Chapitre 17 : Polynômes

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

1 Ensemble $\mathbb{K}[X]$

1.1 Définitions

Définition

- On appelle **polynôme** P à coefficients dans $\mathbb{K}$ en l'indéterminée X tout objet de la forme :

$$P = \sum_{k=0}^{n} a_k X^k$$

où $n \in \mathbb{N}$, $a_0, \ldots, a_n \in \mathbb{K}$.
L'ensemble des polynômes à coefficients dans $\mathbb{K}$ en l'indéterminée X est noté $\mathbb{K}[X]$.

Remarque : On peut poser : $\forall k > n, a_k = 0$ et écrire $P = \sum_{k\geq 0} a_k X^k$ avec (a_k) une suite nulle à partir d'un certain rang.

Exemple : $P = 2 + X + X^2$ est un polynôme de $\mathbb{R}[X]$.

Définition

On dit que deux polynômes $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k \in \mathbb{K}[X]$ sont égaux si et seulement si ils ont les mêmes coefficients :

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

Définition

On appelle polynôme nul le polynôme dont tous les coefficients sont nuls.

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$. On définit :

- la somme : $P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$
- le produit par λ : $\lambda.P = \sum_{k=0}^{n} (\lambda a_k) X^k$
- le produit des polynômes : $P \times Q = \sum_{k=0}^{n+m} c_k X^k$ où $\forall k \in [\![0, n+m]\!]$, $c_k = \sum_{l=0}^{k} a_l b_{k-l} = \sum_{\substack{l,j \in [\![0,k]\!] \\ l+j=k}} a_l b_j$

Remarque : Si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, $P + Q, \lambda.P$ et $P \times Q \in \mathbb{K}[X]$
Exemple : Notons $P = 1 + 2X + 3X^2$ et $Q = 3 - X$. Alors $P + Q = 4 + X + 3X^2$ et $P \times Q = 3 + 5X + 7X^2 - 3X^3$.

Proposition : Propriétés de +

Soit $(P, Q, R) \in \mathbb{K}[X]^3$.

- $(P + Q) + R = P + (Q + R)$ (Associativité)
- $P + Q = Q + P$ (Commutativité).
- $0 + P = P + 0 = P$

Démonstration. laissée en exercice □

Proposition : Propriétés de $\times$

Soit $(P, Q, R) \in \mathbb{K}[X]^3$ et soit $\lambda \in \mathbb{K}$.

- $(P \times Q) \times R = P \times (Q \times R)$ (Associativité de $\times$).
- $P \times Q = Q \times P$ (Commutativité de $\times$).
- $1 \times P = P \times 1 = P$.
- $P \times (Q + R) = (P \times Q) + (P \times R)$ (distributivité de $\times$ sur $+$).
- $\lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$.

Démonstration. Notons $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{n} b_k X^k$ et $R = \sum_{k=0}^{n} c_k X^k \in \mathbb{K}[X]$.

- On note également $PQ = \sum_{k=0}^{2n} d_k X^k$, $QR = \sum_{k=0}^{2n} e_k X^k$, $(P \times Q) \times R = \sum_{k=0}^{3n} g_k X^k$ et $P \times (Q \times R) = \sum_{k=0}^{3n} h_k X^k$.
  Soit $k \in [\![0, 3n]\!]$, on a alors :

$$\begin{aligned} g_k &= \sum_{l=0}^{k} d_l c_{k-l} \\ &= \sum_{l=0}^{n} \sum_{m=0}^{l} a_m b_{l-m} c_{k-l} \end{aligned}$$

  De même, on a :

$$\begin{aligned} h_k &= \sum_{m=0}^{k} a_m e_{k-m} \\ &= \sum_{m=0}^{k} \sum_{p=0}^{k-m} a_m b_p c_{k-m-p} \\ &= \sum_{m=0}^{k} \sum_{l=m}^{k} a_m b_{l-m} c_{k-l} a_k \quad \text{en posant } l = m + p \end{aligned}$$

  Or,

$$\begin{cases} 0 \le m \le k \\ m \le l \le k \end{cases} \iff \begin{cases} 0 \le m \le l \\ 0 \le l \le k \end{cases}$$

  Ainsi :

$$\begin{aligned} h_k &= \sum_{l=0}^{k} \sum_{m=0}^{l} a_m b_{l-m} c_{k-l} \\ &= g_k \end{aligned}$$

  Ainsi , on a :

$$\forall k \in [\![0, 3n]\!], \; h_k = g_k$$

  donc $(P \times Q) \times R = P \times (Q \times R)$.

- On note $QP = \sum_{k=0}^{2n} d'_k X^k \in \mathbb{K}[X]$.
  Soit $k \in [\![0, 2n]\!]$, on a :

$$\begin{aligned} d_k &= \sum_{l=0}^{k} a_l b_{k-l} \\ &= \sum_{m=0}^{k} a_{k-m} b_m \quad \text{en posant } m = k - l \\ &= d'_k \end{aligned}$$

  donc $P \times Q = Q \times P$.

- Notons $P \times 1 = \sum_{k=0}^{n} p_k X^k$ et $1 = \sum_{k=0}^{n} r_k X^k$.
  On a : $\forall k \in \mathbb{N},\ r_k = \delta_{k,0}$. Soit $k \in [\![0, n]\!]$, on a :

$$\begin{aligned} p_k &= \sum_{l=0}^{k} a_l r_{k-l} \\ &= \sum_{l=0}^{k} a_l \delta_{k-l,0} \\ &= a_k \end{aligned}$$

  donc $P \times 1 = P$.
  Par commutativité, on a également, $1 \times P = P$.

- On note $Q + R = \sum_{k=0}^{n} s_k X^k$, $P \times R = \sum_{k=0}^{n} t_k X^k$, $P \times (Q+R) = \sum_{k=0}^{2n} u_k X^k$ et $P \times Q + P \times R = \sum_{k=0}^{2n} v_k X^k$.
  Soit $k \in [\![0, 2n]\!]$, on a :

$$\begin{aligned} u_k &= \sum_{l=0}^{k} a_l s_{k-l} \\ &= \sum_{l=0}^{k} a_l (b_{k-l} + c_{k-l}) \\ &= \sum_{l=0}^{k} a_l b_{k-l} + \sum_{l=0}^{k} a_l c_{k-l} \\ &= d_k + t_k \\ &= v_k \end{aligned}$$

  Donc $P \times (Q+R) = P \times Q + P \times R$.

$\square$

Définition

Soit $P \in \mathbb{K}[X]$, pour tout $n \in \mathbb{N}$, on définit par récurrence P^n en posant $P^0 = 1$, et $\forall n \in \mathbb{N},\ P^{n+1} = P^n \times P$.

Définition

Soit $P = \sum_{k=0}^{n} a_k X^k, Q = \sum_{i=0}^{m} b_i X^i \in \mathbb{K}[X]$. On définit le polynôme composé, noté $P \circ Q$ ou $P(Q)$ par :

$$P \circ Q = \sum_{k=0}^{n} a_k Q^k = \sum_{k=0}^{n} a_k \left(\sum_{l=0}^{m} b_l X^l \right)^k.$$

Exemple : $(X^2+1) \circ (X-2) = (X-2)^2 + 1 = X^2 - 4X + 5$.
$(X-2) \circ (X^2+1) = X^2 + 1 - 2 = X^2 - 1$.
Remarque : La composition de polynômes justifie l'écriture $P = P(X) = P \circ X = P$.

Proposition : Formule du binôme de Newton

Soit $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$, on a

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

Proposition : Formule de Bernoulli

Pour $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}^*$, on a

$$P^n - Q^n = (P - Q) \sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

1.2 Degré d'un polynôme

Définition

Soit $P = \sum_{k=0}^{m} a_k X^k$ un polynôme.
Si P est non nul, on appelle **degré du polynôme** P le plus grand entier naturel n tel que $a_n \neq 0$. On note cet entier $\deg(P)$.
Si $P = 0$, on pose $\deg(P) = -\infty$ par convention.
Si $\deg(P) = n \in \mathbb{N}$, le coefficient a_n est appelé coefficient dominant de P.
On dit que P est **unitaire** si et seulement si son coefficient dominant est égal à 1.

Remarque :

- Si P est non nul, on a donc $P = \sum_{k=0}^{\deg(P)} a_k X^k$.

  Attention, lorsque l'on écrit $P = \sum_{k=0}^{n} a_k X^k$, on n'a pas forcément, $\deg(P) = n$, on sait seulement que $\deg(P) \leq n$.
- $P \neq 0 \iff \deg(P) \in \mathbb{N}$.

Exemple : $X^{2020} - 1$ est unitaire de degré 2020.

Proposition : Degré de la somme, du produit, de la composée

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

1. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$;
   De plus, si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$;
2. Si $\lambda \in \mathbb{K}^*$, $\deg(\lambda.P) = \deg(P)$ et si $\lambda = 0$ alors $\deg(\lambda P) = -\infty$;
3. $\deg(PQ) = \deg(P) + \deg(Q)$;
4. Si $\deg(Q) \geq 1$, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Démonstration.

1. Si $P = 0$, $P + Q = Q$ et $\deg(P+Q) = \deg(Q)$, donc on a le résultat souhaité. De même si $Q = 0$.
   Supposons $P \neq 0$ et $Q \neq 0$ et notons $P = \sum_{k=0}^{p} a_k X^k$ avec $p = \deg(P) \in \mathbb{N}$ et $a_p \neq 0$, $Q = \sum_{k=0}^{q} b_k X^k$ avec $q = \deg(Q) \in \mathbb{N}$ et $b_q \neq 0$.
   Par définition, $P + Q = \sum_{k=0}^{\max(p,q)} (a_k + b_k) X^k$.
   Ainsi, $\deg(P+Q) \leq \max(p, q)$.
   Si $p \neq q$, par exemple $p > q$, alors $\max(p, q) = p$ et $a_p + b_p = a_p \neq 0$.
   Ainsi $\deg((P+Q) = \max(p, q)$.
2. Soit $\lambda \in \mathbb{K}$, si $\lambda = 0$ alors $\lambda P = 0$ donc $\deg(\lambda P) = -\infty$.
   Supposons $\lambda \in \mathbb{K}^*$.
   Si $P = 0$ alors $\lambda P = 0$ donc $\deg(P) = \deg(\lambda P)$.
   Supposons $P \neq 0$ et notons $P = \sum_{k=0}^{p} a_k X^k$ avec $p = \deg(P)$ donc $a_p \neq 0$.
   Par définition $\lambda P = \sum_{k=0}^{p} (\lambda a_k) X^k$ donc $\deg(\lambda P) \leq p$.
   De plus, $\lambda a_p \neq 0$ donc $\deg(\lambda P) = p = \deg(P)$.
3. Si $P = 0$ ou $Q = 0$ alors $PQ = 0$ et on a le résultat.
   Supposons $P \neq 0$ et $Q \neq 0$ et notons $P = \sum_{k=0}^{p} a_k X^k$ avec $p = \deg(P)$ et $a_p \neq 0$, $Q = \sum_{k=0}^{q} b_k X^k$ avec $q = \deg(Q)$ et $b_q \neq 0$.
   Par définition $PQ = \sum_{k=0}^{p+q} c_k X^k$.
   On a :$c_{p+q} = \sum_{k=0}^{p+q} a_l b_{p+q-l} = \sum_{l=0}^{p-1} a_l b_{p+q-l} + a_p b_q + \sum_{l=p+1}^{p+q} a_l b_{p+q-l}$ Or, : si $l \in [\![0, p-1]\!]$, $p + q - l \geq p + q - (p-1) \geq q + 1$
   donc $b_{p+q-l} = 0$;
   si $l \in [\![p+1, p+q]\!]$, $a_l = 0$.
   Ainsi, on obtient : $c_{p+q} = a_p b_q$ donc $c_{p+q} \neq 0$.
   Ainsi, $\deg(PQ) = p + q = \deg(P) + \deg(Q)$.
4. Supposons $\deg(Q) \geq 1$.
   Si $P = 0$ alors, $P \circ Q = 0$ et la propriété est vraie.

Supposons désormais $P \neq 0$ et notons $P = \sum_{k=0}^{p} a_k X^k$ avec $p = \deg(P) \in \mathbb{N}$ et $a_p \neq 0$.

On a par définition

$$P \circ Q = \sum_{k=0}^{p} a_k Q^k$$

Montrons que pour tout $k \in \mathbb{N}$, $\deg(Q^k) = k\deg(Q)$.

Soit $k \in \mathbb{N}$, on a : $\deg(Q^{k+1}) = \deg(Q^k \times Q) = \deg(Q^k) + \deg(Q)$.

Ainsi, la suite $\left(\deg(Q^k)\right)_{k\in\mathbb{N}}$ est une suite arithmétique de raison $\deg(Q)$ et de premier terme $\deg(Q^0) = \deg(1) = 0$.

Ainsi : $\forall k \in \mathbb{N},\ \deg(Q^k) = k\deg(Q)$.

De plus : $P \circ Q = a_n X^n + \sum_{k=0}^{n-1} a_k Q^k$. Or, $\deg(a_n Q^n) = \deg(Q^n) = n\deg(Q)$ et $\deg\left(\sum_{k=0}^{n-1} a_k Q^k\right) \leq \max\left(\deg(a_k Q^k, k \in [\![0, n-1]\!]\right)$.

$$\begin{aligned} &\leq \max\left(\deg(Q^k, k \in [\![0, n-1]\!]\right) \\ &\leq \max\left(\deg(k\deg(Q), k \in [\![0, n-1]\!]\right) \\ &\leq (n-1)\deg(Q) \end{aligned}$$

Ainsi, $a_n Q^n$ et $\sum_{k=0}^{n-1} a_k Q^k$ sont de degrés distincts.

Ainsi : $\deg(P \circ Q) = \max\left(\deg\left(a_n Q^n\right), \deg\left(\sum_{k=0}^{n-1} a_k Q^k\right)\right) = \max\left(n\deg(Q), (n-1)\deg(Q)\right) = n\deg(Q)$.

□

Remarque : Si P et Q sont non nuls, on a prouvé que le coefficient dominant de PQ est le produit des coefficients dominants de P et de Q.

Exemple : Soit $n \in \mathbb{N}^*$, déterminer le degré et le coefficient dominant de $P_n = (X+1)^n - (X-1)^n$.

On a directement $\deg(P_n) \leq \max(\deg((X+1)^n), \deg((X-1)^n)) \leq n$.

Par le binôme de Newton, on a :

$$(X+1)^n = \sum_{k=0}^{n} \binom{n}{k} X^k \quad \text{et} \quad (X+1)^n = \sum_{k=0}^{n} \binom{n}{k} X^k (-1)^{n-k}.$$

Ainsi,

- le coefficient de X^n de $(X+1)^n$ vaut $\binom{n}{n} = 1$.

  le coefficient de X^n de $(X-1)^n$ vaut $\binom{n}{n} = 1$.

  Ainsi, le coefficient de X^n dans P_n vaut 0 donc $\deg(P) \leq n-1$.

- De plus, le coefficient de X^{n-1} de P_n vaut $\binom{n}{n-1} - \binom{n}{n-1}(-1) = n + n = 2n$.

  Or, $2n \neq 0$ donc $\deg(P_n) = n-1$ et le coefficient coefficient dominant de P_n vaut $2n$.

Exemple :

Soit pour tout entier naturel $n \in \mathbb{N}$, $P_n = (X^2+1)^{2n} - (X^2-1)^{2n}$. On a $\deg(P_n) \leq 4n$.

D'après la binôme de newton, on a :

$$P_n = \sum_{k=0}^{2n} \binom{2n}{k} X^{2k} - \sum_{k=0}^{2n} \binom{2n}{k} (-1)^{2n-k} X^{2k}.$$

- le coefficient de X^{4n} de P_n vaut $\binom{2n}{2n} - \binom{2n}{2n}(-1)^{2n-2n} = 0$. Donc $\deg(P_n) \leq 4n-1$.
- le coefficient en X^{4n-1} de P_n vaut 0. En effet, il n'y a que des termes à la puissance paires dans P_n donc $\deg(P_n) \leq 4n-2$
- le coefficient en X^{2n-2} de P_n vaut $\binom{2n}{2n-1} - \binom{2n}{2n-1}(-1)^{2n-(2n-1)} = 2n + 2n = 4n$. Or, $4n \neq 0$

Ainsi P est de degré $4n-2$ et son coefficient dominant vaut $4n$.

Exemple :

On souhaite résoudre l'équation : $P(X^2) = (X^2+1)P$. Considérons P un polynôme non nul. Si P est solution alors en prenant le degré dans cette identité, on obtient $2\deg(P) = 2 + \deg(P)$, donc $\deg(P) = 2$.

Soit P de degré 2, il existe $(a, b, c) \in \mathbb{K}^* \times \mathbb{K}^2$ tel que $P(X) = aX^2 + bX + c$.

$$\begin{aligned} P \text{ est solution} &\iff aX^4 + bX^2 + c = aX^4 + bX^3 + (a+c)X^2 + bX + c \\ &\iff \begin{cases} a = a \\ b = 0 \\ a + c = b \end{cases}, \end{aligned}$$

Ainsi l'ensemble des polynômes satisfaisant cette identité est :

$$\{aX^2 - a | a \in \mathbb{K}\}.$$

Proposition

$$\forall P, Q \in \mathbb{K}[X],\ PQ = 0 \Longleftrightarrow P = 0 \text{ ou } Q = 0$$

Démonstration. Si $P = 0$ ou $Q = 0$ alors $PQ = 0$.
On prouve la réciproque par contraposée.
Supposons que $P \neq 0$ et $Q \neq 0$, alors $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$. Ainsi $PQ \neq 0$. Par contraposée, on a le résultat. □

Proposition : Éléments inversibles

Soit $P \in \mathbb{K}[X]$, on a :

$$(\exists Q \in \mathbb{K}[X], P \times Q = 1\quad) \iff \quad P \in \mathbb{K}^*.$$

Démonstration.

- Soit $P \in \mathbb{K}[X]$. Si $P = p \in \mathbb{K}^*$. Posons $Q = \frac{1}{p}$ convient. On a $PQ = 1$.
- Réciproquement, supposons qu'il existe $Q \in \mathbb{K}[X]$ tel que $P \times Q = 1$. Alors, $P \neq 0$ et $Q \neq 0$. De plus, en prenant le degré dans cette équation, on obtient : $\deg(P) + \deg(Q) = 0$. Comme $\deg(P)$ et $\deg(Q)$ sont des entiers naturels, on en déduit que $\deg(P) = \deg(Q) = 0$. Ainsi, on a $P \in \mathbb{K}^*$.

□

Définition

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

$$\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$$

Remarque : Pour tout $n \in \mathbb{N}$, $0 \in \mathbb{K}_n[X]$ car $-\infty \leq n$.

Proposition

Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est stable par combinaison linéaire :

$$\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}_n[X], \quad \lambda P + \mu Q \in \mathbb{K}_n[X].$$

Démonstration. Soit $\lambda, \mu \in K$ et $P, Q \in \mathbb{K}_n[X]$. Alors on a :

$$\deg(\lambda P + \mu Q) \leq \max(\deg(\lambda P), \deg(\mu Q)) \leq \max(\deg(P), \deg(Q)) \leq n.$$

Ainsi on a bien $\lambda P + \mu Q \in \mathbb{K}_n[X]$. □

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

- Si $n = 0$: Soit $P, Q \in \mathbb{K}_0[X]$, on a $\deg(P) \leq 0$ et $\deg(Q) \leq 0$ d'où $\deg(PQ) = \deg(P) + \deg(Q) \leq 0$ donc $PQ \in \mathbb{K}_0[X]$.
- Pour la réciproque, on raisonne par contraposée.
  Supposons que $n \in \mathbb{N}^*$, on a $X^n \in \mathbb{K}_n[X]$ mais $X^n \times X^n = X^{2n}$ avec $2n > n$ car $n \geq 1$ donc $\mathbb{K}_n[X]$ n'est pas stable par produit.

1.3 Fonctions polynomiales

Définition

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

$$\widetilde{P} : \begin{cases} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \sum_{k=0}^{n} a_k x^k. \end{cases}$$

est appelée fonction polynomiale associée au polynôme P.

Proposition

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

$$\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q} \quad \text{ et } \widetilde{PQ} = \widetilde{P}\widetilde{Q}$$

Définition

Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. On appelle évaluation de P en a le nombre $\widetilde{P}(a)$. Par abus de notation, on le notera $P(a)$, et on parlera de la valeur de P en a.

2 Divisibilité et division euclidienne dans $\mathbb{K}[X]$

2.1 Divisibilité dans $\mathbb{K}[X]$

Définition

Soit $A, B \in \mathbb{K}[X]$. On dit que B **divise** A dans $\mathbb{K}[X]$ ou que A est **un multiple de** B dans $\mathbb{K}[X]$ et on note $B|A$ s'il existe $Q \in \mathbb{K}[X]$ tel que : $A = BQ$.

Remarque : Si $B \mid A$ avec $A \neq 0$ alors, $\deg(B) \leq \deg(A)$. En effet, si $B \mid A$, il existe $C \in \mathbb{K}[X]$ tel que $A = BC$ Or, $A \neq 0$ donc $C \neq 0$ d'où, $\deg(C) \in \mathbb{N}$. On a alors $\deg(A) = \deg(B) + \deg(C) \geq \deg(B)$.

Exemple :

- X^p divise X^n si et seulement si $p \leq n$.
- Tout polynôme divise 0. Un polynôme constant non nul divise tout polynôme.
- $X - 1$ divise $X^n - 1$. En effet, $X^n - 1 = (X-1)\sum_{k=0}^{n-1} X^k$.
  De même, $X + 1$ divise $X^{2n+1} + 1$. En effet, $X^{2n+1} + 1 = X^{2n+1} - (-1)^{2n+1}$.
- Dans $\mathbb{C}[X]$ (mais pas dans $\mathbb{R}[X]$), $X - i$ divise $X^2 + 1$.

Exemple :
Soit $n \in \mathbb{N}^*$, d'après le binôme de Newton, on a :

$$(X+1)^n - nX - 1 = \sum_{k=0}^{n} \binom{n}{k} X^k - nX - 1 = \sum_{k=2}^{n} \binom{n}{k} X^k = X^2 \sum_{k=2}^{n} \binom{n}{k} X^{k-2} = X^2 \sum_{k=0}^{n-2} \binom{n}{k} X^k$$

avec $\sum_{k=0}^{n-2} \binom{n}{k} X^k \in \mathbb{K}[X]$.
Ainsi, on a bien : $X^2 | (X+1)^n - nX - 1$.
Si $n = 0$, $(X+1)^n - nX - 1 = 0$ donc X^2 divise $(X+1)^n - nX - 1$.

Proposition : Caractérisation des polynômes associés

Soit $A, B \in \mathbb{K}[X]$. Alors :

$$A|B \text{ et } B|A \iff \exists \lambda \in \mathbb{K}^*,\ A = \lambda B$$

Dans ce cas, A et B sont dits **associés**.

Démonstration. • (ii) implique (i) immédiat.

- Si $A|B$ et $B|A$, on peut trouver deux polynômes C, D tels que $B = AC$ et $A = BD$.
  - Si $A = 0$ alors comme $B = AD$, $B = 0$ et donc toute valeur de $\lambda \in \mathbb{K}^*$ convient.
  - Si $A \neq 0$, on a : Ainsi $A = A \times (CD)$ et $A \neq 0$, on obtient $CD = 1$, et donc $C, D \in \mathbb{K}^*$. Ainsi il existe bien $\lambda \in \mathbb{K}^*$ tel que $B = \lambda A$.

□

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

Théorème de la division euclidienne

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

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

On appelle Q **quotient** et R le **reste** dans la **division euclidienne de** A **par** B.

Démonstration. **Existence :** Soit $B \neq 0$. Notons $p \in \mathbb{N}$ le degré de B et $B = \sum_{k=0}^{p} b_k X^k$ avec $b_p \neq 0$.

On raisonne par récurrence sur le degré de A.
Pour tout $n \in \mathbb{N}$, on considère la propriété :

$\mathscr{P}(n)$: « Pour tout polynôme A tel que $\deg(A) < n$, il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$. »

- Pour $n = 0$. Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) < 0$. Alors $A = 0$ et on a le résultat en posant $(Q, R) = (0, 0)$ ($\deg(R) < \deg(B)$ car $B \neq 0$).
- Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}(n)$ est vraie.
  Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) < n + 1$ i.e. $\deg(A) \leq n$.

  - Si $\deg(A) < n$, par hypothèse de récurrence, il existe $(Q, R) \in \mathbb{K}[X]$ tel que $A + BQ + R$ et $\deg(R) < \deg(B)$.
    On suppose désormais que $\deg(A) = n$ et on note $A = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$.
  - Si $\deg(B) > n$ en posant $(Q, R) = (0, A)$, on a $A = BQ + R$ et $\deg(R) = n < \deg(B)$.
  - Supposons donc $\deg(B) = p \leq n$.
    On pose :
    $$T = A - \frac{a_n}{b_p} X^{n-p} B.$$
    On a :
    $$\begin{aligned} \deg(T) &\leq \max(\deg(A), \deg(\frac{a_n}{b_p} X^{n-p} B) \\ &\leq \max(n, \deg(X^{n-p} B)) \\ &\leq \max(n, \deg(X^{n-p}) + \deg(B)) \\ &\leq \max(n, n) \\ &\leq n \end{aligned}$$
    De plus, le coefficient de X^n de T vaut : $a_n - \frac{a_n}{b_p} b_p = 0$.
    Ainsi, $\deg(T) \leq n - 1$. Par hypothèse de récurrence, il existe $(Q_1, R) \in \mathbb{K}[X]^2$ tel que :
    $$T = BQ_1 + R \quad \text{et} \quad \deg(R) < \deg(B)$$
    Ainsi, $A = T + \frac{a_n}{b_p} X^{n-p} B = BQ_1 + \frac{a_n}{b_p} X^{n-p} B + R = B(Q_1 + \frac{a_n}{b_p} X^{n-p}) + R$. En posant $Q = Q_1 + \frac{a_n}{b_p} X^{n-p}$, on obtient $A = BQ + R$ et $\deg(R) < \deg(B)$.

  Donc $\mathscr{P}(n + 1)$ est vraie.
- En conclusion, pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie, et on a l'existence.

Unicité : Soit (Q_1, R_1) et (Q_2, R_2) tels que :

$$A = BQ_1 + R_1 \quad \deg(R_1) < \deg(B)$$
$$A = BQ_2 + R_2 \quad \deg(R_2) < \deg(B)$$

On a alors : $R_2 - R_1 = B(Q_1 - Q_2)$.
Si $Q_1 \neq Q_2$, on a alors :

$$\deg(R_2 - R_1) = \deg((Q_1 - Q_2)B) = \deg(Q_1 - Q_2) + \deg(B) \geq \deg(B)$$

et, d'autre part :

$$\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) < \deg(B)$$

ce qui est contradictoire. Donc $Q_1 = Q_2$ et par suite, $R_1 = R_2$. □

Exemple : Déterminons le quotient et le reste dans la division euclidienne de :

1. $X^3 - 3X^2 + 3X + 1$ par $X - 2$.

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

Ainsi la division euclidienne de $X^3 - 3X^2 + 3X - 1$ par $X - 2$ est $X^3 - 3X^2 + 3X + 1 = (X - 2)(X^2 - X + 1) + 3$.

2. de $X^5 + 4X^4 + 2X^3 + X^2 - X - 1$ par $X^3 - 2x + 3$.

$$\begin{array}{r|l}
X^5 + 4X^4 + 2X^3 + X^2 - X - 1 & X^3 - 2X + 3 \\
\hline
-(X^5 - 2X^3 + 3X^2) \qquad\qquad & X^2 + 4X + 4 \\
4X^4 + 4X^3 - 2X^2 - X - 1 & \\
-(4X^4 - 8X^2 + 12X) \qquad & \\
4X^3 + 6X^2 - 13X - 1 & \\
-(4X^3 - 8X + 12) \quad & \\
6X^2 - 5X - 13 &
\end{array}$$

Ainsi, la division euclidienne de $X^5 + 4X^4 + 2X^3 + X^2 - X - 1$ par $X^3 - 2X + 3$ est :
$X^5 + 4X^4 + 2X^3 + X^2 - X - 1 = (X^3 - 2 + 3)(X^2 + 4x + 4) + 6X^2 - 5X - 13$.

Proposition

Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On a : B divise A si et seulement si le reste de la division euclidienne de A par B est nul.

Démonstration. $\Rightarrow$ Si $B|A$, alors il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. L'unicité dans la division euclidienne prouve que Q et 0 sont respectivement les quotient et reste de la division euclidienne de A par B, puisque $\deg(0) = -\infty$ et $\deg(B) \in \mathbb{N}$ donc $\deg(0) < \deg(B)$.

$\Leftarrow$ Si le reste de la division euclidienne de A par B est nul, on obtient qu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + 0 = BQ$. Donc on a bien $B|A$.

□

3 Dérivation dans $\mathbb{K}[X]$

Définition

Soit $n \in \mathbb{N}$, soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On appelle polynôme dérivé de P et on note P' le polynôme défini par :

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

Remarque : La dérivée de la fonction polynomiale associée à P est égal à la fonction polynomiale de la dérivée P, autrement dit $\tilde{P}' = \widetilde{(P')}$.

Proposition

Soit $P, Q \in \mathbb{K}[X]$ des polynômes. On a :

1. Si $\deg(P) \geq 1$, on a $\deg(P') = \deg(P) - 1$.
2. $P' = 0 \Leftrightarrow P$ est constant.
3. La dérivation est linéaire : $\forall \lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
4. $(P \times Q)' = P' \times Q + P \times Q'$.
5. $(P \circ Q)' = Q' \times (P' \circ Q)$

Démonstration.

1. On note $P = \sum\limits_{k=0}^{p} a_k X^k$ avec $\deg(P) = p > 0$ et donc $a_p \neq 0$.
   Par définition, $P' = \sum\limits_{k=0}^{p-1} (k+1) a_{k+1} X^k$. Ainsi, $\deg(P') \leq p-1$. De plus, $p a_p \neq 0$, donc $\deg(P') = p - 1$.
2. Si P est un polynôme constant, alors $P' = 0$.
   Pour la réciproque, on raisonne par contraposée.
   Supposons P non constant alors, $\deg(P) \geq 1$, alors d'après le point précédent, on a $\deg(P') = \deg(P) - 1 \in \mathbb{N}$ donc $P' \neq 0$.
3. Notons $P = \sum\limits_{k=0}^{n} a_k X^k$ et $Q = \sum\limits_{k=0}^{n} b_k X^k$ $(n \geq \max(\deg(P), \deg(Q))$.
   Soient $\lambda, \mu \in \mathbb{K}$, on a : On a $\lambda P + \mu Q = \sum\limits_{k=0}^{n} (\lambda a_k + \mu b_k) X^k$, donc
   $$(\lambda P + \mu Q)' = \sum_{k=0}^{n-1} (k+1)(\lambda a_{k+1} + \mu b_{k+1}) X^k = \lambda \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k + \mu \sum_{k=0}^{n-1} (k+1) b_{k+1} X^k = \lambda P' + \mu Q'.$$
4. Notons $PQ = \sum\limits_{k=0}^{2n} c_k X^k$, $P'Q + PQ' = \sum\limits_{k=0}^{2n-1} u_k X^k$ et $(PQ)' = \sum\limits_{k=0}^{2n-1} v_k X^k$.
   On a : $P' = \sum\limits_{k=0}^{n-1} (k+1) a_{k+1} X^k$ et $Q' = \sum\limits_{k=0}^{n-1} (k+1) b_{k+1} X^k$.
   De plus :
   $$\forall k \in [\![0, 2n]\!],\ c_k = \sum_{l=0}^{k} a_l b_{k-l}$$
   Soit $k \in [\![0, 2n-1]\!]$, on a :
   $$v_k = (k+1) c_{k+1}$$
   De plus :
   $$\begin{aligned}
   u_k &= \sum_{l=0}^{k} (l+1) a_{l+1} b_{k-l} + \sum_{l=0}^{k} a_l (k+1-l) b_{k+1-l} \\
   &= \sum_{m=1}^{k+1} m a_m b_{k+1-m} + \sum_{l=0}^{k} a_l (k+1-l) b_{k+1-l} \qquad \text{en posant le changement de variable } m = l+1 \\
   &= \left(\sum_{m=1}^{k} m a_m b_{k+1-m} \right) + (k+1) a_{k+1} b_0 + (k+1) a_0 b_{k+1} + \left(\sum_{l=1}^{k} a_l (k+1-l) b_{k+1-l} \right) \\
   &= (k+1) a_{k+1} b_0 + (k+1) a_0 b_{k+1} + \sum_{l=1}^{k} (l a_l b_{k+1-l} + a_l (k+1-l) b_{k+1-l}) \\
   &= (k+1) a_{k+1} b_0 + (k+1) a_0 b_{k+1} + \sum_{l=1}^{k} (l + k + 1 - l) a_l b_{k+1-l} \\
   &= (k+1) \left[a_{k+1} b_0 + a_0 b_{k+1} + \sum_{l=1}^{k} a_l b_{k+1-l} \right] \\
   &= (k+1) \sum_{l=0}^{k+1} a_l b_{k+1-l} \\
   &= (k+1) c_{k+1} \\
   &= v_k
   \end{aligned}$$
   Ainsi, on a $(PQ)' = P'Q + PQ'$.

5. Pour tout $n \in \mathbb{N}^*$, on considère la propriété $\mathscr{P}(n)$: « $(P^n)' = nP'P^{n-1}$ ».
Montrons par récurrence que pour tout $n \in \mathbb{N}^*$, $\mathscr{P}^n$ est vraie.
   - Pour $n = 1$, on a $P' = 1 \times P'P^0$. donc $\mathscr{P}(1)$ est vraie.
   - Soit $n \in \mathbb{N}^*$, supposons que $\mathscr{P}(n)$ est vraie.
   On a $(P^{n+1})' = (P^n \times P)' = (P^n)'P + P^nP'$ (d'après le point précédent)
   Donc $(P^{n+1})' = nP'P^{n-1}P + P^nP' = (n+1)P'P^n$. Ainsi on a $\mathscr{P}(n+1)$ est vraie.
   - En conclusion : $\forall n \in \mathbb{N}^*$, $(P^n)' = nP'P^{n-1}$.

   Soit $P = \sum_{k=0}^{n} a_k X^k$, on a $P \circ Q = \sum_{k=0}^{n} a_k Q^k$. Par linéarité, on en déduit que

$$(P \circ Q)' = \sum_{k=0}^{n} a_k (Q^k)' = \sum_{k=1}^{n} a_k k Q' Q^{k-1} = Q' \sum_{k=1}^{n} k a_k Q^{k-1}$$

   Or, $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ donc $P' \circ Q = \sum_{k=1}^{n} k a_k Q^{k-1}$.
   D'où $(P \circ Q)' = Q' \times P' \circ Q$.

□

Définition

Soit $P \in \mathbb{K}[X]$. On définit par récurrence les polynômes dérivés successifs de P en posant

$$P^{(0)} = P \text{ et } \forall n \in \mathbb{N},\ P^{(n+1)} = (P^{(n)})'$$

Exemple : Soit $a \in \mathbb{K}$ et soit $n \in \mathbb{N}$. Soit $p \in \mathbb{N}$, on a :

$$\left((X-a)^n\right)^{(p)} = \begin{cases} \dfrac{n!}{(n-p)!}(X-a)^{n-p} & \text{si } p \in [\![0,n]\!] \\ 0 & \text{si } p > n \end{cases}$$

Démonstration. Raisonnons par récurrence.

- Pour $p = 0$, on a $((X-a)^n)^{(0)} = (X-a)^n$.
- Soit $p \in [\![0, n-1]\!]$, supposons que $((X-a)^n)^{(p)} = \dfrac{n!}{(n-p)!}(X-a)^{n-p}$.

  Alors, on a :

$$\begin{aligned}(X-a)^n)^{(p+1)} &= \left((X-a)^n)^{(p)}\right)' \\ &= \left(\frac{n!}{(n-p)!}(X-a)^{n-p}\right)' \\ &= \frac{n!}{(n-p)!}\left((X-a)^{n-p}\right)' \\ &\frac{n!}{(n-p)!}(n-p)(X-a)^{n-p-1} \\ &= \frac{n!}{(n-p-1)!}(X-a)^{n-p-1}\end{aligned}$$

- Ainsi, on a :$\forall p \in [\![0,n]\!]$, $((X-a)^n)^{(p)} = \dfrac{n!}{(n-p)!}(X-a)^{n-p}$.
- En particulier, on a : $((X-a)^n)^{(n)} = \dfrac{n!}{0!}(X-a)^0 = n!$.

  Ainsi, on a : $\forall p > n$, $((X-a)^n)^{(p)} = 0$.

□

Proposition

Soit P et Q des éléments de $\mathbb{K}[X]$.

- Pour tout $\lambda, \mu \in \mathbb{K}$, on a : $\forall n \in \ \mathbb{N}$, $\left(\lambda P + \mu Q\right)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$
- Si $\deg(P) = n$, alors $P^{(k)} = 0$ pour tout $k > n$ et $\deg(P^{(k)}) = \deg(P) - k$ pour tout $k \in [\![0,n]\!]$.

Proposition : Formule de Leibniz

Soit $P, Q \in \mathbb{K}[X]$ des polynômes, $n \in \mathbb{N}$. On a :

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

Démonstration. La preuve est identique à celle réalisée dans le chapitre dérivation. □

Proposition : Formule de Taylor

Soit $n \in \mathbb{N}$. Soit $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors :

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

Démonstration. Pour tout $n \in \mathbb{N}$, on considère la propriété $\mathscr{P}(n)$: « $\forall P \in \mathbb{K}_n[X]$, $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$ ».
Montrons par récurrence que pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

- Soit $P \in \mathbb{K}_0[X]$. Alors, $\deg(P) \leq 0$ donc P est constant, donc $P = P(a)$. Ainsi, $\mathscr{P}(0)$ est vraie.
- Soit $n \in \mathbb{N}$, supposons que $\mathscr{P}(n)$ est vraie.
  Soit $P \in \mathbb{K}_{n+1}[X]$. Alors $\deg(P) \leq n+1$ donc $\deg(P') \leq n$, donc par hypothèse de récurrence, $P' = \sum_{k=0}^{n} \frac{(P')^{k}}{k!}(a)(X-a)^k = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!}(X-a)^k$. Soit $Q = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(X-a)^k$. On a

  $$Q' = \sum_{k=1}^{n+1} \frac{P^{(k)}(a)}{k!} k(X-a)^{k-1} = \sum_{k=1}^{n+1} \frac{P^{(k)}(a)}{(k-1)!}(X-a)^{k-1} = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!}(X-a)^k = P'$$

  donc $(Q-P)' = 0$. Ainsi $Q - P$ est constant. En prenant la valeur en a, on obtient $Q - P = Q(a) - P(a) = P(a) - P(a) = 0$, donc $P = Q$ et on a prouvé $\mathscr{P}(n+1)$.
- En conclusion, pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

□

Remarque : Si $P = \sum_{k=0}^{n} a_k X^k$, en prenant $a = 0$ dans la formule de Taylor, on obtient par identification des coefficients : $\forall k \in [\![0, n]\!],\ a_k = \frac{P^{(k)}(0)}{k!}$.

4 Racines d'un polynôme

4.1 Racines

Définition

On dit que $a \in \mathbb{K}$ est une **racine** dans $\mathbb{K}$ d'un polynôme $P \in \mathbb{K}[X]$ si $P(a) = 0$.

Exemple :

- Tout polynôme de degré 1 a une racine : la racine de $aX + b$ (avec $a \neq 0$) est $-\frac{b}{a}$.
- Pour un polynôme de degré 2, l'existence de racines dépend de $\mathbb{K}$: par exemple $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, il a les racines $\pm i$ dans $\mathbb{C}$.

Proposition

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

- Le reste dans la division euclidienne de P par $(X-a)$ est $P(a)$.
- a est racine de P si et seulement si $X - a$ divise P.

Démonstration. Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Ecrivons la division euclidienne de P par $(X-a)$: il existe $(Q,R) \in \mathbb{K}[X]^2$ tel que $P = (X-a)Q + R$ et $\deg(R) < 1$ donc R est constant : $R = R(a)$. En évaluant cette égalité en a, on obtient $P(a) = (a-a)Q(a) + R(a) = R(a)$. Ainsi, $R = R(a) = P(a)$.
En gardant les mêmes notations : $(X-a)|P$ si et seulement si $R = 0$ si et seulement si $P(a) = 0$ si et seulement si a est racine de P. □

Exemple : Considérons le polynôme $P = X^3 - X + 6$. On voit que -2 est racine évidente de P. Par la proposition précédente, P se factorise par $(X+2)$. Pour obtenir sa factorisation, on peut :

- soit écrire $P = (X+2)(aX^2 + bX + c)$ avec $(a,b,c) \in \mathbb{K}^3$ puis développer et identifier les coefficients :
  Soit $(a,b,c) \in \mathbb{K}^3$

$$
\begin{aligned}
& P = (X-2)(aX^2+bX+c) \\
\iff\ & X^3 - X + 6 = aX^3 + X^2(b+2a) + X(c+2b) + 2c \\
\iff\ & \begin{cases} a = 1 \\ b + 2a = 0 \\ c + 2b = -1 \\ 2c = 6 \end{cases} \\
\iff\ & \begin{cases} a = 1 \\ b = -2 \\ c = 3 \end{cases}
\end{aligned}
$$

  Ainsi, $P = (X+2)(X^2 - 2X + 3)$.
- soit faire la division euclidienne de P par $(X+2)$: le quotient correspond à l'autre facteur de la factorisation et le reste doit être nul .

$$
\begin{array}{r|l}
X^3 - X + 6 & X + 2 \\ \hline
-(X^3 + 2X^2) & X^2 - 2X + 3 \\
-2X^2 - X + 6 & \\
-(-2X^2 - 4X) & \\
3X + 6 & \\
0 &
\end{array}
$$

Proposition

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $a_1, \cdots a_n \in \mathbb{K}$ deux à deux distincts.
$a_1, a_2, \cdots, a_n$ sont racines de P si et seulement si $\displaystyle\prod_{i=1}^{n}(X - a_i)|P$.

Démonstration. $\Leftarrow$ Si $\prod_{i=1}^{n}(X-a_i)|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = \prod_{i=1}^{n}(X-a_i)Q(X)$. Soit $k \in [\![1,n]\!]$, en évaluant en a_k, on obtient $P(a_k) = 0$ donc a_k est racine de P.
Donc a_1, ... a_n sont racines de P

$\Rightarrow$ Pour tout $n \in \mathbb{N}^*$, on note $\mathscr{P}(n)$ la propriété : « tout polynôme qui admet n racines distinctes deux à deux, notées $a_1, ..., a_n$ est divisible par $\displaystyle\prod_{i=1}^{n}(X-a_i)$. »

- Pour $n = 1$, on a le résultat avec une proposition précédente.

- Soit $n \in \mathbb{N}^*$, supposons $\mathscr{P}(n)$ vraie.
  Soit $P \in \mathbb{K}[X]$ admettant $n+1$ racines distinctes deux à deux que l'on note $a_1, ..., a_{n+1}$.
  D'après l'hypothèse de récurrence, il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = Q\prod_{i=1}^{n}(X-a_i)$$

  Comme a_{n+1} est racine de P, on a : $Q(a_{n+1})\displaystyle\prod_{i=1}^{n}(a_{n+1}-a_i) = P(a_{n+1}) = 0$. Or, $\displaystyle\prod_{i=1}^{n}(a_{n+1}-a_i)$ est un élément de $\mathbb{K}$ non nul car les a_i sont 2 à 2 non nuls. Donc $Q(a_{n+1}) = 0$. Ainsi, il existe un polynôme $Q_1 \in \mathbb{K}[X]$, tel que $Q = (X - a_{n+1})Q_1$. On obtient ainsi :

$$P = Q_1\prod_{i=1}^{n+1}(X-a_i)$$

Donc $\prod_{i=1}^{n+1}(X-a_i)|P$

- Pour tout $n\in\mathbb{N}$, la propriété est donc vraie.

$\square$

Exemple :
Soit $n\in\mathbb{N}^*$. Posons $P_n=(X-2)^{2n}+(X-1)^n-1$. On commence par remarquer que $X^2-3X+2=(X-2)(X-1)$. Ainsi, $X^2-3X+2|(X-2)^{2n}+(X-1)^n-1$ si et seulement si 1 et 2 sont racines de P_n si et seulement si $P_n(2)=P_n(1)=0$.
Or, $P_n(2)=0$ et $P_n(1)=(-1)^{2n}-1=0$. Ainsi, $X^2-3X+2|(X-2)^{2n}+(X-1)^n-1$.

Corollaire

Un polynôme non nul de degré $n\in\mathbb{N}$ a au plus n racines deux à deux distinctes.

Démonstration. Soit P un polynôme non nul admettant pour racines les p éléments de $\mathbb{K}$ deux à deux distincts $a_1,\dots,a_p$. Alors, d'après la proposition précédente, $\prod_{k=1}^{p}(X-a_k)\mid P$. On a donc $p\leq\deg(P)$. $\square$

Corollaire

- Un polynôme de $\mathbb{K}_n[X]$ ayant au moins $n+1$ racines deux à deux distinctes est le polynôme nul.
- Le seul polynôme qui possède une infinité de racines (distinctes) est le polynôme nul.

Corollaire

Soit $P=\sum_{k=0}^{n}a_kX^k$ un polynôme, on a l'équivalence :

$$P=0\ (\text{ c'est à dire : }\forall k\in[\![0,n]\!],\ a_k=0\ )\iff \widetilde{P}=0\ (\text{ c'est à dire : }\forall t\in\mathbb{K},\ \widetilde{P}(t)=0\ ).$$

Démonstration. On sait déja que si $P=0$ alors $\widetilde{P}=0$ par définition de $\widetilde{P}$.
Réciproquement, si $\widetilde{P}=0$ alors, P admet une infinité de racines donc P est le polynôme nul donc tous ses coefficients sont nuls. $\square$

Proposition

$$\begin{array}{ccc}\mathbb{K}[X] & \to & \mathscr{F}(\mathbb{K},\mathbb{K})\\ P & \mapsto & \widetilde{P}\end{array}$$

est injective.

Démonstration. Soient A, $B\in\mathbb{K}[X]$. Supposons que $\widetilde{A}=\widetilde{B}$ d'où $\widetilde{A-B}=0$ donc $A-B=0$.

$\square$

Remarque : Ceci justifie qu'on puisse faire l'identification entre P et sa fonction polynomiale.

4.2 Ordre de multiplicité des racines d'un polynôme

Définition

Soit P un polynôme non nul de $\mathbb{K}[X]$ et $a\in\mathbb{K}$ une racine de P. On appelle ordre de multiplicité de la racine a, le plus grand entier $m\in\mathbb{N}^*$ tel que $(X-a)^m$ divise P, autrement dit, l'entier $m\in\mathbb{N}^*$ tel que :

$$(X-a)^m\mid P\quad\text{et}\quad(X-a)^{m+1}\nmid P$$

On dit alors que a est racine d'ordre m de P.

Remarque :

- Lorsque $m\geq 2$, on parle de racine multiple.

- Les racines d'ordre 1,2,3 de P sont respectivement appelées racines simples, doubles, triples de P.

Définition

Soit P un polynôme de $\mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On dit que a est racine d'ordre au moins m de P si et seulement si $(X-a)^m \mid P$

Proposition

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a l'équivalence entre :

- $(X-a)^m$ divise P (i.e a est racine d'ordre au moins m de P)
- $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$.

Démonstration. $\Leftarrow$ Supposons que $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$. Soit $n \geq \max(\deg(P), m)$, en appliquant la formule de Taylor à P en a, on obtient :

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

avec $\displaystyle\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m} \in \mathbb{K}[X]$ car pour tout $k \in [\![m, n]\!]$, $k-m \in \mathbb{N}$. Ainsi $(X-a)^m$ divise bien P.

$\Rightarrow$ Supposons que $(X-a)^m$ divise bien P. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$. Soit $k \in [\![0, m-1]\!]$, par la formule de Leibniz, on obtient :

$$\begin{aligned} P^{(k)} &= \sum_{l=0}^{k} \binom{k}{l} ((X-a)^m)^{(l)} Q^{(k-l)} \\ &= \sum_{l=0}^{k} \binom{k}{l} \frac{m!}{(m-l)!}(X-a)^{m-l} Q^{(k-l)} \\ &= (X-a)\left(\sum_{l=0}^{k} \binom{k}{l} \frac{m!}{(m-l)!}(X-a)^{m-l-1} Q^{(k-l)} \right) \end{aligned}$$

avec $m-l-1 \geq m-k-1 \geq 0$. Ainsi, en évaluant $P^{(k)}$ en a, on obtient $P^{(k)}(a) = 0$ pour tout $k \in [\![0, m-1]\!]$.

□

Exemple : Posons $P_n = \left(\displaystyle\sum_{k=0}^{n-1} X^k \right)^2 - n^2 X^{n-1}$. Avec la proposition précédente, $(X-1)^2 | P_n$ si et seulement si 1 est racine de P_n d'ordre au moins 2 si et seulement si $P_n(1) = 0$ et $P_n'(1) = 0$.

Or, $P_n(1) = \left(\displaystyle\sum_{k=0}^{n-1} 1 \right)^2 - n^2 = n^2 - n^2 = 0$.

De plus, $P_n' = 2 \times \left(\displaystyle\sum_{k=0}^{n-1} X^k \right) \times \left(\displaystyle\sum_{k=1}^{n-1} kX^{k-1} \right) - n^2(n-1)X^{n-2}$.

Ainsi, $P_n'(1) = 2 \times \left(\displaystyle\sum_{k=0}^{n-1} 1 \right) \times \left(\displaystyle\sum_{k=1}^{n-1} k \right) - n^2(n-1) = 2 \times n \times \left(\displaystyle\sum_{k=1}^{n-1} k \right) - n^2(n-1) = 2 \times n \times \dfrac{n(n-1)}{2} - n^2(n-1) = 0$.

On obtient ainsi, le résultat voulu.

Proposition

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a l'équivalence entre :

1. $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P (i.e a est racine d'ordre m de P) ;
2. $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.
3. il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ et $Q(a) \neq 0$

Démonstration. • (1) $\Rightarrow$ (2) : Par la proposition précédente, on a déjà que $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$. De plus, si $P^{(m)}(a) = 0$,
alors $(X-a)^{m+1}$ diviserait également P, ce qui n'est pas le cas. Donc $P^{(m)}(a) \neq 0$.

- (2) $\Rightarrow$ (3) : D'après la proposition précédente, on a déjà que $(X-a)^m$ divise P, et il existe donc $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$.
  Montrons que $Q(a) \neq 0$. Par l'absurde. Supposons que $Q(a) = 0$ alors a est racine de Q donc $(X-a)$ divise Q. Ainsi, il existe $Q_1 \in \mathbb{K}[X]$ tel que $Q = (X-a)Q_1$ donc $P = (X-a)^{m+1}Q_1$. D'où $(X-a)^{m+1}$ divise P. Avec la proposition précédente, on a alors $P^{(m)}(a) = 0$. D'où une contradiction. Donc $Q(a) \neq 0$.
- (3) $\Rightarrow$ (1) : On a déjà que $(X-a)^m$ divise P. Supposons que $(X-a)^{m+1}$ divise aussi P, alors il existe $S \in \mathbb{K}[X]$ tel que $P = (X-a)^{m+1}S$. D'où l'égalité : $(X-a)^m Q = (X-a)^{m+1}S$ d'où $Q = (X-a)S$ car $(X-a)^m \neq 0$. Mais alors $Q(a) = 0$ ce qui est contradictoire.

$\square$

Exemple : Avec la caractérisation 3.
Le polynôme $P = (X-3)^4(X-2)^5$ admet 3 comme racine de multiplicité 4 et 2 comme racine de multiplicité 5.
Exemple :
Avec la caractérisation 2.
Soit $P = X^5 - 6X^4 + 14X^3 - 16X^2 + 9X - 2$. Montrer que 1 est racine de P et déterminer son ordre de multiplicité.
On a $P(1) = 0$, donc 1 est racine de P.
On calcule $P' = 5X^4 - 24X^3 + 42X^2 - 32X + 9$. On a $P'(1) = 0$, donc 1 est racine au moins double de P.
On calcule $P'' = 20X^3 - 72X^2 + 84X - 32$. On a $P''(1) = 0$, donc 1 est racine au moins triple de P.
On calcule $P^{(3)} = 60X^2 - 144X + 84$. On a $P^{(3)}(1) = 0$, donc 1 est racine de P de multiplicité au moins 4.
On calcule $P^{(4)} = 120X - 144$. On a $P^{(4)}(1) = -24 \neq 0$, donc 1 est racine de P de multiplicité 4.

En déduire une factorisation de P sous forme d'un produit de polynômes de degré 1.
Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-1)^4 Q(X)$. Or, $\deg(Q) = \deg(P) - 4 = 1$. Ainsi, il existe $(\alpha, \beta) \in \mathbb{K}^* \times \mathbb{K}$ tels que $Q = \alpha X + \beta$. En égalisant les coefficients dominants de P et de $(X-1)^4 Q$, on obtient : $\alpha = 1$. En égalisant les termes constants, on obtient : $\beta = -2$. Ainsi, $P = (X-1)^4(X-2)$.

Proposition

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ $a_1, \cdots, a_n \in \mathbb{K}$ deux à deux distincts, $m_1, \cdots m_n \in \mathbb{N}^*$. Alors :

$$\text{Pour tout } i \in [\![1, n]\!],\ a_i \text{ est racine de } P \text{ de multiplicité au moins } m_i \iff \prod_{i=1}^{n}(X-a_i)^{m_i} | P.$$

Démonstration. $\Leftarrow$ Supposons que $(X-a_1)^{m_1} \cdots (X-a_n)^{m_n}$ divise P.
Soit $i \in [\![1, n]\!]$, on a en particulier que $(X-a_i)^{m_i}$ divise P. On en déduit que a_i est racine de P de multiplicité au moins m_i.

$\Rightarrow$ On procède par récurrence.
Pour tout $n \in \mathbb{N}$, on considère la propriété :

$\mathscr{P}(n)$: « tout polynôme $P \in \mathbb{K}[X]$ admettant n racines 2 à 2 distinctes que l'on note $a_1, ..., a_n$ d'ordre respectivement au moins égal à $m_1, ..., m_n$ est divisible par $\prod_{i=1}^{n}(X-a_i)^{m_i}$. »

- Pour $n = 1$, la propriété est vraie par définition.

- Soit $n \in \mathbb{N}^*$, supposons $\mathscr{P}(n)$ vraie.
  Considérons $P \in \mathbb{K}[X]$ admettant $n+1$ racines 2 à 2 distinctes que l'on note $a_1, ..., a_{n+1}$ d'ordre respectivement au moins égal à $m_1, ..., m_{n+1}$.
  En particulier, p admet n racines 2 à 2 distinctes $a_1, ..., a_n$ d'ordre respectivement au moins égal à $m_1, ..., m_n$.
  Ainsi, d'après l'hypothèse de récurrence, il existe $B \in \mathbb{K}[X]$ tel que

$$P = B\prod_{i=1}^{n}(X-a_i)^{m_i}$$

  De plus, $P(a_{n+1}) = 0$ donc $B(a_{n+1})\prod_{i=1}^{n}(a_{n+1}-a_i)^{m_i} = 0$. Ainsi, $B(a_{n+1}) = 0$ car les a_i sont deux à deux distincts.
  Ainsi, a_{n+1} est racine de B.
  Notons r son ordre de multiplicité en tant que racine de B. On sait alors qu'il existe $B_1 \in \mathbb{K}[X]$ tel que :

$$B = (X-a_{n+1})^r B_1 \quad \text{et} \quad B_1(a_{n+1}) \neq 0$$

On a alors :

$$P = (X - a_{n+1})^r \underbrace{B_1 \prod_{i=1}^{n} (X - a_i)^{m_i}}_{=B_2}$$

De plus, $B_2(a_{n+1}) = B_1(a_{n+1}) \times \prod_{i=1}^{n} (a_{n+1} - a_i)^{m_i} \neq 0$. Ainsi, a_{n+1} est une racine de P d'ordre r. Donc $m_{n+1} \leq r$. Par suite, $(X - a_{n+1})^{m_{n+1}} | (X - a_{n+1})^r$ donc $\prod_{i=1}^{n+1} (X - a_i)^{m_i}$ divise $(X - a_{n+1})^r \prod_{i=1}^{n} (X - a_i)^{m_i}$ et donc aussi P. On a ainsi montré la proposition au rang $n+1$.

- On a donc prouvé par récurrence que pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

□

Corollaire

Soit $n \in \mathbb{N}$. Un polynôme (non nul) de degré n a au plus n racines comptées avec leur ordre de multiplicité.

Démonstration. Soit P un polynôme non nul admettant pour racines les p éléments de $\mathbb{K}$ 2 à 2 distincts $a_1, ..a_p$ d'ordre respectif égal à $m_1, ..., m_p \in \mathbb{N}^*$.
Alors, par la proposition précédente, $\prod_{i=1}^{p} (X - a_i)^{m_i} | P$. Donc $\sum_{i=1}^{p} m_i \leq \deg(P)$. □

4.3 Polynômes scindés

Définition

Un polynôme P non nul est dit scindé sur $\mathbb{K}$ s'il est constant ou s'il peut s'écrire comme produit de polynômes de $\mathbb{K}[X]$ de degré 1. Autrement dit, un polynôme non nul est scindé s'il existe $\lambda \in \mathbb{K}^*$ (le coefficient dominant de P), un entier naturel $n \in \mathbb{N}$ et des éléments $a_1, ..., a_n \in \mathbb{K}$ (les racines de P) tels que :

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

Proposition

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \geq 1$. On a équivalence entre :

1. P est scindé dans $\mathbb{K}$;
2. la somme des multiplicités des racines de P est égale à $\deg(P)$.

Si c'est le cas, on a alors :

$$P = \lambda \prod_{k=1}^{n} (X - a_k)^{m_k}$$

où λ est le coefficient dominant de P, les $a_i \in \mathbb{K}$ sont les racines de P (deux à deux distinctes) dans $\mathbb{K}$ et les $m_i \in \mathbb{N}^*$ leur multiplicité respective.

Démonstration.

- (2) ⇒ (1) : Notons $a_1, \cdots, a_p \in \mathbb{K}$ les racines deux à deux distinctes de P dans $\mathbb{K}$, et $m_1, \cdots, m_p \in \mathbb{N}^*$ leur multiplicité. Alors d'après une propriété précédente, $\prod_{k=1}^{p} (X - a_k)^{m_k}$ divise P. Il existe donc $Q \in \mathbb{K}[X]$ tel que :

$$P = \prod_{k=1}^{p} (X - a_k)^{m_k} Q.$$

En prenant les degrés, on obtient $\deg(P) = \sum_{i=1}^{p} m_i + \deg(Q)$, d'où avec l'hypothèse $\deg(Q) = 0$. Ainsi $Q = \lambda \in \mathbb{K}^*$, et P est bien scindé dans $\mathbb{K}$.

- (1) ⇒ (2) : Supposons P scindé sur $\mathbb{K}$ de degré $n \geq 1$, alors on peut écrire $P = \lambda \prod_{k=1}^{n} (X - a_k)$ où $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}^*$ et $a_1, ..., a_n \in \mathbb{K}$. En regroupant entre eux les a_k et quitte à les renuméroter, on peut écrire :

$$P = \lambda \prod_{k=1}^{p} (X - a_k)^{m_k} \qquad (*)$$

avec $a_1,\dots,a_p$ deux à deux distincts et $m_1,\dots,m_p \in \mathbb{N}^*$. Alors avec les caractérisations des racines multiples (la 3ème), on en déduit immédiatement que pour tout $i \in [\![1,p]\!]$, a_i est racine de P de multiplicité m_i . L'égalité $(*)$ entraine alors $\sum_{i=1}^{p} m_i = \deg(P)$.

□

Exemple :

- Soit $P = X^5 + 3X^4 + 3X^3 + X^2 = X^2(X^3 + 3X^2 + 3X + 1) = X^2(X+1)^3$.Ainsi, P est scindé sur $\mathbb{R}$ et $\mathbb{C}$.
- Le polynôme $P = X^2 + 1$ est scindé sur $\mathbb{C}$ car $P = (X-i)(X+i)$. En revanche, si on le considère comme un polynôme de $\mathbb{R}[X]$, il n'est pas scindé, car il n'admet pas de racine réelle. En effet, pour tout $t \in \mathbb{R}$, $t^2 + 1 > 0$. Il n'est donc pas scindé sur $\mathbb{R}$.
- Le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$. On connait n racines distinctes de ce polynôme, les racines n-ièmes de l'unité $e^{\frac{2ik\pi}{n}}$, $k \in [\![0, n-1]\!]$. Puisque le polynôme $X^n - 1$ est de degré n et unitaire, on obtient grâce à la proposition précédente l'égalité :
$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

5 Décomposition en facteurs d'irréductibles

Définition

On dit que $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ si P est non constant et si les seuls diviseurs de P dans $\mathbb{K}[X]$ sont les polynômes constants non nuls (i.e les polynômes associés à 1) et les polynômes associés à P.
Ainsi, un polynôme $P \in \mathbb{K}[X]$ est irréductible ssi :

- P est non constant
- $\forall A \in \mathbb{K}[X],\ A|P \implies \exists \lambda \in \mathbb{K}^*,\ A = \lambda$ ou $A = \lambda P$

Rappel : On dit que P et Q sont associés s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.
Remarque : Les polynômes irréductibles dans $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans $\mathbb{N}$.
Remarque :

- un polynôme $P \in \mathbb{K}[X]$ est irréductible ssi :
  - P est non constant
  - Si $P = QR$ avec $Q, R \in \mathbb{K}[X]$ alors Q ou R est constant (non nul), l'autre étant associé à P.
- un polynôme $P \in \mathbb{K}[X]$ est irréductible ssi :
  - P est non constant
  - $\forall Q, R \in \mathbb{K}[X],\ P = QR \implies \deg(Q) = 0 \quad \text{ou} \quad \deg(R) = 0$.

Proposition

Tout polynôme de degré 1 est irréductible dans $\mathbb{K}[X]$.

Démonstration. Soit $P \in \mathbb{K}[X]$ un polynôme de degré 1.
P est donc non constant.
Considérons $B \in \mathbb{K}[X]$ un diviseur de P. Alors, il existe $C \in \mathbb{K}[X]$ tel que $P = BC$. On a alors B et C non nuls car P est non nul et $\deg(B) + \deg(C) = \deg(P) = 1$. Comme $\deg(B),\ \deg(C) \in \mathbb{N}$ l'un des deux vaut 0 et l'autre vaut 1. C'est à dire que l'un des polynômes B et C est constant non nul et l'autre est donc associé à P. Ainsi les seuls diviseurs de P sont les polynômes constants et les polynômes associés à P donc P est irréductible. □

5.1 Factorisation dans $\mathbb{C}[X]$

Théorème Théorème de d'Alembert-Gauss

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

Démonstration. Admis □

Proposition

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

Démonstration. On a déjà que les polynômes de degré 1 sont irréductibles (propriété précédente).
Réciproquement, soit P un polynôme irréductible. Alors, P est non constant. Par le Théorème de d'Alembert Gauss, P admet une racine dans $\mathbb{C}$ que l'on note a. Ainsi, $(X-a)$ divise P. Comme de plus P est irréductible, on en déduit que P et $(X-a)$ sont associés donc P est de degré 1. □

Proposition

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

Démonstration. Pour tout $n \in \mathbb{N}$, on note $\mathscr{P}(n)$: « tout polynôme de $\mathbb{C}[X]$ de degré n est scindé ».
Montrons par récurrence que pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

- Pour $n=0$: $P \in \mathbb{K}^*$ est bien scindé, donc $\mathscr{P}(0)$ est vraie.
- Soit $n \in \mathbb{N}$ et supposons $\mathscr{P}(n)$ vraie.
  Soit P de degré $n+1$. D'après le Théorème de d'Alembert Gauss, P admet au moins une racine $a \in \mathbb{C}$. Alors $(X-a)$ divise P et il existe $Q \in \mathbb{K}[X]$ tel que $P=(X-a)Q$. De plus, Q est non nul et $\deg(Q)=n$. Ainsi, par hypothèse de récurrence, Q est scindé : il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$ et $a_1,\dots a_n \in \mathbb{K}$ tel que :
  $$Q=\lambda\prod_{k=1}^{n}(X-a_k).$$
  Ainsi $P=\lambda(X-a)\prod_{k=1}^{n}(X-a_k)$ et P est scindé, donc $\mathscr{P}(n+1)$ est vraie.
- Ainsi, pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

□

Proposition

Factorisation dans $\mathbb{C}[X]$
Soit P un polynôme non nul de $\mathbb{C}[X]$, alors P s'écrit de façon unique (à l'ordre près des facteurs) sous la forme :
$$P=\lambda\prod_{k=1}^{n}(X-a_k)^{m_k}$$
où $n \in \mathbb{N}$, λ est le coefficient dominant de P, $a_1,\cdots,a_n$ sont les racines deux à deux distinctes de P de multiplicité $m_1,\cdots,m_n \in \mathbb{N}^*$.

5.2 Factorisation dans $\mathbb{R}[X]$

Remarque :

- Dans $\mathbb{R}[X]$, tout polynôme n'est pas nécessairement scindé. Un polynôme du second degré à discriminant strictement négatif, par exemple, n'admet pas de racines dans $\mathbb{R}$.
- On ne peut donc pas factoriser un polynôme de $\mathbb{R}[X]$ sous la même forme que plus haut.

Proposition

Soit $P \in \mathbb{R}[X]$. Si $a \in \mathbb{C}\backslash\mathbb{R}$ est racine de P, alors $\overline{a}$ est aussi racine de P, de même multiplicité que a.

Démonstration. Notons $P=\sum_{k=0}^{n}a_kX^k$, avec $n=\deg(P)$ et $a_0,\dots,a_n \in \mathbb{R}$.
Supposons que a est racine de P.
On a
$$P(\overline{a})=\sum_{k=0}^{n}a_k(\overline{a})^k=\sum_{k=0}^{n}a_k\overline{a^k}=\sum_{k=0}^{n}\overline{a_ka^k}=\overline{P(a)}=0$$
donc $\overline{a}$ est racine de P.
Notons m la multiplicité de a comme racine de P.
Soit $k \in [\![0,m-1]\!]$, $P^{(k)}(a)=0$ et $P^{(k)}$ est à coefficients réels, donc le raisonnement ci-dessus montre que $P^{(k)}(\overline{a})=0$.
Supposons que $P^{(m)}(\overline{a})=0$. Comme $P^{(m)}$ est à coefficients réels, on aurait alors $P^{(m)}(\overline{\overline{a}})=0$ soit $P^{(m)}(a)=0$... absurde !
Ainsi $P^{(m)}(\overline{a})\neq 0$ et $\overline{a}$ est racine de P de multiplicité m. □

Proposition

Les polynômes irréductibles de $\mathbb{R}[X]$ sont

- les polynômes de degré 1 ;
- les polynômes de degré 2 dont le discriminant est strictement négatif.

Démonstration.

- On a déjà vu que les polynômes de degré 1 sont irréductibles.
  Soit P un polynôme de degré 2 de discriminant strictement négatif. Soit $A \in \mathbb{R}[X]$ un diviseur de P. Alors, il existe $B \in \mathbb{R}[X]$ tel que $P = AB$. De plus, on sait que $A \neq 0$, $B \neq 0$ et $\deg(A) + \deg(B) = 2$.
  Si $\deg(A) = 1$ alors, A et donc P ont une racine réelle. Absurde.
  Donc $\deg(A) = 0$ ou $\deg(A) = 2$. Ainsi, $\deg(A) = 0$ ou $\deg(B) = 0$. Ainsi, A ou B est constant non nul donc A est constant ou associé à P.
  Ainsi, tout diviseur de P est constant ou associé à P.
- Réciproquement, soit $P \in \mathbb{R}[X]$ un polynôme irréductible. Alors P est non constant. Donc d'après le théorème de d'Alembert-Gauss, il admet une racine a dans $\mathbb{C}$.
  - Si $a \in \mathbb{R}$, $X - a$ divise P dans $\mathbb{R}[X]$ donc P est associé à $X - a$ puisque P est irréductible donc $\deg(P) = 1$.
  - Si $a \in \mathbb{C}\backslash\mathbb{R}$, et alors $\overline{a}$ est racine de P par la proposition précédente. Ainsi $R = (X-a)(X-\overline{a}) = X^2 - 2\text{Re}(a)X + |a|^2$ divise P dans $\mathbb{C}[X]$. Ainsi, il existe $Q \in \mathbb{C}[X]$ tel que $P = RQ$. On a alors : $\overline{P} = \overline{RQ}$. Or, $P, R \in \mathbb{R}[X]$ donc $P = R\overline{Q}$.
    Par unicité de la division euclidienne dans $\mathbb{C}[X]$, on a $Q = \overline{Q}$ donc $Q \in \mathbb{R}[X]$.
    Ainsi, R divise P dans $\mathbb{R}[X]$ donc P est associé à R (car P est irréductible).
    De plus, le discriminant de R vaut $4(\text{Re}(a)^2 - |a|^2) < 0$ car $a \in \mathbb{C} \setminus \mathbb{R}$. Ainsi, P est un polynôme de degré 2 de discriminant strictement négatif.

□

Proposition

Factorisation dans $\mathbb{R}[X]$
Soit P un polynôme non nul de $\mathbb{R}[X]$, alors P s'écrit de manière unique (à l'ordre près) sous la forme

$$P = \lambda \prod_{i=1}^{p} (X - a_i)^{m_i} \prod_{j=1}^{q} (X^2 + b_j X + c_j)^{n_j}$$

où $p, q \in \mathbb{N}$, $\lambda \in \mathbb{R}$ est le coefficient dominant de P, $a_1, \dots, a_p$ sont les racines réelles deux à deux distinctes de P de multiplicités respectives $m_1, \dots, m_p \in \mathbb{N}^*$, les couples de réels $(b_1, c_1), \dots, (b_q, c_q)$ sont deux à deux distincts et tels que pour tout $k \in [\![1, q]\!]$, $b_k^2 - 4c_k < 0$ et $n_1, \dots, n_q \in \mathbb{N}^*$.

Méthode :

Pour obtenir en pratique une factorisation d'un polynôme P dans $\mathbb{R}[X]$, il suffit de faire la factorisation de P dans $\mathbb{C}[X]$ puis de regrouper les termes complexes non réels qui sont conjugués.

Exemple :
Factorisons le polynôme $X^n - 1$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ ($n \geq 1$). On a déjà obtenu la factorisation dans $\mathbb{C}[X]$:

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

Pour obtenir la factorisation dans $\mathbb{R}[X]$, on doit distinguer les cas où n est pair et impair.
Soit $n \in \mathbb{N}^*$

- Si n est pair, il existe $p \in \mathbb{N}^*$ tel que $n = 2p$. P admet deux racines réelles. On a en regroupant les termes complexes conjugués :

$$\begin{aligned}
X^{2p}-1 &= (X-1)\prod_{k=1}^{p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\left(X-e^{\frac{2ip\pi}{n}}\right)\prod_{k=p+1}^{2p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\\
&= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{k=p+1}^{2p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\\
&= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{l=1}^{p-1}\left(X-e^{\frac{(2in\pi-2il\pi)}{n}}\right) \quad \text{en posant } k=n-l=2p-l\\
&= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{l=1}^{p-1}\left(X-e^{2i\pi}e^{\frac{-2il\pi}{n}}\right)\\
&= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X-e^{\frac{2ik\pi}{n}}\right)\left(X-e^{\frac{-2ik\pi}{n}}\right)\\
&= (X-1)(X+1)\prod_{k=1}^{p-1}\left(X^2-2\cos(\frac{2k\pi}{n})X+1\right).
\end{aligned}$$

- Si n est impair, il existe $p\in\mathbb{N}$ tel que $n=2p+1$. P admet une seule racine réelle. On obtient de même :

$$\begin{aligned}
X^{2p+1}-1 &= (X-1)\prod_{k=1}^{p}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{k=p+1}^{2p}\left(X-e^{\frac{2ik\pi}{n}}\right)\\
&= (X-1)\prod_{k=1}^{p}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{l=1}^{p}\left(X-e^{\frac{(2in\pi-2il\pi)}{n}}\right) \text{ en posant } k=n-l=2p+1-l\\
&= (X-1)\prod_{k=1}^{p}\left(X-e^{\frac{2ik\pi}{n}}\right)\prod_{l=1}^{p}\left(X-e^{2i\pi}e^{\frac{-2il\pi}{n}}\right)\\
&= (X-1)\prod_{k=1}^{p}\left(X-e^{\frac{2ik\pi}{n}}\right)\left(X-e^{-\frac{2ik\pi}{n}}\right)\\
&= (X-1)\prod_{k=1}^{p}\left(X^2-2\cos(\frac{2k\pi}{n})X+1\right).
\end{aligned}$$

5.3 Relations entre coefficients et racines

Rappelons le résultat suivant.

Proposition Relations coefficients racines

Soit $P(X)=aX^2+bX+c\in\mathbb{K}[X]$ avec $a\neq 0$. Soit $\alpha_1,\ \alpha_2\in\mathbb{K}$. Alors :

$$\alpha_1,\alpha_2 \text{ sont les racines de } P \quad\Leftrightarrow\quad \begin{cases}\alpha_1+\alpha_2=-\frac{b}{a}\\ \alpha_1\alpha_2=\frac{c}{a}\end{cases}$$

Démonstration. $\Rightarrow$ Si α_1,α_2 sont les racines de P, alors P est scindé et $P=a(X-\alpha_1)(X-\alpha_2)$.

En développant, on obtient $P=aX^2-a(\alpha_1+\alpha_2)X+a\alpha_1\alpha_2$. En identifiant les coefficients, on obtient $\begin{cases}\alpha_1+\alpha_2=-\frac{b}{a}\\ \alpha_1\alpha_2=\frac{c}{a}\end{cases}$.

$\Leftarrow$ Supposons que $\begin{cases}\alpha_1+\alpha_2=-\frac{b}{a}\\ \alpha_1\alpha_2=\frac{c}{a}\end{cases}$. Alors $a(X-\alpha_1)(X-\alpha_2)=aX^2-a(\alpha_1+\alpha_2)X+a\alpha_1\alpha_2=aX^2+bX+xc=P$ donc α_1,α_2 sont racines de P.

□

Ce résultat se généralise aux polynômes de degré n de la manière suivante.

Proposition : Relations coefficients/racines

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$, scindé dans $\mathbb{K}[X]$ dont les racines sont $x_1, \dots, x_n$ (chacune étant écrite autant de fois que sa multiplicité). Si $P = \sum_{k=0}^{n} a_k X^k$ (avec $a_n \neq 0$), alors

$$\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n} \qquad \text{et} \qquad \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}.$$

Démonstration. Comme P est scindé, et les x_i sont ses racines, P s'écrit sous la forme $a_n \prod_{i=1}^{n}(X - x_i)$. En évaluant en 0, on obtient : $a_n(-1)^n \prod_{i=1}^{n} x_i$ ce qui correspond au terme constant donc $a_0 = a_n(-1)^n \prod_{i=1}^{n} x_i$ ce qui nous donne $\prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}$.
En développant l'expression de P, on obtient que le coefficient de X^{n-1} de P vaut $-a_n \sum_{i=1}^{n} x_i$ donc $a_{n-1} = -a_n \sum_{i=1}^{n} x_i$,
ce qui donne $\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}$. □

Exemple : Soit $P = X^n - 1$. Les racines de P dans $\mathbb{C}$ sont les racines n-ièmes de l'unité. Il y en a $n = \deg(X^n - 1)$, donc P est scindé. D'après les relations coefficients racines, $\sum_{\omega \in \mathbb{U}_n} \omega = -\frac{0}{1} = 0$ et $\prod_{\omega \in \mathbb{U}_n} \omega = \frac{(-1)^{n+1}}{1} = (-1)^{n+1}$.