Chapitre 9

Polynômes

Dans ce chapitre, après avoir vu la définition et les premières propriétés des polynômes, nous allons nous intéresser à l'arithmétique des polynômes, ainsi, il serait bon d'avoir travaillé la partie arithmétique dans $\mathbb{Z}$, ce qui permettra, par analogie, une meilleure appropriation des résultats sur les polynômes.

Table des matières

1 Polynôme et premières propriétés

1.1 Définition d'un polynôme, degré et opérations

Définition d'un polynôme

Un **polynôme** à coefficients dans $\mathbb{K}$ est un objet de la forme $\sum\limits_{k=0}^{n} a_k X^k = a_0 X^0 + a_1 X^1 + \ldots + a_n X^n$ pour $n \in \mathbb{N}$ et $a_k \in \mathbb{K}$. On appelle X l'**indéterminée**. Par convention $X^0 = 1$. On note $\mathbb{K}[X]$ l'ensemble des polynômes.

Remarques 1.

- L'indéterminée X n'est pas *vraiment* définie ici. C'est un objet formel (ce n'est pas un nombre ni une variable ni une fonction) utilisé pour définir les polynômes. De même, le nombre complexe i, qui n'est pas *vraiment* défini, est utilisé pour définir les complexes.
- Le n dépend du polynôme choisi. Par exemple, pour $2+3X$: $n=1$, pour $1-X^4$: $n=4$. Malheureusement, comme $2+3X = 2+3X+0X^2+0X^3$, ce n n'est pas unique, on peut aussi prendre $n'=3$. On peut toujours prendre $n' > n$ et si besoin poser $a_k = 0$ pour $k > n$.
- Deux polynômes sont égaux si seulement si leurs coefficients sont égaux :

$$\forall P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X] \quad \forall Q = \sum_{k=0}^{n} b_k X^k \in \mathbb{K}[X] \qquad (P = Q \quad \Longleftrightarrow \quad \forall k \in [\![0\,;n]\!] \quad a_k = b_k)$$

Définition du degré d'un polynôme, du coefficient dominant, d'un polynôme unitaire

- Si tous les coefficients d'un polynôme sont nuls, on dit que c'est le **polynôme nul**, noté 0.
- Soient $P = \sum\limits_{k=0}^{n} a_k X^k$ un polynôme non nul et $d = \max\{k \in [\![0\,;n]\!] \mid a_k \neq 0\}$ de sorte que $P = \sum\limits_{k=0}^{d} a_k X^k$. L'entier d est appelé **degré** de P et est noté $d^\circ P = d$. On pose, par convention, $d^\circ 0 = -\infty$.
- On appelle **coefficient dominant** de P le coefficient a_d. On dit que P est **unitaire** si $a_d = 1$.
- On dit que P est un **polynôme constant** si $d^\circ P \leqslant 0$, dans ce cas $P = a_0$.
- Les polynômes λX^n, avec $\lambda \neq 0$, sont appelés **monômes**.
- On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égale à n.

Exemples 1. $d^\circ 3 =$ $\qquad$ $d^\circ X + 2 =$ $\qquad$ $d^\circ X^n =$ $\qquad$ $d^\circ(aX^2 + bX + c) =$

Attention à ne pas confondre degré n et somme dont le dernier terme est X^n

L'écriture $P = \sum\limits_{k=0}^{n} a_k X^k$ n'implique pas $d^\circ P = n$ seulement que $d^\circ P \leqslant n$. De plus, $a_n \neq 0$ ssi $d^\circ P = n$.

Définition de somme/multiplication par un scalaire/multiplication/composée

Soient $P = \sum\limits_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$, $\tilde{P} = \sum\limits_{k=0}^{p} \tilde{a}_k X^k$, $Q = \sum\limits_{k=0}^{q} b_k X^k \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On définit les polynômes suivants :

- $P + \tilde{P} = \sum\limits_{k=0}^{p} a_k X^k + \sum\limits_{k=0}^{p} \tilde{a}_k X^k = \sum\limits_{k=0}^{p} (a_k + \tilde{a}_k) X^k$ $\qquad$ et $\qquad$ $\lambda P = \lambda \sum\limits_{k=0}^{p} a_k X^k = \sum\limits_{k=0}^{p} (\lambda a_k) X^k$
- $PQ = \sum\limits_{k=0}^{p+q} c_k X^k$ avec pour tout $k \in [\![0\,;p+q]\!]$, $c_k = \sum\limits_{i=0}^{k} a_i b_{k-i}$ autrement dit

$$\sum_{k=0}^{p} a_k X^k \times \sum_{k=0}^{q} b_k X^k = \sum_{k=0}^{p+q} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k$$

- On pose, par convention, $P^0 = 1$ et pour tout $n \in \mathbb{N}^*$, $P^n = P \times P \times \ldots \times P$.
- $P \circ Q = P(Q) = \sum\limits_{k=0}^{p} a_k Q^k$

Exemples 2. Si $P = 2X^2 + 3X$, $Q = X^3 - 2X$ et $R = -2X^2 + 2$, calculer $P + Q$, $P + R$ et PQ et $P \circ Q$.

Remarques 2.
- Pour définir la somme de deux polynômes, il faut le même nombre de termes dans les deux sommes (quitte à rajouter des zéros manquants).
- Ce n'est pas le cas, en revanche pour le produit de deux polynômes. De plus, $c_0 = a_0 b_0$ tandis que $c_{p+q} = a_p b_q$.
- $P(X) = P$

Proposition n° 1 : propriétés des opérations sur les polynômes

Si $(P, Q, R) \in \mathbb{K}[X]^3$ et $(\lambda, \mu) \in \mathbb{K}^2$ alors :

1. $P + Q = Q + P$ (commutativité)
2. $(P + Q) + R = P + (Q + R)$ (associativité)
3. $0 + P = P$ (0 neutre de l'addition)
4. $P + (-1) \times P = 0$ (existence de l'opposé)
5. $(\lambda P) \times Q = \lambda(PQ)$ $\qquad 1 \times P = P$
6. $\lambda(P + Q) = \lambda P + \lambda Q$ $\qquad (\lambda + \mu)P = \lambda P + \mu P$
7. $PQ = QP$ (commutativité)
8. $(PQ)R = P(QR)$ (associativité)
9. $P(Q + R) = PQ + PR$ (distributivité)
10. $(P + Q)^n = \sum\limits_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}$ binôme de Newton
11. $P^n - Q^n = (P - Q) \sum\limits_{k=0}^{n-1} P^k Q^{n-1-k}$

Exemple 3. Grâce à $(1 + X)^{2n}$, démontrer que $\sum\limits_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Exemples 4. Si $P = 2X^2 + 3X$, $Q = X^3 - 2X$ et $R = -2X^2 + 2$, que penser du degré de $P + Q$, $P + R$ et PQ ?

Proposition n° 2 : propriétés sur le degré et intégrité

Soit $(P, Q) \in \mathbb{K}[X]^2$, alors :

1. $d^\circ(P + Q) \leqslant \max(d^\circ P, d^\circ Q)$
2. Si $d^\circ P \neq d^\circ Q$, alors $d^\circ(P + Q) = \max(d^\circ P, d^\circ Q)$
3. $d^\circ PQ = d^\circ P + d^\circ Q$
4. $d^\circ \lambda P = d^\circ P$ si $\lambda \in \mathbb{K}^*$
5. Si Q non constant, $d^\circ(P \circ Q) = d^\circ P \times d^\circ Q$
6. Si $PQ = 0$, alors $P = 0$ ou $Q = 0$ (intégrité)

Attention au degré de la somme

En général, le degré de la somme n'est pas égale à la somme des degrés ni au maximum des degrés.

Démonstration de la proposition n° 2 : Posons $p = d^\circ P$ et $q = d^\circ Q$, de sorte que $P = \sum\limits_{k=0}^{p} a_k X^k$ et $Q = \sum\limits_{k=0}^{q} b_k X^k$ avec $a_p \neq 0$ et $b_q \neq 0$.

1. Il y a trois cas :
   - Si $p > q$, alors $P+Q = \sum\limits_{k=0}^{q} (a_k+b_k)X^k + \sum\limits_{k=q+1}^{p} a_k X^k$ avec $a_p \neq 0$, de sorte que $d^\circ(P+Q) = p = \max(p, q) = \max(d^\circ P, d^\circ Q)$.
   - Si $p < q$, alors idem que précédemment, en changeant les rôles de P et Q.
   - Si $p = q$, alors $P + Q = \sum\limits_{k=0}^{p} (a_k + b_k)X^k$. Donc si $a_k + b_k \neq 0$, alors $d^\circ(P + Q) = p = \max(d^\circ P, d^\circ Q)$. Si $a_k + b_k = 0$, alors $P + Q = \sum\limits_{k=0}^{p-1} (a_k + b_k)X^k$ et donc $d^\circ(P + Q) \leqslant p - 1 < p = \max(d^\circ P, d^\circ Q)$.
2. Par définition, du produit de deux polynômes, $PQ = \sum\limits_{k=0}^{p+q} c_k X^k$ avec $c_{p+q} = a_p b_q \neq 0$, ainsi $d^\circ PQ = p + q = d^\circ P + d^\circ Q$.
3. Utiliser la propriété précédente avec $Q = \lambda$, alors $d^\circ Q = 0$.
4. Par le point 2 : $d^\circ Q^2 = d^\circ Q + d^\circ Q = 2q$. Puis, par une récurrence facile, $d^\circ Q^k = kq$. Ainsi,
$$P(Q) = \sum_{k=0}^{p} a_k Q^k = a_p Q^p + \sum_{k=0}^{p-1} a_k Q^k$$
Or, $d^\circ a_p Q^p = pq$ ($a_p \neq 0$) et $d^\circ \left(\sum\limits_{k=0}^{p-1} a_k Q^k \right) \leqslant (p - 1)q < pq$ ($q \geqslant 1$). Comme les degrés sont différents, par la propriété du degré de la somme : $d^\circ P(Q) = pq = d^\circ P \times d^\circ Q$.
5. Par contraposée, si $P \neq 0$ et $Q \neq 0$. Ainsi, $d^\circ P \geqslant 0$, $d^\circ Q \geqslant 0$. Par conséquent, $d^\circ PQ = d^\circ P + d^\circ Q \geqslant 0$, dès lors, $PQ \neq 0$. ■

1.2 Fonctions polynomiales et racines

Définition d'une fonction polynômiale

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On dit que $\tilde{P}$: $\begin{cases} \mathbb{K} \longrightarrow \mathbb{K} \\ x \longmapsto P(x) = \sum_{k=0}^{n} a_k x^k \end{cases}$ est la **fonction polynomiale** associée à P.

Remarques 3.
- Formellement, le polynôme P et la fonction polynomiale $\tilde{P}$ sont des objets différents. Cependant, les concours autorisent parfois de confondre les deux notions.
- Pour tout $x \in \mathbb{K}$, $\widetilde{P+Q}(x) = \widetilde{P}(x) + \widetilde{Q}(x)$ et $\widetilde{PQ}(x) = \widetilde{P}(x)\widetilde{Q}(x)$, $\widetilde{P \circ Q}(x) = \widetilde{P}\left(\widetilde{Q}(x)\right)$.

Définition d'une racine d'un polynôme

Soit P un polynôme et $x \in \mathbb{K}$, on dit que x est une racine de P si $P(x) = 0$.

Exemple 5. Est-ce que 1 est racine de $P = X^3 + X^2 - X - 1$?

Remarque 4. Si $P = \sum_{k=0}^{n} a_k X^k$ et $x_0 \in \mathbb{K}$, alors $P(x_0)$ se calcule par la méthode de Horner avec moins de calculs que la méthode naïve : $P(x_0) = a_0 + x_0(a_1 + x_0(a_2 + x_0(a_3 + \ldots))))$

1.3 Polynôme dérivé

Définition de la dérivée d'un polynôme

On définit le **polynôme dérivé** de $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, par $P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{j=0}^{n-1} (j+1) a_{j+1} X^j$

Pour $k \in \mathbb{N}$, on définit $P^{(k)}$ comme le polynôme obtenu en dérivant k fois P : $P^{(0)} = P$, $P^{(1)} = P'$, $P^{(2)} = P''$

Proposition n° 3 : propriétés de la dérivée

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

1. Si P est non constant alors $d^\circ P' = d^\circ P - 1$
2. $d^\circ P' \leqslant d^\circ P - 1$ et $d^\circ P^{(k)} \leqslant d^\circ P - k$
3. $(\lambda P + Q)' = \lambda P' + Q'$
4. $(PQ)' = PQ' + P'Q$
5. $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$ (formule de Leibniz)
6. $(X^n)^{(k)} = \dfrac{n!}{(n-k)!} X^{n-k}$ si $k \leqslant n$ et 0 si $k > n$.

Démonstration de la proposition n° 3 :

1.
2. Prenons $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$ (encore une fois, on complète avec des zéros pour que les sommes finissent avec le même indice n). Alors, $(\lambda P + Q) = \sum_{k=0}^{n} (\lambda a_k + b_k) X^k$. Ainsi :
$$(\lambda P + Q)' = \sum_{k=1}^{n} k(\lambda a_k + b_k) X^{k-1} = \lambda \sum_{k=1}^{n} a_k X^{k-1} + \sum_{k=1}^{n} b_k X^{k-1} = \lambda P' + Q'$$
3. Par produit de deux polynômes et par dérivation :
$$\begin{aligned} PQ &= \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k \\ (PQ)' &= \sum_{k=1}^{2n} \left(k \sum_{i=0}^{k} a_i b_{k-i} \right) X^{k-1} \\ (PQ)' &= \sum_{j=0}^{2n} \left((j+1) \sum_{i=0}^{j+1} a_i b_{j+1-i} \right) X^j \end{aligned}$$

De plus,

$$\begin{aligned}
PQ'+P'Q &= \sum_{k=0}^{n} a_k X^k \sum_{k=0}^{n-1}(k+1)b_{k+1}X^k + \sum_{k=0}^{n-1}(k+1)a_{k+1}X^k \sum_{k=0}^{n} b_k X^k \\
&= \sum_{k=0}^{2n-1}\left(\sum_{i=0}^{k} a_i(k-i+1)b_{k-i+1}\right)X^k + \sum_{k=0}^{2n-1}\left(\sum_{i=0}^{k}(i+1)a_{i+1}b_{k-i}\right)X^k \\
&= \sum_{k=0}^{2n-1}\left(\sum_{i=0}^{k} a_i(k-i+1)b_{k-i+1} + \sum_{i=1}^{k+1} i a_i b_{k+1-i}\right)X^k \\
&= \sum_{k=0}^{2n-1}\left(\sum_{i=0}^{k+1} a_i(k-i+1)b_{k-i+1} + i a_i b_{k+1-i}\right)X^k \\
&= \sum_{k=0}^{2n-1}\left((k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}\right)X^k
\end{aligned}$$

Posons l'hypothèse de récurrence $\mathscr{P}(n)$: « $(PQ)^{(n)} = \sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}$ ».

- Pour $n=0$, $(PQ)^0 = PQ$ et $\sum_{k=0}^{0}\binom{0}{k}P^{(k)}Q^{(0-k)} = PQ$. Ainsi, $\mathscr{P}(0)$ est vraie.
- Soit $n \in \mathbb{N}$. Supposons $\mathscr{P}(n)$ vraie. D'après $\mathscr{P}(n)$, $(PQ)^{(n)} = \sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}$. En dérivant une somme puis un produit

$$\begin{aligned}
((PQ)^{(n)})' &= \left(\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}\right)' = \sum_{k=0}^{n}\binom{n}{k}\left(P^{(k)}Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n}\binom{n}{k}\left[\left(P^{(k)}\right)'Q^{(n-k)} + P^{(k)}\left(Q^{(n-k)}\right)'\right] = \sum_{k=0}^{n}\binom{n}{k}\left[P^{(k+1)}Q^{(n-k)} + P^{(k)}Q^{(n+1-k)}\right] \\
&= \sum_{k=0}^{n}\binom{n}{k}P^{(k+1)}Q^{(n-k)} + \sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n+1-k)} \\
&= \sum_{i=1}^{n+1}\binom{n}{i-1}P^{(i)}Q^{(n+1-i)} + \sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n+1-k)} \\
&= \sum_{i=1}^{n}\binom{n}{i-1}P^{(i)}Q^{(n+1-i)} + \binom{n}{n}P^{(n+1)}Q^{(0)} + \sum_{k=1}^{n}\binom{n}{k}P^{(k)}Q^{(n+1-k)} + \binom{n}{0}P^{(0)}Q^{(n+1)} \\
&= P^{(n+1)}Q^{(0)} + P^{(0)}Q^{(n+1)} + \sum_{k=1}^{n}\left[\binom{n}{k-1}+\binom{n}{k}\right]P^{(k)}Q^{(n+1-k)} \\
&= \binom{n+1}{n+1}P^{(n+1)}Q^{(0)} + \binom{n+1}{0}P^{(0)}Q^{(n)} + \sum_{k=1}^{n}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)} \\
(PQ)^{(n+1)} &= \sum_{k=0}^{n+1}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)}
\end{aligned}$$

  Ceci prouve que $\mathscr{P}(n+1)$ est vraie.
- Par récurrence, pour tout $n \in \mathbb{N}$, $\mathscr{P}(n)$ est vraie.

4. Soit $n \in \mathbb{N}$ et $P = X^n$. Posons $\mathscr{P}(k)$: « $P^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!}X^{n-k} & \text{si} \quad k \leqslant n \\ 0 & \text{si} \quad k > n \end{cases}$ »
   - Pour $k=0$, $\dfrac{n!}{(n-0)!}X^{n-0} = X^n = P^{(0)}$ avec $0 \leqslant n$. Ainsi, $\mathscr{P}(0)$ est vraie.
   - Soit $k \in \mathbb{N}^*$. Supposons, $\mathscr{P}(k)$ vérifiée et montrons $\mathscr{P}(k+1)$, distinguons trois cas :
     — Si $k < n$, alors $P^{(k)} = \dfrac{n!}{(n-k)!}X^{n-k}$, ainsi en dérivant :

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

     Comme $k < n$, $k+1 \leqslant n$.
     — Si $k = n$, alors $P^{(k)} = n!$ ainsi $P^{(k+1)} = 0$ avec $k+1 > n$.
     — Si $k > n$, $P^{(k)} = 0$ en dérivant $P^{(k+1)} = 0$ avec $k+1 > n$.

     Dans tous les cas, $P^{(k+1)} = \begin{cases} \dfrac{n!}{(n-(k+1))!}X^{n-(k+1)} & \text{si} \quad k \leqslant n+1 \\ 0 & \text{si} \quad k > n+1 \end{cases}$. Ceci prouve que $\mathscr{P}(k+1)$ est vraie.

- Par récurrence, pour tout $k \in \mathbb{N}^*$, $\mathscr{P}(k)$ est vraie. ■

Théorème n° 1 : formule de Taylor pour les polynômes *(admis provisoirement)*

Soit $P = \sum_{k=0}^{n} c_k X^k \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$, alors $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$

En particulier, pour $a = 0$, pour tout $k \in [\![0\,; n]\!]$, $c_k = P^{(k)}(0)/k!$.

2 Arithmétique des polynômes

2.1 Divisiblité

Définition de la divisibilité

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

Exemples 6. Est-ce que $X^2 + X - 2$ est un multiple de $X + 2$? Est-ce que $X - 1|X^n - 1$? Est-ce que $X + 1|X^3 + 1$?

2.2 Division euclidienne

Théorème n° 2 de la division euclidienne

Soit $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \backslash \{0\})$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $d^\circ R < d^\circ B$. L'écriture $A = BQ + R$ s'appelle la **division euclidienne** de A par B, Q est le **quotient** et R le **reste**.

Démonstration du théorème n° 2 :

- Méthode 1 pour démontrer l'existence. Notons $d = d^\circ B$. Posons l'hypothèse de récurrence, pour $n \in \mathbb{N}$: $\mathscr{P}(n)$:

$$\text{«} d^\circ A < n \quad \Longrightarrow \quad \big(\exists (Q, R) \in \mathbb{K}[X]^2 \quad A = BQ + R \text{ avec } d^\circ R < d^\circ B\big) \text{»}$$

  Remarquons que si $d^\circ A < d = d^\circ B$, alors $A = B \times 0 + R$ avec $R = A$. Ainsi, $\mathscr{P}(d)$ est vraie. Soit un entier $n \geqslant d$, supposons $\mathscr{P}(n)$ et montrons $\mathscr{P}(n+1)$. Supposons $d^\circ A < n+1$, si $d^\circ A < n$, alors on applique directement $\mathscr{P}(n)$ à A. Si $d^\circ A = n$. Dotons α le coefficient dominant de A et β le coefficient dominant de B. Posons $\tilde{A} = A - \frac{\alpha}{\beta} X^{n-d} B$. Alors, $d^\circ \tilde{A} < d^\circ A \leqslant n$. On applique donc $\mathscr{P}(n)$ à $\tilde{A}$: il existe $(\tilde{Q}, \tilde{R}) \in \mathbb{K}[X]^2$ tel que $\tilde{A} = B\tilde{Q} + \tilde{R}$ avec $d^\circ \tilde{R} < d^\circ B$. Ainsi, $A = (\frac{\alpha}{\beta} + \tilde{Q})B + \tilde{R}$. Ainsi, $\mathscr{P}(n+1)$ est vraie. Par récurrence, la propriété est vraie pour tout entier $n \geqslant d'$.
- Méthode 2 pour démontrer l'existence. Considérons $D = \{d^\circ(A - BQ) \mid Q \in \mathbb{K}[X]\} \subset \mathbb{N} \cup \{-\infty\}$. Comme $D \neq \varnothing$ (prendre $Q = 0$, permet d'affirmer que $d^\circ A \in D$). Ainsi, $\min(D)$ existe : il existe $Q \in \mathbb{K}[X]$ tel que $d^\circ(A - BQ) = \min(D)$ [1]. Posons $R = A - BQ$, de sorte que $A = BQ + R$. Raisonnons par l'absurde et supposons que $d = d^\circ R \geqslant d' = d^\circ B$. Notons r_d le coefficient dominant de R et $b_{d'}$ celui de B. Posons

$$\tilde{R} = R + \left(-\frac{r_d}{b_{d'}} X^{d-d'} B\right)$$

  Alors $d^\circ(-\frac{r_d}{b_{d'}} X^{d-d'} B) = d^\circ X^{d-d'} + d^\circ B = d - d' + d' = d$ et le coefficient dominant de $(-\frac{r_d}{b_{d'}} X^{d-d'})B$ est $-r_d$. Ainsi, on a deux polynômes de même degré avec des coefficients dominants opposés donc $d^\circ \tilde{R} < d^\circ R = \min(D)$. Pourtant $\tilde{R} = A - B(Q + \frac{r_d}{b_{d'}} X^{d-d'})$, donc $d^\circ \tilde{R} \in D$ ce qui contredit la minimalité de D. Ceci démontre que $d^\circ R < d^\circ B$, avec $A = BQ + R$.
- Démonstration de l'unicité : supposons que $A = BQ + R = B\tilde{Q} + \tilde{R}$ avec $d^\circ R < d^\circ B$ et $d^\circ \tilde{R} < d^\circ B$. Alors $B(Q - \tilde{Q}) = \tilde{R} - R$, alors

$$d^\circ B + d^\circ(Q - \tilde{Q}) = d^\circ(\tilde{R} - R) \leqslant \max(d^\circ \tilde{R}, d^\circ R) < d^\circ \tilde{B}$$

  Il est donc nécessaire que $d^\circ(Q - \tilde{Q}) < 0$, donc que $Q = \tilde{Q}$. Ainsi, $R = A - BQ = A - B\tilde{Q} = \tilde{R}$. ■

1. Potentiellement, $\min(D) = -\infty$ ce qui est un peu litigieux, on pourrait l'exclure, en notant d'abord que l'existence est acquise si B divise A.

Exemples 7. Effectuer la division euclidienne de X^4+1 par X^2+3X+2 en déduire une primitive de $x \mapsto \dfrac{x^4+1}{x^2+3x+2}$.
Calculer $\displaystyle\int_2^3 \frac{t\,\mathrm{d}t}{t+1}$, $\displaystyle\int_2^3 \frac{t^3}{t+1}\,\mathrm{d}t$ et $\displaystyle\int_2^3 \frac{t^5}{t(t+1)}\,\mathrm{d}t$.

Attention à ne pas confondre la divisibilité et la division euclidienne

La question «B divise A ?» à laquelle on répond par oui ou par non.
La division euclidienne de A par B consiste **à trouver** Q et R tel que $A = BQ + R$ avec $d^\circ R < d^\circ B$.

Proposition n° 4 : équivalence entre divisibilité et reste de la division euclidienne

Soit B un polynôme non nul. $B|A$ ssi le reste de la division euclidienne de A par B est nul.

Démonstration de la proposition n° 4 : Si le reste de la division euclidienne de A par B est nul, alors $A = BQ+0$ donc $A = BQ$ et B divise A. Si B divise A, alors $A = BQ$ pour un certain $Q \in \mathbb{K}[X]$. Dès lors, $A = BQ + R$ avec $R = 0$ et $d^\circ R = -\infty < d^\circ B$. Par unicité de la division euclidienne, $R = 0$ est le reste de la division euclidienne. ■

Comment calculer une division euclidienne ?

Deux méthodes :

1. Poser la division comme à l'école primaire (fonctionne si $d^\circ A$ est petit)
2. Utiliser les racines de B permet de trouver seulement le reste (en remplaçant X par les racines de B quitte à dériver s'il manque des équations).

Exemples 8. Trouver le reste de la division euclidienne de $X^n + X^{n-1} + 1$ par $X^2 - 3X + 2$ puis par $X^2 - 4X + 4$.

2.3 Racines et divisibilité

Proposition n° 5 : caractérisation des racines avec la divisibilité

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le nombre a est racine de P si et seulement si $X - a|P$.

Démonstration de la proposition n° 5 : Supposons que $X - a|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$. Dès lors, $P(a) = (a-a)Q(a) = 0$ donc a est racine de P. Supposons que a soit racine de P. Effectuons la division euclidienne de P par $X-a$: il existe deux polynômes Q et R tel que $P = (X-a)Q+R$ avec $d^\circ R < d^\circ(X-a) = 1$. Ainsi, R est un polynôme constant $R = r_0 \in \mathbb{K}$. Donc $P = (X-a)Q+r_0$. En substituant a à X, il vient $P(a) = (a-a)Q(a)+r_0$, donc $0 = 0+r_0$, bref $r_0 = 0$ et donc $P = (X-a)Q$. Ceci prouve que $X - a|P$. ■

Définition de la multiplicité d'une racine

Soit $P \in \mathbb{K}[X]$ non nul. La **multiplicité** ou **ordre** de $a \in \mathbb{K}$ dans P est le plus grand entier m tel que $(X-a)^m|P$.

Remarques 5.
- Formellement l'ensemble $\left\{k \in \mathbb{N} \mid (X-a)^k \text{ divise } P\right\}$ est un ensemble de $\mathbb{N}$ non vide et majorée donc admet bien un plus grand élément que l'on appelle la multiplicité de a dans P.
- Si $m = 0$, alors a n'est pas racine de P
- Si $m = 1$, alors on dit que a est une racine **simple** de P
- Si $m = 2$, alors on dit que a est une racine **double** de P.

Proposition n° 6 : caractérisation d'une racine de multiplicité m

Soient $P \in \mathbb{K}[X]$ non nul, $m \in \mathbb{N}$ et $a \in \mathbb{K}$. Sont équivalents :

1. a est racine d'ordre m
2. $\exists Q \in \mathbb{K}[X] \mid P = (X-a)^m Q$ et $Q(a) \neq 0$
3. $\forall i \in [\![0\,; m-1]\!]\ P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$

Démonstration de la proposition n° 6 :

$1 \Longrightarrow 2$ Comme a est racine d'ordre m, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$. Supposons que $Q(a) = 0$, alors $X - a|Q$ et donc $Q = (X-a)R$, ainsi, $P = (X-a)^{m+1}R$ ce qui contredit le fait que m soit la multiplicité de a dans P. Donc $Q(a) \neq 0$.

$2 \Longrightarrow 1$ Supposons que $P = (X-a)^m Q$ avec $Q(a) \neq 0$. Notons μ la multiplicité de a. Comme $(X-a)^m|P$, $m \leqslant \mu$, alors $P = (X-a)^\mu R$ pour un certain $R \in \mathbb{K}[X]$. En factorisant la différence des deux expressions de P, on obtient :

$$P - P = (X-a)^m \left[(X-a)^{\mu-m}R - Q\right] = 0$$

Comme $(X-a)^m$ n'est pas le polynôme nul, par intégrité de $\mathbb{K}[X]$, $(X-a)^{\mu-m}R - Q = 0$. En substituant a à X, on obtient $Q(a) = (a-a)^{\mu-m}R(a) \neq 0$ ce qui est possible que si $\mu = m$. Ainsi, m est bien la multiplicité de a.

$2 \Longrightarrow 3$ Supposons que $P = (X-a)^m Q$ avec $Q(a) \neq 0$. Alors, on calcule $P^{(i)}$ pour $i \in [\![0 ; m]\!]$, grâce à la formule de Leibniz et on observe que $P^{(i)}(a) = 0$ pour $i < m$ et $P^{(m)}(a) \neq 0$.

$3 \Longrightarrow 2$ Supposons que pour tout $i \in [\![0 ; m-1]\!]$, $P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$. Alors en appliquant la formule de Taylor :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = (X-a)^m \underbrace{\left[\sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}\right]}_{Q}$$

Avec $Q(a) = \dfrac{P^{(m)}(a)}{m!} \neq 0$. ■

Exemple 9. Si $P = X^3 - 7X^2 + 15X - 9$, quelles sont les multiplicités de 1, 2 et 3 dans P ?

Proposition n° 7 : racine et racine conjugué d'un polynôme réel

Soit $P \in \mathbb{R}[X]$ et $z \in \mathbb{C}$ une racine de P, alors $\overline{z}$ est aussi racine de P avec même multiplicité que z.

Démonstration de la proposition n° 7 : Soit $Q = \sum\limits_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$ tel que $Q(z) = 0$, alors

$$Q(\overline{z}) = \sum_{k=0}^{n} a_k \overline{z}^k = \sum_{k=0}^{n} \overline{a_k}\,\overline{z^k} = \sum_{k=0}^{n} \overline{a_k z^k} = \overline{\sum_{k=0}^{n} a_k z^k} = \overline{Q(z)} = \overline{0} = 0$$

De même, si $Q(\overline{z}) = 0$ alors en appliquant ce résultat à $z' = \overline{z}$, $Q(z) = 0$. Ce qui montre que z est racine de Q ssi $\overline{z}$ est racine de Q. Ainsi, pour $k \in \mathbb{N}$, $P^{(k)}(z) = 0$ si et seulement si $P^{(k)}(\overline{z}) = 0$. Ainsi, d'après la proposition 9, z et $\overline{z}$ sont racines de P avec même multiplicité. ■

2.4 Polynômes irréductibles et factorisation d'un polynôme

Définition d'un polynôme scindé, scindé à racines simples

On dit que $P \in \mathbb{K}[X]$ est **scindé** dans $\mathbb{K}[X]$ s'il s'écrit comme le produit de polynômes de degré 1.
De plus, s'il est scindé et que toutes ses racines sont simples, on dit qu'il est **scindé à racines simples**.

Exemple 10. $X^2 + 1$ est scindé à racines simples dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$.

Remarque 6. Soit P un polynôme et $\lambda \in \mathbb{K}^*$, alors $\lambda P|P$ et $\lambda|P$. On dit que λP et λ sont des **diviseurs triviaux**.

Définition d'un polynôme irréductible

Un polynôme $P \in \mathbb{K}[X]$ non constant est dit **irréductible** si ses seuls diviseurs sont λP et λ pour $\lambda \in \mathbb{K}^*$.

Exemples 11.
1. $X^2 - 3X + 2$ n'est pas irréductible.
2. Les polynômes de degré 1 de $\mathbb{K}[X]$ sont irréductibles.
3. Les polynômes de degré 2 de $\mathbb{R}[X]$ dont le discriminant est strictement négatif sont irréductibles.

Solution des exemples 11 :

1. $(X^2 - 3X + 2) = (X-1)(X-2)$, ainsi $X - 1$ divise $X^2 - 3X + 2$ et $X - 1$ n'est ni un polynôme constant est n'est pas de la forme $\lambda(X^2 - 3X + 2)$ (par exemple pour des raisons de degrés). Ainsi, $X^2 - 3X + 2$ n'est pas un polynôme irréductible.
2. Soit P un polynôme de degré 1. Montrons qu'il est irréductible. Si D un diviseur de P, montrons que D est constant ou colinéaire à P. Il existe $Q \in \mathbb{C}[X]$ tel que $P = DQ$. Ainsi, $1 = d^\circ P = d^\circ D + d^\circ Q$. Remarquons que D et Q ne peuvent pas être nuls (car sinon le produit ne vaut pas P). Ainsi, $d^\circ D$ et $d^\circ Q$ sont des entiers naturels. Donc $d^\circ D = 0$ ou $d^\circ D = 1$. Si $d^\circ D = 0$ alors D est constant. Si $d^\circ D = 1$, alors $d^\circ Q = 0$ et donc $Q = \lambda \in \mathbb{K}^*$, dès lors, $D = \dfrac{1}{\lambda}P$. Bref, dans tous les cas, D est un diviseur trivial de P. Par conséquent, P est irréductible.
3. Soit $P \in \mathbb{R}[X]$ de degré 2 dont le discriminant est strictement négatif. Si $D \in \mathbb{R}[X]$ tel que $D|P$, alors il existe $\mathbb{R} \in \mathbb{R}[X]$ tel que $P = DR$. En utilisant les degrés, on obtient que $d^\circ P = d^\circ D + d^\circ R$, ainsi, $d^\circ D \in \{0, 1, 2\}$. Si $d^\circ D = 1$, alors $D = aX + b$ admet une racine $x \in \mathbb{R}$, donc $P(x) = D(x)R(x) = 0$, ce qui est impossible, car P a un discriminant strictement négatif, donc $d^\circ D = 0$ (donc D est constant) ou $d^\circ D = 2$ (et donc R est constant, en notant c la constante non nulle, on a $P = Dc$ donc $D = \lambda P$ avec $\lambda = \dfrac{1}{c}$). Ceci prouve que P est irréductible.

Théorème n° 3 de d'Alembert-Gauss (théorème fondamental de l'algèbre) *(admis)*

Soit $P \in \mathbb{C}[X]$ un polynôme non constant, alors P admet au moins une racine complexe.

Exemple 12. Donner le degré, le coefficient dominant, les racines et leur multiplicités de $P = 3(X-1)^4(X-2)^2$.

Théorème n° 4 : factorisation d'un polynôme à coefficients réels ou complexes

1. Si $P \in \mathbb{C}[X]$ est non constant, alors il est scindé : il s'écrit sous la forme $$P = \lambda \prod_{i=1}^{r} (X - z_i)^{m_i}$$
   Cette décomposition est unique à l'ordre des facteurs près : λ est le coefficient dominant, les $z_i \in \mathbb{C}$ sont les racines (deux à deux distinctes) de multiplicité $m_i \in \mathbb{N}^*$.
2. Si $P \in \mathbb{R}[X]$ est non constant, alors P s'écrit sous la forme $$P = \lambda \prod_{i=1}^{r} (X - x_i)^{m_i} \times \prod_{i=1}^{s} {Q_i}^{n_i}$$
   Cette décomposition est unique à l'ordre des facteurs près : λ est le coefficient dominant, les $x_i \in \mathbb{R}$ sont les racines (deux à deux distinctes) de multiplicité $m_i \in \mathbb{N}^*$, Q_i des polynômes unitaires de degré 2 à discriminant strictement négatifs et $n_i \in \mathbb{N}^*$.

Démonstration du théorème n° 4 :

1. Posons l'hypothèse de récurrence : $\mathscr{P}(k)$: «Si $d^\circ P = k$, alors il existe des complexes z_i deux à deux distincts, des entiers naturels non nuls m_i et $\lambda \in \mathbb{C}^*$ tels que $P = \lambda \prod_{i=1}^{r} (X - z_i)^{m_i}$ ».
   - Si $k = 1$. Prenons donc $P \in \mathbb{C}[X]$ de degré 1. Alors $P = aX + b$ avec $(a, b) \in \mathbb{C}^2$ et $a \neq 0$, alors $P = a\left(X - \dfrac{-b}{a}\right)$. P est donc bien de la forme voulue. Ainsi, $\mathscr{P}(1)$ est vraie.
   - Soit $k \in \mathbb{N}$. Supposons par récurrence forte que pour tout $j \in [\![1\,; k]\!]$, $\mathscr{P}(j)$ vraie. Soit $P \in \mathbb{C}[X]$ tel que $d^\circ P = k + 1 \geqslant 1$. Alors d'après le théorème de d'Alembert-Gauss, P admet une racine $z_1 \in \mathbb{C}$. Notons $m_1 \in \mathbb{N}^*$ sa multiplicité : il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - z_1)^{m_1} Q$ avec $Q(z_1) \neq 0$. Si Q est constant alors (Q est nécessairement non nul) et $P = \lambda(X - z_1)^{m_1}$ avec $\lambda = Q \in \mathbb{C}^*$ convient. Si $d^\circ Q \geqslant 1$: or, $n + 1 = d^\circ P = m_1 + d^\circ Q$. Ceci prouve que $d^\circ Q = k + 1 - m_1 \leqslant n$ (car $m_1 \geqslant 1$). Si on note $j = d^\circ Q$, alors $j \in [\![1\,; n]\!]$, d'après l'hypothèse de récurrence forte, $\mathscr{P}(j)$ est vraie. Donc $Q = \lambda \prod_{i=2}^{r} (X - z_i)^{m_i}$ pour des z_i 2 à 2 distincts, $m_i \in \mathbb{N}^*$ et $\lambda \in \mathbb{C}^*$. Notons, que comme $Q(z_1) \neq 0$, $Q(z_2) = 0$, $Q(z_3) = 0$, …, $Q(z_r) = 00$, on en déduit que $z_1 \neq z_2$, $z_1 \neq z_3$, …, $z_1 \neq z_r$. Ainsi, $P = \lambda \prod_{i=1}^{r} (X - z_i)^{m_i}$ avec $\lambda \in \mathbb{C}^*$, les z_i 2 à 2 distincts et $m_i \in \mathbb{N}^*$. Ainsi, $\mathscr{P}(k+1)$ est vraie.
   - Par récurrence forte, pour tout $k \in \mathbb{N}^*$, $\mathscr{P}(k)$ est vraie.

   Montrons que si $P = \lambda \prod_{i=1}^{r} (X - z_i)^{m_i}$ avec les z_i deux à deux distincts, les m_i des entiers naturels non nuls et $\lambda \in \mathbb{C}^*$, alors nécessairement les racines de P sont exactement les z_i avec chacune une multiplicité m_i et que λ est le coefficient dominant. Fixons $j \in [\![1\,; r]\!]$, alors, en isolant le terme pour $i = j$:
$$P = (X - z_j)^{m_j} \lambda \prod_{\substack{i=1 \\ i \neq j}}^{r} (X - z_i)^{m_i} = (X - z_j)^{m_j} Q \quad \text{avec} \quad Q(z_i) = \lambda \prod_{\substack{i=1 \\ i \neq j}}^{r} (z_j - z_i)^{m_i} \neq 0$$

Donc z_j est bien une racine de P de multiplicité m_j. Réciproquement si z est une racine de P alors $0 = P(z) = \lambda \prod_{i=1}^{r} (z - z_i)^{m_i}$, un produit de termes étant nul, on en déduit que l'un d'eux est nul, donc il existe $i \in [\![1\,; r]\!]$ tel que $(z - z_i)^{m_i} = 0$, donc que $z = z_i$, ainsi les racines de P sont exactement les z_i. De plus, en développant le produit $P = \lambda \prod_{i=1}^{r} (X - x_i)^{m_i}$, le terme de plus haut degré est $\lambda X^{\sum_{i=1}^{r} m_i}$ avec $\lambda \neq 0$, ainsi λ est bien le coefficient dominant de P.

2. Soit $P \in \mathbb{R}[X]$ non constant. Alors $P \in \mathbb{C}[X]$ et donc d'après le résultat précédent, $P = \lambda \prod_{i=1}^{p} (X - z_i)^{m_i}$. Avec les z_i des complexes 2 à 2 différents et $m_i \in \mathbb{N}^*$. Parmi ces z_i, un certain nombre sont réels, quitte à les renommer on va supposer que x_1, x_2,... x_s sont réels. Et que les autres : $z_{s+1}, z_{s+2}, \ldots, z_p$ sont des complexes non réels. Rappelons que si P admet une racine complexe z, alors $\overline{z}$ est aussi racine avec même multiplicité. Donc quitte à renommer, on peut supposer les racines complexes non réels sont rangés ainsi $(z_1, \overline{z_1}, z_2, \overline{z_2}, \ldots, z_s, \overline{z_s})$. Avec n_i la multiplicité commune de z_i et $\overline{z_i}$. Dès lors, on a

$$P = \lambda \prod_{i=1}^{s} (X - x_i)^{m_i} \times \prod_{i=1}^{s} (X - z_i)^{n_i} (X - \overline{z_i})^{n_i} = \lambda \prod_{i=1}^{s} (X - x_i)^{m_i} \times \prod_{i=1}^{s} [(X - z_i)(X - \overline{z_i})]^{n_i}$$

Remarquons que $(X - z_i)(X - \overline{z_i}) = X^2 - 2\mathrm{Re}(z_i)X + |z_i|^2$ est bien un polynôme réel de degré 2 à discriminant strictement négatif (en effet ses racines sont complexes non réelles).

Pour exactement les mêmes raisons que pour le cas complexe, λ est le coefficient dominant de P, les x_i sont les racines réelles de P de multiplicité m_i. ■

Remarques 7.
- Un polynôme à coefficients complexes de degré n a donc toujours exactement n racines **complexes comptées avec multiplicité** contrairement au nombre de racines réelles d'un polynôme à coefficients réels. Les réels sont plus complexes que les complexes...
- Un polynôme $B \in \mathbb{C}[X]$ non nul divise A ssi toute racine de B est racine de A avec une multiplicité dans A supérieure ou égale à celle dans B.

Exemple 13. Soit $n \in \mathbb{N}^*$. Factoriser $X^n - 1$ dans $\mathbb{C}[X]$.

Proposition n° 8 : irréductibilité des polynômes de $\mathbb{K}[X]$

1. Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement ceux de degré 1.
2. Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement ceux de degré 1 et ceux de degré 2 dont le discriminant est strictement négatif.

Démonstration de la proposition n° 8 :

1. On a déjà montré à l'exemple 11 que les polynômes de degré 1 sont irréductibles.
   Réciproquement, soit P un polynôme irréductible. Comme P est non constant, P admet au moins une racine z, donc $X - z | P$, or les seuls diviseurs de P sont triviaux et $X - z$ n'est pas constant, donc $(X - z) = \lambda P$ avec $\lambda \in \mathbb{C}^*$, en passant au degré, on obtient que $d^\circ P = 1$.
2. Soit $P \in \mathbb{R}[X]$ de degré 1 ou de degré 2 avec un discriminant strictement négatif, alors il est irréductible (exemple 11).
   Réciproquement, si $P \in \mathbb{R}[X]$ est irréductible. Alors, d'après ce qu'on a prouvé, $P = \lambda \prod_{i=1}^{r} R_i{}^{m_i}$ où R_i est soit un polynôme de degré 1, soit un polynôme de degré 2 à discriminant strictement négatif. Or, $R_1 | P$, R_1 n'est pas constant et P est irréductible, donc il existe $\lambda \in \mathbb{R}^*$ tel que $P = \lambda R_1$. Ainsi, $d^\circ P = d^\circ R_1 \in \{1, 2\}$. Si, $d^\circ R_1 = 2$, alors son discriminant est strictement négatif, donc celui de P aussi.
   Ainsi, les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et ceux de degré 2 dont le discriminant est strictement négatif. ■

Exemple 14. Combien $P = (X^2 + 1)(X^2 - 6X + 9)$ admet-il de racines réelles ? complexes ?

Proposition n° 9 : racines comptées avec multiplicité

Soit $P \in \mathbb{K}[X]$ non nul, x_1, x_2, …, x_r des racines (2 à 2 distinctes) de P de multiplicités m_1, m_2, …, m_r.

1. $\prod_{i=1}^{r} (X - x_i)^{m_i} | P$
2. $\sum_{i=1}^{r} m_i \leqslant d^\circ P$.
3. Si $P \in \mathbb{K}_n[X] \backslash \{0\}$, P admet au plus n racines.
4. Si $P \in \mathbb{K}_n[X]$ a au moins $n+1$ racines, alors $P = 0$.
5. Soit $(P, Q) \in \mathbb{K}_n[X]^2$, si P et Q coïncident en $n + 1$ points, alors $P = Q$.

Démonstration de la proposition n° 9 :

1. Si x_1, x_2, ..., x_r des racines de P de multiplicités m_1, m_2..., m_r (pas forcément toutes les racines de P, alors d'après la factorisation, P s'écrit comme un produit de termes dans lequel apparaît $\prod_{i=1}^{r}(X-x_i)^{m_i}$, ainsi, $P = \prod_{i=1}^{r}(X-x_i)^{m_i}Q$ avec $Q \in \mathbb{K}[X]$. En passant au degré, $d^\circ P = \sum_{i=1}^{r} m_i + d^\circ Q$. Nécessairement Q est non nul donc $d^\circ Q \geqslant 0$. Dès lors, $\sum_{i=1}^{r} m_i \leqslant d^\circ P$.
2. Notons $(x_1, x_2, \ldots, x_{n+1})$ des racines de P deux à deux distinctes et m_i leur multiplicité. Supposons $P \neq 0$ d'après ce qui précède, $n+1 \leqslant \sum_{i=1}^{n+1} m_i \leqslant d^\circ P \leqslant n$ ce qui est impossible. Donc $P = 0$.
3. Si $P(x_i) = Q(x_i)$ pour tout $i \in [\![0\,; n]\!]$ avec $(x_0, x_1, \ldots, x_n)$ des réels deux à deux distincts, alors $P - Q$ a au moins $n+1$ racines et $P - Q \in \mathbb{K}_n[X]$ d'après le point précédent $P - Q = 0$ donc $P = Q$. ■

Exemple 15. Si $P = \lambda(X-x_1)(X-x_2)$, $Q = \mu(X-x_1)(X-x_2)(X-x_3)$, quels sont les coefficients de P ? de Q ?

Proposition n° 10 : relations coefficients-racines

Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de degré n scindé : $P = \lambda \prod_{k=1}^{n}(X-x_k)$, alors :

1. $\lambda = a_n$
2. $\sum_{k=1}^{n} x_k = -\dfrac{a_{n-1}}{a_n}$
3. $\prod_{k=1}^{n} x_k = \dfrac{(-1)^n a_0}{a_n}$

Remarque 8. Dans cette proposition, on ne suppose pas que les racines sont simples, si une racine est de multiplicité 3, il y aura trois des x_k qui seront égaux.

Exemples 16. 1. Soit un entier $n \geqslant 2$. Quelle est la somme et le produit des racines n-ièmes de l'unité ?

2. Factoriser $X^2 - 2\cos(\theta)X + 1$.
3. Factoriser $2X^3 - 26X^2 + 46X - 22$ (commencer par chercher une racine évidente et sa multiplicité).

3 Décomposition en éléments simples

Soit A et B deux polynômes avec B non nul, on dit que la fonction $x \mapsto A(x)/B(x)$ est une **fonction rationnelle** définie sur $\mathbb{C}\backslash E$ où E est l'ensemble des racines de B. Si x est racine de B, on dit que x est un **pôle** de $x \mapsto A(x)/B(x)$ et n'est bien sûr par dans l'ensemble de définition de $x \mapsto A(x)/B(x)$.

Théorème n° 5 : décomposition en éléments simples d'une fraction à pôles simples *(admis)*

Soit $(R, B) \in \mathbb{K}[X]^2$ tel que $d^\circ R < d^\circ B$ et B scindé à racines simples, de racines $b_1, b_2, \ldots, b_n$. Il existe un unique $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{K}^n$ tels que : $\forall x \in \mathbb{C}\backslash\{b_1, \ldots, b_n\}$ $\dfrac{R(x)}{B(x)} = \sum_{i=1}^{n} \dfrac{\alpha_i}{x - b_i}$.

Comment effectuer la décomposition en éléments simples ?

1. Effectuer la division euclidienne de A par B : $A = BQ + R$, avec $d^\circ R < d^\circ B$.
2. Trouver les racines de B (et vérifier qu'il est bien scindé à racines simples) notées $b_1, b_2, \ldots, b_n$.
3. Si x n'est pas une racine de B, alors $\dfrac{A(x)}{B(x)} = Q(x) + \dfrac{R(x)}{B(x)}$
4. Écrire $\dfrac{R(x)}{B(x)} = \sum_{k=1}^{n} \dfrac{\alpha_k}{x - b_k}$
5. Multiplier par $x - b_i$ et remplacer x par b_i, on trouve ainsi la valeur de α_i.
6. Conclure que $\dfrac{A(x)}{B(x)} = Q(x) + \sum_{k=1}^{n} \dfrac{\alpha_k}{x - b_k}$.

Exemple 17. Décomposer en éléments simples $x \mapsto \dfrac{x^5+1}{x^3-6x^2+11x-6}$. En déduire une primitive.

Péril imminent à ne pas oublier la division euclidienne

Si $d^\circ A \geqslant d^\circ B$, il faut faire la division euclidienne : c'est $\dfrac{R(x)}{B(x)}$ que l'on écrit comme $\sum\limits_{i=1}^{n} \dfrac{\alpha_i}{x-b_i}$ et non $\dfrac{A(x)}{B(x)}$.

Attention il faut que le polynôme soit scindé à racines simples pour appliquer le théorème

S'il y a une racine double cela ne fonctionne pas. Par exemple, si $B = (X-1)(X-1)$, vous ne pouvez pas trouver a_1 et a_2 tels que $\dfrac{A(x)}{B(x)} = Q(x) + \dfrac{a_1}{x-1} + \dfrac{a_2}{x-1}$. De même si B n'est pas scindé. Dans ce cas, il faudra que la forme de la décomposition en éléments simples vous soit donnée car elle n'est pas au programme.

4 Construction des polynômes (non exigible)

Dans cette partie, hors programme, nous allons donner une «*vraie*» définition des polynômes. En particulier, nous répondrons à la question suivante : mais qui est ce mystérieux X ? En effet, on l'a dit, X n'est ni un nombre, ni une variable ni une fonction.

Définition des polynômes

On appelle **polynôme** à coefficients dans $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ nulle à partir d'un certain rang : il existe $N \in \mathbb{N}$ tel que pour tout entier $n \geqslant N$, $a_n = 0$.

Remarque 9. En tant que suites, deux polynômes $(a_n)_n$ et $(b_n)_n$ sont égaux ssi pour tout $n \in \mathbb{N}$, $a_n = b_n$.

Définition des opérations sur les polynômes

Soit $P = (a_n)_n$ $Q = (b_n)_n$ deux polynômes $\lambda \in \mathbb{K}$, on pose $\lambda P = (\lambda a_n)_n$, $P+Q = (a_n+b_n)_n$ et $PQ = \left(\sum\limits_{k=0}^{n} a_k b_{n-k}\right)_n$.

On vérifie alors que λP, $P+Q$ et PQ sont bien des polynômes, *i.e.* des suites nulles à partir d'un certain rang.

Exemples 18. Si $P = (1,2,3,0,0,\ldots)$, plus rigoureusement, $P = (a_n)_{n\in\mathbb{N}}$ avec $a_0 = 1$, $a_1 = 2$, $a_2 = 3$ et pour tout entier $n \geqslant 3$, $a_n = 0$, $Q = (3,2,1,2,0,0,\ldots,)$, $R = (1,0,0,\ldots)$, $S = (0,1,0,0,\ldots)$ et $\lambda = 2$ alors

- $\lambda P = (2,4,6,0,0,\ldots)$
- $P+Q = (4,4,4,2,0,0,\ldots)$
- $PQ = (3,8,14,10,7,6,0,0,0\ldots)$
- $R^2 = R \times R = (1,0,0,\ldots)$
- $RP = P$
- $S^2 = S \times S = (0,0,1,0,0,\ldots)$
- $S^3 = S^2 \times S = (0,0,0,1,0,0,\ldots)$

Proposition n° 11 : propriétés algébriques des polynômes

L'addition est commutative, associative, tout polynôme admet un polynôme opposé.
La multiplication est commutative, associative et distributive par rapport à l'addition.
Le polynôme R est l'élément neutre pour la multiplication : pour tout polynôme P, $PR = P$.

Remarque 10. On pose $X = S = (\delta_{1,n})_{n\in\mathbb{N}}$ et $1 = R = (\delta_{0,n})_{n\in\mathbb{N}}$. Pour tout polynôme P, on pose $P^0 = R = 1$ et pour tout $n \in \mathbb{N}^*$, $P^n = P \times P \times \ldots \times P$.

Théorème n° 6 : décomposition d'un polynôme en fonction des puissances de X

Avec les notations précédentes, pour tout $k \in \mathbb{N}$, $X^k = (\delta_{n,k})_{n\in\mathbb{N}}$.

Soit un polynôme $P = (a_n)_n$, une suite nulle à partir du rang N, alors $$P = \sum_{n=0}^{N} a_n X^n.$$

Remarques 11.

- Ainsi, ici, l'identité $P = \sum_{n=0}^{N} a_n X^n$ n'est pas issue de la définition même d'un polynôme mais elle provient d'un théorème.
- Dès qu'on a posé $X = (\delta_{1,n})_{n\in\mathbb{N}}$, on décide de nommer $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$. La notation X est donc une lettre, muette, pour désigner un polynôme particulier. Le X n'est donc ni une variable, ni un nombre réel, mais une certaine suite. En particulier, on aurait aussi pu poser $Y = (\delta_{1,n})_{n\in\mathbb{N}}$ et dans ce cas $\mathbb{K}[Y]$ désignerait l'ensemble des polynômes.
- Ceci est un procédé théorique de construction pour justifier l'existence et les notations des polynômes. Dans la pratique, on préfère oublier que ce sont des suites nulles à partir d'un certain rang et utiliser le X comme un objet mystère en feignant d'ignorer sa vraie nature.
- Cela est très similaire à la construction de $\mathbb{C}$, on construit i comme un couple de réels et on feint d'ignorer sa vraie nature et on se réduit à l'utiliser comme un élément dans le carré vaut -1.