}(\alpha) = \sum_{k=n}^{d} \frac{\widetilde{P}^{(k)}(\alpha)}{k!} (\alpha-\alpha)^{k-n}$$

avec $k-n=0$ si $k=n$ et $k-n \neq 0$ si $k>n$, d'où

$$\widetilde{Q}(\alpha) = \frac{\widetilde{P}^{(n)}(\alpha)}{n!} \times 1 + \sum_{k=n+1}^{d} 0 = \frac{\widetilde{P}^{(n)}(\alpha)}{n!} \neq 0.$$

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

Proposition 64.

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 65. 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.

3.2. Factorisation d'un polynôme

Proposition 66.

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)⟹(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

$$\widetilde{P}(\alpha_{r+1}) = \underbrace{\prod_{k=1}^{r} (X-\alpha_k)^{m_k}}_{\neq 0} \widetilde{Q}(\alpha_{r+1}).$$

Or $\widetilde{P}(\alpha_{r+1}) = 0$ car α_{r+1} est racine de P, donc $\widetilde{Q}(\alpha_{r+1}) = 0$, *i.e.* 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

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

Ensuite,

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

On a alors $Q_2(\alpha_{r+1}) = Q_1(\alpha_{r+1}) \times \prod_{k=1}^{r} (\alpha_{r+1}-\alpha_k)^{m_k} \neq 0$. Ainsi α_{r+1} est racine de P d'ordre de multiplicité exactement m. Par suite, $m_{r+1} \leqslant m$ et $\prod_{k=1}^{r+1} (X-\alpha_k)^{m_k}$ divise $(X-\alpha_{r+1})^m \prod_{k=1}^{r} (X-\alpha_k)^{m_k}$ et donc aussi P. D'où H_{r+1}.
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 Proposition 64. □

Exemple 67. $P^n - 1$ possède n racines simples, à savoir $\mathrm{e}^{i\frac{2k\pi}{n}}$ pour $k \in [\![0, n-1]\!]$. Ainsi,

$$\underbrace{\prod_{k=1}^{n} (X - \mathrm{e}^{i\frac{2k\pi}{n}})}_{\text{degré } n} \mid \underbrace{X^n - 1}_{\text{degré } n}.$$

Donc le quotient de ces deux polynômes est de degré 0, ce qui entraîne l'existence de $\lambda \in \mathbf{C}^\star$ tel que

$$\underbrace{X^n - 1}_{\text{coeff. dominant : 1}} = \lambda \times \underbrace{\prod_{k=1}^{n} (X - \mathrm{e}^{i\frac{2k\pi}{n}})}_{\text{coeff. dominant : 1}}.$$

Donc $\lambda = 1$.

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

Corollaire 68.

Soit $P \in \mathbf{K}[X]$ 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. $m_1 + ... + m_r \leqslant \deg(P)$
2. Si $m_1 + ... + m_r = \deg(P)$, alors
   - $\alpha_1, ..., \alpha_r$ sont les racines de P.
   - $P = \lambda \prod_{k=1}^{r} (X-\alpha_k)^{m_k}$ où λ est le coefficient dominant de P.

Exemple 69. $P = 2X^4 - 7X^3 + 6X^2 + X - 2$ 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 70.

Soit $n \in \mathbf{N}$. Si P est de degré au plus n et possède $n+1$ racines, alors $P = 0$. En particulier, si $P, Q \in \mathbf{K}[X]$ coïncident sur une partie infinie de $\mathbf{K}$, alors $P = Q$.

Démonstration.
La première partie du corollaire est une conséquence directe du corollaire précédente. Soit $P, Q \in \mathbf{K}[X]$, soit $E \in \mathcal{P}(\mathbf{K})$ infinie telle que pour tout $x \in E$, $\widetilde{P}(x) = \widetilde{Q}(x)$. Alors $P - Q$ possède une infinité de racines, donc $P - Q = 0$. □

Corollaire 71.

L'application $\Phi : \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathcal{E} \\ P & \longmapsto & \widetilde{P} \end{array}$ est bijective, où

$$\mathcal{E} = \left\{ f \in \mathcal{F}(\mathbf{K}, \mathbf{K}) \;\middle|\; \exists n \in \mathbf{N}, \exists (a_0, \ldots, a_n) \in \mathbf{K}^n,\ \forall x \in \mathbf{K},\ f(x) = \sum_{k=0}^{n} a_k x^k \right\}.$$

Démonstration.
Soit $f \in \mathcal{E}$. Il existe $n \in \mathbf{N}$, $(a_0, \ldots, a_n) \in \mathbf{K}^n$ tel que $f : x \longmapsto \sum_{k=0}^{n} a_k x^k$. En posant $P = \sum_{k=0}^{n} a_k X^k$, on a $\Phi(P) = f$. Ainsi Φ est surjective.
Soit $P_1, P_2 \in \mathbf{K}[X]$ tels que $\Phi(P_1) = \Phi(P_2)$. Alors $\Phi(P_1 - P_2) = 0$, donc $x \longmapsto \widetilde{P_1}(x) - \widetilde{P_2}(x)$ est nulle, ce qui entraîne que $P_1 - P_2$ admet une infinité de racines puis $P_1 = P_2$. Ainsi Φ est injective. □

Le corollaire précédent justifie l'identification faite entre les polynômes et les fonctions polynomiales.

Définition 72.

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

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

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 73.

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

Exemple 74.
1. $2X^4 - 7X^3 + 6X^2 + X - 2 = 2(X-1)^2(X-2)(X-\frac{1}{2})$ 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 75.

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

Exemple 76. 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 $X^{12} - 1$.

Proposition 77.

Soit $P \in \mathbf{K}[X]$, $\alpha_1, ..., \alpha_r$ des racines de P de multiplicités respectives $m_1, ..., m_r \in \mathbf{N}^\star$ où $r \in \mathbf{N}^\star$.
Pour tout $k \in [\![1, r]\!]$, si $m_k \geqslant 2$, alors α_k est une racine de P' de multiplicité $m_k - 1$.

Démonstration.
Immédiat grâce à la Proposition 64. □

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

4.1. 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. La notion de nombre premier dans $N^\star$ a son analogue dans $\mathbf{K}[X]$: la notion de polynôme irréductible 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 $\mathbf{K}$ pour assurer l'unicité de la décomposition dans $\mathbf{K}[X]$.

Définition 78.

Soit $P \in \mathbf{K}[X]$. On dit que P est **irréductible** si et seulement si $\deg(P) \geqslant 1$ et

$$\forall (A, B) \in \mathbf{K}[X]^2, \quad P = AB \Longrightarrow \deg(A) = 0 \text{ ou } \deg(B) = 0.$$

Remarque 79. Soit $P \in \mathbf{K}[X]$ de degré supérieur ou égal à 1.
P est irréductible si et seulement si ses seuls diviseurs sont les constantes non nulles et les produits de P par une constante non nulle. Sous cette forme, on comprend plus facilement l'analogie avec la notion de nombre premier sur $\mathbf{Z}$.

Exemple 80. On a $X^2+1 = (X-i)(X+i)$ dans $\mathbf{C}[X]$, donc $X-i \mid X^2+1$. Par ailleurs, $\deg(X-i) \neq 0$ et $\deg(X-i) \neq \deg(X^2+1)$, donc X^2+1 n'est pas irréductible dans $\mathbf{C}[X]$.

Montrons que X^2+1 est irréductible dans $\mathbf{R}[X]$. Soit $P \in \mathbf{R}[X]\backslash\{0\}$ 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.
Supposons $\deg(P) = 2$: il existe $\lambda \in \mathbf{K}^\star$ tel que $X^2+1 = \lambda P$, donc $P = \frac{1}{\lambda}(X^2+1)$.

Exercice d'application 81. Montrer qu'un polynôme réel de degré $n \geqslant 3$ impair n'est jamais irréductible.

$\hookrightarrow$ Notons $n = \deg(P)$ et a_n le coefficient dominant de P. On a $\widetilde{P}(x) \underset{x\to+\infty}{\sim} a_n x^n$ et $\widetilde{P}(x) \underset{x\to-\infty}{\sim} a_n x^n$, et en particulier les limites en $-\infty$ et $+\infty$ de $\widetilde{P}$ sont infinies de signe contraire. A l'aide du théorème des valeurs intermédiaires, on peut en déduire qu'il existe $\alpha \in \mathbf{R}$ tel que $\widetilde{P}(\alpha) = 0$. Donc $(X-\alpha) \mid P$, et donc P n'est pas 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 82.

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.
Soit $\alpha \in \mathbf{K}$ une racine de P. Il existe $Q \in \mathbf{K}[X]$ tel que $P = (X-\alpha)Q$. On obtient $\deg(Q) = \deg(P)-1 \geqslant 1$. □

⚠ **Attention** ⚠**.** La réciproque est fausse. X^2+1 est irréductible sur $\mathbf{R}$ et n'a pas de racines réelles.

Théorème 83.

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

Démonstration.
Soit $P \in \mathbf{K}[X]$ avec $\deg(P) = 1$. Soit $(A,B) \in \mathbf{K}[X]^2$ tel que $P = AB$. On a $1 = \deg(P) = \deg(A) + \deg(B)$, d'où $(\deg(A), \deg(B)) \in \{(0,1),(1,0)\}$. Ainsi P est irréductible. □

4.2. Décomposition dans $\mathbf{C}[X]$

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

Théorème 84 - Théorème de D'Alembert-Gauss.

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

Démonstration.
Admis (difficile). □

La propriété énoncée dans le théorème de D'Alembert-Gauss signifie que $\mathbf{C}$ est algébriquement clos.

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 de degré supérieur ou égal à 5 : « l'équation polynomiale générale de degré supérieur ou égal à 5 n'est pas résolution par radicaux ». Ceci n'empêche pas de savoir résoudre, ponctuellement, certaines équations de degré 5 (comme $z^5-1=0$ d'inconnue $z\in\mathbf{C}$ par exemple).

Corollaire 85.

Tout polynôme de degré supérieur ou égal à 1 de $\mathbf{C}[X]$ est scindé sur $\mathbf{C}$.
Plus précisément, pour tout élément P de $\mathbf{C}[X]$ de degré $n\geqslant 1$, il existe $\lambda\in\mathbf{C}^\star$ et $(a_1,\dots,a_n)\in\mathbf{C}^n$ tel que

$$P=\lambda(X-a_1)\dots(X-a_n).$$

Démonstration.
Pour tout $n\in\mathbf{N}^\star$, on pose H_n : « tout polynôme de $\mathbf{C}[X]$ de degré n est scindé sur $\mathbf{C}$ ».

Tout élément de $\mathbf{C}[X]$ de degré 1 est produit d'un polynôme de degré, donc H_1 est vraie.

Soit $n\in\mathbf{N}$ tel que H_n soit vraie. Soit $P\in\mathbf{C}[X]$ de degré $n+1$. D'après le théorème de d'Alembert-Gauss, comme $n+1\geqslant 1$, P admet au moins une racine $a\in\mathbf{C}$. Alors $(X-a)$ divise P et il existe $Q\in\mathbf{K}[X]$ tel que $P(X)=(X-a)Q(X)$. Or $\deg(Q)=n$ donc H_n fournit que Q est scindé. Il s'ensuit qu'il existe $(\lambda,a_1,...,a_n)\in\mathbf{C}^{n+1}$ tel que

$$Q=\lambda(X-a_1)\cdots(X-a_n).$$

Ainsi $P=\lambda(X-a)(X-a_1)\cdots(X-a_n)$ est scindé donc H_{n+1} est vraie.

Finalement le principe de récurrence permet de conclure. □

Théorème 86.

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

Démonstration.
- Le Théorème 83 assure que les polynômes de degré 1 sont irréductibles.
- Soit $P\in\mathbf{K}[X]$ de degré supérieur ou égal à 2. Le théorème de D'Alembert-Gauss assure que P possède une racine et la Proposition 82 permet de conclure. □

Théorème 87 - Décomposition des polynômes à coefficients dans C.

Soit $P \in \mathbf{C}[X]$ de degré $n \geqslant 1$. P se décompose de manière unique à l'ordre près des facteurs sous la forme

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

avec

- λ le coefficient dominant de P ;
- $\alpha_1, ..., \alpha_r \in \mathbf{C}$ les racines complexes distinctes de P ;
- $m_1, ..., m_r \in \mathbf{N}^\star$ les ordres de multiplicité respectifs de $\alpha_1, ..., \alpha_r$.

Ainsi tout polynôme de $\mathbf{C}[X]$ se décompose de manière unique, à l'ordre des facteurs près, en produit de polynôme irréductibles de $\mathbf{C}[X]$.

Démonstration.
L'unicité de la décomposition vient du fait que nécessairement λ est le coefficient dominant de P, $\alpha_1, ..., \alpha_k$ sont nécessairement les racines deux à deux distinctes de P et $m_1, ..., m_k$ leurs ordres de multiplicités respectifs.

D'après le Corollaire 85, P est scindé sur $\mathbf{C}[X]$, d'où l'existence d'une telle factorisation. □

Exemple 88.
1. $X^3 - 1 = (X-1)(X-j)(X-j^2)$, où $j = e^{\frac{2i\pi}{3}}$.
2. $X^4 - 1 = (X-1)(X-i)(X+1)(X+i)$.

◇◇

Remarque technique 89. Pour factoriser un polynôme dans $\mathbf{C}[X]$, on cherche toutes ses racines.

Exercice d'application 90. Factoriser dans $\mathbf{C}[X]$ le polynôme $X^4 + 1$.

↪ Pour $z \in \mathbf{C}$, $z^4 = -1 \iff z^4 = e^{i\pi} \iff \exists k \in [\![0,3]\!],\ z = e^{i\frac{\pi+2k\pi}{4}}$. Ainsi

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

Exercice d'application 91. Factoriser dans $\mathbf{C}[X]$ le polynôme $X^6 + X^3 + 1$.

↪ Soit $z \in \mathbf{C}$.

$$\begin{aligned} z^6 + z^3 + 1 = 0 &\iff (z^3)^2 + (z^3) + 1 = 0 \\ &\iff z^3 = j \text{ ou } z^3 = j^2 \\ &\iff \exists k \in [\![0,2]\!],\ z = e^{i(\frac{2\pi}{9} + \frac{2k\pi}{3})} \text{ ou } z = e^{i(\frac{4\pi}{9} + \frac{2k\pi}{3})} \end{aligned}$$

Finalement,

$$P = (X - e^{i\frac{2\pi}{9}})(X - e^{i\frac{8\pi}{9}})(X - e^{i\frac{14\pi}{9}})(X - e^{i\frac{10\pi}{9}})(X - e^{i\frac{16\pi}{9}})(X - e^{i\frac{4\pi}{9}}).$$

◇◇

4.3. Polynôme conjugué

Définition 92.

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 donnée ci-après.

Proposition 93.

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. $\overline{A(z)} = \overline{A}(\overline{z})$.

Démonstration.
Notons $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{n} b_k X^k$, où a_k, b_k sont des complexes éventuellement nuls.

1. $\overline{A+B} = \sum_{k=0}^{n} \overline{a_k + b_k} X^k = \sum_{k=0}^{n} (\overline{a_k} + \overline{b_k}) X^k = \sum_{k=0}^{n} \overline{a_k} X^k + \overline{b_k} X^k = \overline{A} + \overline{B}$.
2. $\overline{\lambda \cdot P} = \sum_{k=0}^{n} \overline{\lambda a_k} X^k = \sum_{k=0}^{n} (\overline{\lambda} \cdot \overline{a_k}) X^k = \overline{\lambda} \sum_{k=0}^{n} \overline{a_k} X^k = \overline{\lambda} \cdot \overline{A}$.
3. $\overline{A \times B} = \sum_{k=0}^{2n} \overline{\left(\sum_{p=0}^{k} a_p b_{k-p} \right)} X^k = \sum_{k=0}^{2n} \left(\sum_{p=0}^{k} \overline{a_p} \cdot \overline{b_{n-p}} \right) X^k = \overline{A} \times \overline{B}$.
4. $\overline{\overline{A}} = \overline{\left(\sum_{k=0}^{n} \overline{a_k} X^k \right)} = \sum_{k=0}^{n} \overline{\overline{a_k}} X^k = \sum_{k=0}^{n} a_k X^k = A$.
5. $A \in \mathbf{R}[X] \iff \forall k \in [\![1, n]\!],\ a_k \in \mathbf{R} \iff \forall k \in [\![1, n]\!],\ \overline{a_k} = a_k \iff \overline{A} = A$.
6. $\overline{A(z)} = \overline{\left(\sum_{k=0}^{n} a_k z^k \right)} = \sum_{k=0}^{n} \overline{a_k} \overline{z}^k = \overline{A}(\overline{z})$. □

Proposition 94.

Soit $P \in \mathbf{R}[X]$ de degré supérieur ou égal à 1. Soit $z \in \mathbf{C}$.
z est une racine de P si et seulement si $\overline{z}$ est racine de P. Le cas échéant, z et $\overline{z}$ ont même ordre de multiplicité.

Démonstration.
On suppose que z est racine de P. Notons $k \in \mathbf{N}^\star$ l'ordre de multiplicité de z. Alors il existe $Q \in \mathbf{C}[X]$ tel que $P = (X-z)^k Q$ et $Q(z) \neq 0$. En conjuguant cette égalité, on obtient que $P = (X-\overline{z})^k \overline{Q}$ (puisque $\overline{P} = P$). Donc $\overline{z}$ est racine de multiplicité au moins k. Par ailleurs, $\overline{Q}(\overline{z}) = \overline{Q(z)} \neq 0$, donc $\overline{z}$ est racine de P de multiplicité exactement k.

□

4.4. Factorisation dans $\mathbf{R}[X]$

Théorème 95.

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

Démonstration.
- Le Théorème 83 assure que les polynômes de degré 1 sont irréductibles.
- Soit $P \in \mathbf{R}[X]$ de degré 2 sans racines réelles. Soit $A, B \in \mathbf{R}[X]$ tels que $P = AB$. Alors $2 = \deg(A) + \deg(B)$, donc $(\deg(A), \deg(B)) \in \{(0,2),(1,1),(2,0)\}$. Supposons que $\deg(A) = 1$ et $\deg(B) = 1$. Il existe $(a,b) \in \mathbf{R}^\star \times \mathbf{R}$ tel que $A = aX + b$. Ainsi $aX + b \mid P$ et $-\frac{b}{a}$ est racine de P, ce qui est contradictoire.
- Soit $P \in \mathbf{R}[X]$ de degré supérieur ou égal à 3. Le théorème de d'Alembert-Gauss que P admet une racine $\alpha \in \mathbf{C}$.
  Si $\alpha \in \mathbf{R}$, la Proposition 82 permet de conclure.
  Si $\alpha \notin \mathbf{R}$, $\overline{\alpha}$ est aussi une racine de P (avec $\alpha \neq \overline{\alpha}$). Ainsi P est divisible par $(X-\alpha)(X-\overline{\alpha}) = (X^2 - 2\mathfrak{Re}(\alpha)X + |\alpha|^2) \in \mathbf{R}[X]$. Ainsi il existe $Q \in \mathbf{R}[X]$ tel que $P = Q(X-\alpha)(X-\overline{\alpha})$. En considérant les degrés, on obtient que $\deg(Q) = \deg(P) - 2 \geqslant 1$, ce qui montre que P n'est pas irréductible. □

Remarque 96. Si P est de degré 2 à coefficients réels, les assertions « P est irréductible sur $\mathbf{R}$ » et « P n'a pas de racine réelle » sont équivalentes. Ce résultat est faux dans le cas général. On a par exemple constaté ci-avant que le polynôme $X^4 + X^2 + 1$ n'a pas de racine réelle et pourtant n'est pas irréductible sur $\mathbf{R}$.

Exercice d'application 97. Soit $\theta \in \mathbf{R}$. Soit $A = X^2 - 2\cos(\theta)X + 1$. A quelle condition nécessaire et suffisante A est-il irréductible sur $\mathbf{R}$?

$\hookrightarrow$ A est irréductible sur $\mathbf{R}$ si et seulement si son discriminant est strictement négatif. Or

$$\cos^2(\theta) - 1 < 0 \iff -\sin^2(\theta) < 0.$$

Finalement, P est irréductible si et seulement si θ n'est pas multiple de π.
Notons qu'on peut déterminer la décomposition de P sur $\mathbf{C}[X]$.

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

De plus, $\mathrm{e}^{i\theta} = \mathrm{e}^{-i\theta} \iff \mathrm{e}^{2i\theta} = 1 \iff 2\theta \in 2\pi\mathbf{Z} \iff \theta \in \pi\mathbf{Z}$: on retrouve la condition nécessaire et suffisante obtenue avant (les racines sont ici conjuguées ; elles sont donc complexes si et seulement si elles sont distinctes). On peut ainsi obtenir la décomposition de P sur $\mathbf{R}[X]$.
- Si $\theta \notin \pi\mathbf{Z}$, $A = X^2 - 2\cos\theta X + 1$.
- Si $\theta \in 2\pi\mathbf{Z}$, $A = X^2 - 2X + 1 = (X-1)^2$.
- Si $\theta \in \pi + 2\pi\mathbf{Z}$, $A = X^2 + 2X + 1 = (X+1)^2$.

On peut maintenant se diriger vers la factorisation sur $\mathbf{R}[X]$ à partir du théorème de décomposition sur $\mathbf{C}[X]$ (on considère $\mathbf{R}$ comme un sous-ensemble de $\mathbf{C}$ et l'« inclusion » $\mathbf{R}[X] \subset \mathbf{C}[X]$).

Soit P un élément de $\mathbf{R}[X]$ de degré supérieur ou égal à 1. Notons λ le coefficient dominant de P, $\alpha_1, ..., \alpha_r$ les r racines réelles de P (avec $r \in \mathbf{N}$) de multiplicités respectives $m_1, ..., m_r$, $\omega_1, ..., \omega_s$ les s racines complexes de partie imaginaire strictement positives (avec $s \in \mathbf{N}$) de multiplicités respectives $n_1, ..., n_s$. On obtient, avec la Proposition 94, que $\overline{\omega_1}, ..., \overline{\omega_s}$ sont exactement les racines complexes de partie imaginaire strictement négative, de multiplicités respectives $n_1, ..., n_s$. Ainsi, le théorème de décomposition sur $\mathbf{C}[X]$ donne

$$P = \lambda \left(\prod_{k=1}^{r} (X - \alpha_k)^{m_k} \right) \left(\prod_{k=1}^{s} (X - \omega_k)^{n_k} (X - \overline{\omega_k})^{n_k} \right).$$

En regroupant les facteurs conjugués et en utilisant que pour tout $k \in [\![1, s]\!]$, $(X - \omega_k)(X - \overline{\omega_k}) = X^2 - 2\mathfrak{Re}(\omega_k)X + |\omega_k|^2$, on obtient

$$P = \lambda \left(\prod_{k=1}^{r} (X - \alpha_k)^{m_k} \right) \left(\prod_{k=1}^{s} (X^2 + b_k X + c_k)^{n_k} \right).$$

où $b_k = -2\mathfrak{Re}(\omega_k)$ et $c_k = |\omega_k|^2$ sont deux réels. On a par ailleurs, pour tout $k \in [\![1, s]\!]$, $b_k^2 - 4c_k < 0$, puisque, pour tout $k \in [\![1, s]\!]$, les racines de $X^2 + b_k X + c_k$ sont les complexes non réels ω_k et $\overline{\omega_k}$.

Théorème 98 - 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 sous la forme :

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

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).

Ainsi tout polynôme de $\mathbf{R}[X]$ se décompose de manière unique, à l'ordre des facteurs près, en produit de polynôme irréductibles de $\mathbf{R}[X]$.

◇◇

Remarque technique 99. Pour décomposer dans $\mathbf{R}[X]$ ou $\mathbf{C}[X]$, on peut chercher des racines évidentes α, déterminer leur multiplicité m à l'aide de polynômes dérivés puis factoriser par $(X - \alpha)^m$. S'il reste des polynômes de degré 2 dans la factorisation obtenue, il faudra bien vérifier que le discriminant de ces trinômes est négatif avant de conclure.

Exercice d'application 100. Décomposer $P = X^4 - 2X^3 + 2X^2 - 2X + 1$ dans $\mathbf{R}[X]$ et $\mathbf{C}[X]$.

$\hookrightarrow$ On remarque que $\widetilde{P}(1) = 0$ donc 1 est une racine de P. De plus, $P' = 4X^3 - 6X^2 + 4X - 2$, puis $\widetilde{P'}(1) = 4 - 6 + 4 - 2 = 0$ donc 1 est une racine au moins double de P. Ainsi, il existe $Q \in \mathbf{C}[X]$ tel que $P = (X - 1)^2\, Q$. Une division euclidienne permet de déterminer Q :

$$\begin{array}{r|l} X^4 - 2X^3 + 2X^2 - 2X + 1 & X^2 - 2X + 1 \\ \cline{2-2} -X^4 + 2X^3 \;\; - X^2 & X^2 + 1 \\ \hline X^2 - 2X + 1 & \\ -X^2 + 2X - 1 & \\ \hline 0 & \end{array}$$

Ainsi, $P = (X - 1)^2(X^2 + 1)$.
$X^2 + 1$ est un polynôme de second degré et ne possède pas de racines réelles donc il s'agit de la décomposition de P dans $\mathbf{R}[X]$.
La décomposition dans $\mathbf{C}[X]$ est $P = (X - 1)^2(X - i)(X + i)$.

◇◇

◇◇

Remarque technique 101. Si on connaît la décomposition d'un polynôme dans $\mathbf{C}[X]$, on peut facilement le factoriser dans $\mathbf{R}[X]$ en regroupant les expressions conjuguées.

Exercice d'application 102. Factoriser dans $\mathbf{R}[X]$ le polynôme $X^3 - 1$.

$\hookrightarrow$ On a obtenu dans $\mathbf{C}[X]$, $X^3 - 1 = (X - 1)(X - j)(X - j^2)$, d'où dans $\mathbf{R}[X]$, $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

Notons qu'on aurait aussi pu remarquer que 1 était racine simple évidente, puis conclure avec une division euclidienne.

Exercice d'application 103. Factoriser $X^6 + X^3 + 1$ dans $\mathbf{R}[X]$.

$\hookrightarrow$ A partir de la décomposition dans $\mathbf{C}[X]$:

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

◇◇◇

Exercice d'application 104. Factoriser dans $\mathbf{R}[X]$, X^4+1.

$\hookrightarrow$ *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.

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

Exercice d'application 105. Soit $n\in\mathbf{N}^\star$. Déterminer la factorisation dans $\mathbf{R}[X]$ de X^n-1.

$\hookrightarrow$ 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,

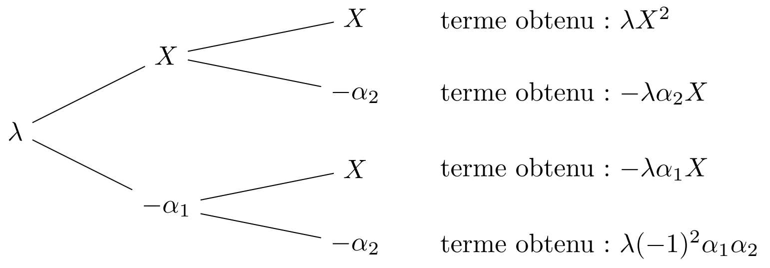
$$\begin{aligned} X^{2k}-1 &= (X-1)(X+1)\prod_{p=1}^{k-1}\left(X-\mathrm{e}^{i\frac{2p\pi}{n}}\right)\left(X-\mathrm{e}^{-i\frac{2p\pi}{n}}\right) \\ &= (X-1)(X+1)\prod_{p=1}^{k-1}\left(X-2\cos\left(\frac{p\pi}{n}\right)+1\right). \end{aligned}$$

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

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

5. Relations coefficients-racines

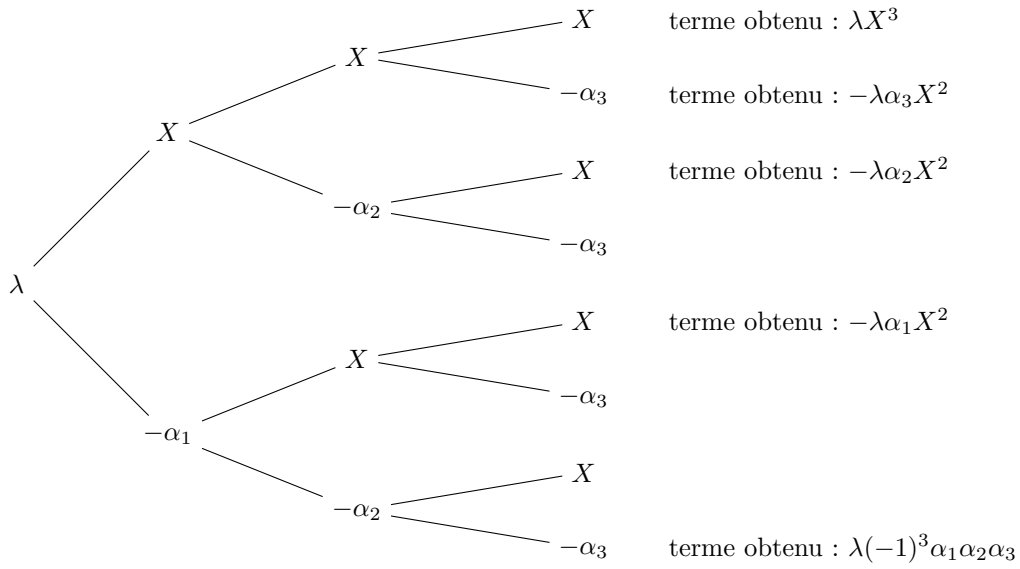
Soit $P\in\mathbf{K}[X]$ un polynôme scindé de degré 2 qu'on note $P=\sum_{k=0}^{2}a_kX^k$. Notons de plus α_1,α_2 ses racines. Développons $\lambda(X-\alpha_1)(X-\alpha_2)$:



En identifiant, on obtient que $a_2 = \lambda$, $a_1 = \lambda(-\alpha_1 - \alpha_2)$ et $a_0 = \lambda(-1)^2\alpha_1\alpha_2$ et on retrouve les relations coefficients-racines déjà mentionnées :

$$\sum_{k=1}^{2} \alpha_k = -\frac{a_1}{a_2} \quad \text{et} \quad \prod_{k=1}^{2} \alpha_k = (-1)^2\frac{a_0}{a_2}.$$

Soit $P \in \mathbf{K}[X]$ un polynôme scindé de degré 3 qu'on note $P = \sum_{k=0}^{3} a_k X^k$. Notons de plus $\alpha_1\alpha_2$, α_3 ses racines. Développons $\lambda(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$:



En identifiant, on obtient que $a_3 = \lambda$, $a_2 = \lambda(-\alpha_1 - \alpha_2 - \alpha_3)$ et $a_0 = \lambda(-1)^3\alpha_1\alpha_2\alpha_3$ et ainsi :

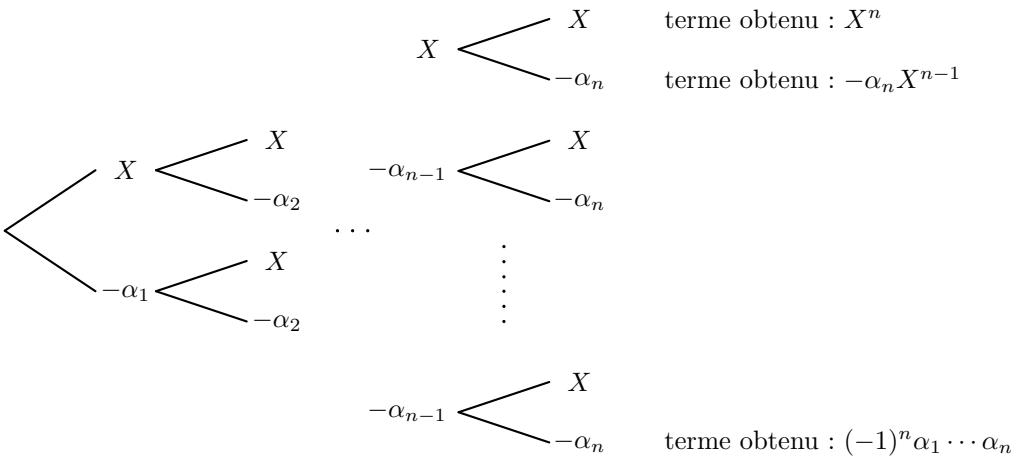
$$\sum_{k=1}^{3} \alpha_k = -\frac{a_1}{a_3} \quad \text{et} \quad \prod_{k=1}^{3} \alpha_k = (-1)^3\frac{a_0}{a_3}.$$

Proposition 106 - Relations de Viète.

Soit $P \in \mathbf{K}[X]$ un polynôme scindé. Notons $n = \deg(P)$, $P = \sum_{k=0}^{n} a_k X^k$ 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 107. Soit $n \in \mathbf{N}^\star$. $X^n - 1 = \prod_{k=0}^{n-1} (X - \mathrm{e}^{i\frac{2k\pi}{n}})$. Les relations coefficients-racines s'écrivent

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