19 | Polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$

Il est impossible de résoudre par des radicaux l'équation générale du cinquième degré.

Niels Henrik Abel, 1802-1829

Dans ce cours, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

I – Une petite introduction à la notion de polynôme

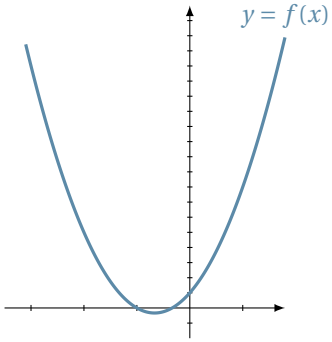
Jusqu'ici, vous n'avez jamais distingué les « polynômes » des « fonctions polynomiales », qui sont pour vous toutes les fonctions sur $\mathbb{R}$ de la forme $x \longmapsto a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ avec $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{R}$. Nous allons voir dans ce chapitre qu'en fait **NON, LES « POLYNÔMES » NE SONT PAS DES FONCTIONS** .

Notons par exemple P le polynôme $3X^2 + 4X + 1$. Calculer $P(5)$, c'est transformer 5 en un autre nombre conformément à certaines opérations élémentaires - puissances, multiplication par un réel et addition. Or il y a tout un tas de mondes mathématiques dans lesquels on sait calculer des puissances, multiplier par un réel et additionner les objets :

- $\mathbb{R}$ bien sûr — d'où la possibilité de calculer $P(5)$,
- l'ensemble des matrices $\mathcal{M}_n(\mathbb{R})$ - d'où la possibilité de calculer $P(A)$ pour tout $A \in \mathcal{M}_n(\mathbb{R})$,
- l'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ - d'où la possibilité de noter $P(\exp)$ la fonction $x \longmapsto 3\mathrm{e}^{2x} + 4\mathrm{e}^x + 1$.

En fait, dans tout anneau A dans lequel on sait multiplier par un réel, on a bien envie de poser $P(a) = 3a^2 + 4a + 1_A$ pour tout $a \in A$. On en a bien envie, certes, mais il faut dans ce cas renoncer à l'idée qu'un polynôme est une fonction, car la **FONCTION** $x \longmapsto 3x^2 + 4x + 1$ est définie sur $\mathbb{R}$, pas sur $\mathcal{M}_n(\mathbb{R})$ ou $\mathbb{R}^{\mathbb{R}}$. Finalement, on ne sait toujours pas ce qu'est le polynôme $P = 3X^2 + 4X + 1$, mais ce n'est pas la gentille fonction $x \xmapsto{f} 3x^2 + 4x + 1$ en tout cas.

Le piège, c'est que jusqu'ici, quand on vous définissait une fonction polynomiale, on vous donnait aussi ses coefficients. Or, quand on connaît la suite $(1,4,3)$ des coefficients de f, on peut facilement calculer toutes ses valeurs, par exemple $f(5) = 3\times5^2+4\times5+1 = 96$, mais quand on connaît f comme **FONCTION, C'EST-À-DIRE PAR LA DONNÉE COMPLÈTE DE SES VALEURS** , peut-on déterminer ses coefficients ? Vous pouvez tenter l'expérience sur la figure ci-contre, vous ne les « verrez » pas directement. Conclusion : l'essentiel, ce sont les coefficients, pas le fait qu'on se donne une fonction. L'essentiel du polynôme $3X^2 + 4X + 1$ n'est pas la nature de son X mais la liste $(1,4,3)$ de ses coefficients degré par degré. Vous voilà maintenant prêts pour la définition des polynômes.



Définition 19.1 (Polynômes à une indéterminée à coefficients dans $\mathbb{K}$) – On appelle polynôme (à une indéterminée) à coefficients dans $\mathbb{K}$ toute suite presque nulle d'éléments de $\mathbb{K}$, i.e. toute suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{N}$ dont tous les éléments sont nuls à partir d'un certain rang. Pour tout $k \in \mathbb{N}$, le coefficient a_k est appelé le coefficient de degré k du polynôme.
L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ si on choisit de noter X l'indéterminée.

ATTENTION ! L'indéterminée X est un nouvel objet, bien précis, et n'est pas un nombre !

Conformément à cette définition, un polynôme est une suite de la forme $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$ à coefficients dans $\mathbb{K}$. Nous **NOTERONS** conformément à l'habitude $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ une telle suite, mais il peut être utile de garder en tête cette définition pour bien comprendre la suite de ce chapitre.

Quoi qu'on pense de son abstraction, la définition précédente rend au moins trivial le résultat suivant, si l'on n'oublie pas ce que c'est qu'une suite. Le résultat analogue sur les **FONCTIONS** polynomiales est autrement délicat !

Théorème 19.2 – Identification des coefficients
Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

II – Généralités sur les polynômes

1 – Définitions et opérations sur les polynômes

Définition 19.3 – Soit $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{K}[X]$.

- Si $a_n \neq 0$, alors le réel a_n est appelé **coefficient dominant** du polynôme P. S'il est égal à 1 , on dit que P est **unitaire**.
- Si $a_n \neq 0$, alors l'entier n est appelé le **degré** du polynôme P et on note $\deg(P) = n$.
- Le polynôme dont tous les coefficients sont nuls est appelé le **polynôme nul** et il est noté $0_{\mathbb{K}[X]}$.
- Tout polynôme de la forme $a_i X^i$ où $i \in \mathbb{N}$ et $a_i \in \mathbb{K}$, est appelé un **monôme**.
- Les polynômes de la forme a_0 sont appelés les **polynômes constants**.

Remarque 19.4 – Par convention, le polynôme nul a pour degré $-\infty$. Un polynôme constant non nul est de degré 0.

Exemple 19.5 – Le polynôme $P = -3X^5 + 2X^3 + X^2 + X - 4$ est un polynôme de degré 5 et de coefficient dominant égal à -3 .

Définition 19.6 – Pour tout entier naturel n, on note $\mathbb{K}_n[X]$ **l'ensemble des polynômes de degré inférieur ou égal à n.** On a donc

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

Exemple 19.7 – $\mathbb{C}_2[X] = \{aX^2 + bX + c \mid (a,b,c) \in \mathbb{C}^3\}$.
L'ensemble $\mathbb{R}_0[X]$ est l'ensemble des polynômes réels constants (y compris le polynôme nul).

Définition 19.8 (Égalité et opérations) **–**
Soient $p, q \in \mathbb{N}$, $P = a_0 + a_1 X + \cdots + a_p X^p$ et $Q = b_0 + b_1 X + \cdots + b_q X^q$ deux polynômes à coefficients dans $\mathbb{K}$.
Quitte à rajouter des coefficients nuls, on peut écrire P et Q sous la forme ($n = \max(p,q)$) :

$$P = a_0 + a_1 X + \cdots + a_n X^n = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad Q = b_0 + b_1 X + \cdots + b_n X^n = \sum_{i=0}^{n} b_i X^i$$

1. P et Q sont dit **égaux** si et seulement si tous leurs coefficients sont les mêmes :
$$P = Q \iff \forall k \in [\![0, n]\!],\ a_k = b_k$$
2. La **somme** de P et Q est
$$P + Q = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n = \sum_{i=0}^{n} (a_i + b_i) X^i$$
3. La **multiplication externe** de P par un scalaire $\lambda \in \mathbb{K}$ est
$$\lambda \cdot P = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n = \sum_{i=0}^{n} \lambda a_i X^i$$
4. Le **produit** de P et Q est
$$P \times Q = \sum_{i=0}^{p+q} c_i X^i \quad \text{où} \quad \forall i \in \mathbb{N},\ c_i = \sum_{\substack{k+\ell=i \\ k \in \{0,\ldots,p\} \\ \ell \in \{0,\ldots,q\}}} a_k b_\ell = \sum_{\ell=0}^{i} a_{i-\ell} b_\ell$$

Ces opérations confèrent au triplet $(\mathbb{K}[X], +, \times)$ une structure d'anneau commutatif, d'éléments neutres le polynôme nul pour + et le polynôme constant 1 pour ×.

Exemple 19.9 – $(X^5+2X-i)+(X^3-X^2-X+i)=X^5+X^3-X^2+X$,
$(3X^3-4X+1)+(-3X^3+X^2+1)=X^2-4X+2$,
$(X+1)\cdot(-iX^2+X+2)=-iX^3+(1-i)X^2+3X+2$.

Le résultat suivant ne nous est d'aucune utilité pour le moment, mais nous l'utiliserons plus tard dans nos pérégrinations probabilistes et c'est pile poil le bon moment pour le démontrer.

Exemple 19.10 – Formule de Vandermonde : pour tout $n\in\mathbb{N}$: $\displaystyle\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

Démonstration. L'égalité $(X+1)^{2n}=(X+1)^n(X+1)^n$ s'écrit aussi : $\displaystyle\sum_{k=0}^{2n}\binom{2n}{k}X^k=\sum_{i=0}^{n}\binom{n}{i}X^i\times\sum_{j=0}^{n}\binom{n}{j}X^j$. À gauche, le coefficient de degré n vaut $\binom{2n}{n}$, et il vaut $\displaystyle\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}=\sum_{i=0}^{n}\binom{n}{i}^2$ à droite par définition du produit de deux polynômes.
produit de deux polynômes. □

Le théorème 19.2 justifie ce qu'on appelle la **méthode d'identification** des coefficients de deux polynômes égaux.

Exemple 19.11 – Soit P le polynôme défini par : $P=X^4-6X^3+13X^2-12X+4$.
Montrer que P est le carré d'un polynôme Q de degré 2 à déterminer.
On cherche un polynôme Q de degré 2 tel que $P=Q^2$. Posons $Q=aX^2+bX+c$. Calculons :

$$\begin{aligned}Q^2&=(aX^2+bX+c)^2=a^2X^4+2abX^3+2acX^2+b^2X^2+2bcX+c^2\\&=a^2X^4+2abX^3+(2ac+b^2)X^2+2bcX+c^2\end{aligned}$$

Pour que $P=Q^2$, par unicité de l'écriture d'un polynôme, on identifie les coefficients :

$$\begin{cases}a^2&=1\\2ab&=-6\\2ac+b^2&=13\\2bc&=-12\\c^2&=4\end{cases}\iff\begin{cases}a&=1\\b&=-3\\c&=2\end{cases}\text{ ou }\begin{cases}a&=-1\\b&=3\\c&=-2\end{cases}.$$

Ainsi $P=(X^2-3X+2)^2$ ou $P=(-X^2+3X-2)^2$.

2 – Composition des polynômes

Définition 19.12 – Soit $P=\displaystyle\sum_{k=0}^{n}a_kX^k$ et Q deux polynômes de $\mathbb{K}[X]$.
On définit le **polynôme composé** $P\circ Q$, noté aussi $P(Q)$ par

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

Exemple 19.13 – Si $P=X^2+2X-1$ et $Q=X+3$, alors
$P\circ Q=(X+3)^2+2(X+3)-1=X^2+6X+9+2X+6-1=X^2+8X+14$.

Remarque 19.14 – Dans le cas particulier où $Q=X$, le polynôme $P\circ Q=P(Q)=P(X)$ est égal à P. On peut donc aussi bien utiliser la notation $P(X)$ que la notation P pour désigner le polynôme P.

3 – Propriétés du degré

Proposition 19.15

Soient P et Q deux polynômes de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

- $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$,
- $\deg(\lambda P) = \deg(P)$ si $\lambda \neq 0$,
- $\deg(P \times Q) = \deg(P) + \deg(Q)$,
- Si $\deg(Q) \geqslant 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

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

De plus, on peut préciser que si

- Si $\deg(P) \neq \deg(Q)$ alors $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big)$.
- Si P et Q ne sont pas nuls, si $\deg(P) = \deg(Q)$ et que les coefficients dominants de P et Q ne sont pas opposés, alors $\deg(P+Q) = \max\big(\deg(P), \deg(Q)\big) = \deg(P) = \deg(Q)$.

Exemple 19.16 – Soit $P = 3X^2 + X + 1$, $Q = -X^3 + 1$ et $R = X^3 + X^2 + 1$. Alors, $\deg(P) = 2$, $\deg(Q) = 3$ et $\deg(R) = 3$.
$P + Q = -X^3 + 3X^2 + X + 2$,
$Q + R = X^2 + 2$ et
$P \times Q = -3X^5 - X^4 - X^3 + 3X^2 + X + 1$.
On constate que $\deg(P+Q) = 3 = \max\big(\deg(P), \deg(Q)\big)$, $\deg(Q+R) = 2 < \max\big(\deg(P), \deg(Q)\big)$ et $\deg(P \times Q) = 5 = \deg(P) + \deg(Q)$.

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

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

  Dans tous les cas, on constate que $\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big)$.
- Degré d'un produit.
  - Si $P = 0$ ou $Q = 0$, alors $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$, et $P \times Q = 0$ donc $\deg(P \times Q) = -\infty = \deg(P) + \deg(Q)$.
  - On suppose que $P \neq 0$ et $Q \neq 0$. Alors P et Q s'écrivent $P = \sum_{i=0}^{d} a_i X^i$ et $Q = \sum_{i=0}^{d'} b_i X^i$ où $a_0, \dots, a_d, b_0, \dots, b_{d'} \in \mathbb{K}$ et $a_d \neq 0$ et $b_{d'} \neq 0$. On a
  $$P \times Q = \sum_{i=0}^{d+d'} \Big(\sum_{\substack{k+\ell=i \\ k \in \{0,\dots,d\} \\ \ell \in \{0,\dots,d'\}}} a_k b_\ell \Big) X^k..$$
  Dans la somme précédente, le coefficient devant $X^{d+d'}$ est $a_d b_{d'}$ qui n'est pas nul. Donc
  $$\deg(P \times Q) = d + d' = \deg(P) + \deg(Q).$$

□

On en déduit la conséquence importante suivante :

Proposition 19.17 – Intégrité

Soient P et Q deux éléments de $\mathbb{K}[X]$. Alors

$$PQ = 0 \iff P = 0 \quad \text{ou} \quad Q = 0.$$

Démonstration. La réciproque est évidente, il suffit donc de vérifier le sens direct. On raisonne par contraposée : supposons que que $P \neq 0$ et $Q \neq 0$. Par passage au degré, on en déduit que $\deg(P) \geqslant 0$ et $\deg(Q) \geqslant 0$. Or $\deg(PQ) = \deg(P) + \deg(Q)$. Donc $\deg(PQ) \geqslant 0$. Donc $PQ) \neq 0$, d'où le résultat. □

Remarque 19.18 –

- Cette propriété d'intégrité est fausse dans l'espace des matrices, et est également fausse dans l'espace des fonctions...
- Ce résultat serait nettement plus difficile à prouver si on travaillait avec des fonctions polynomiales et non avec des polynômes. En effet, si $P(x)Q(x) = 0$ pour tout $x \in \mathbb{R}$, alors en tout point l'une des fonctions P et Q s'annule, mais qui nous dit que l'une des deux s'annule tout le temps ? Rien a priori.

4 – Fonctions polynomiales

Définition 19.19 –

1. On appelle **fonction polynomiale** sur $\mathbb{K}$ toute application f de $\mathbb{K}$ dans $\mathbb{K}$ telle qu'il existe un entier n et des éléments $a_0, \dots, a_n$ de $\mathbb{K}$ tels que
$$\forall x \in \mathbb{K}, f(x) = \sum_{i=0}^{n} a_i x^i.$$
2. Pour $P = \sum_{i=0}^{n} a_i X^i$, on appelle **fonction polynomiale associée** à P la fonction $\widetilde{P}$: $\begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \sum_{i=0}^{n} a_i x^i. \end{array}$
3. On dit qu'on **évalue** P en $x_0 \in \mathbb{K}$ lorsque l'on calcule $\widetilde{P}(x_0)$

Remarque 19.20 –

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

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

ATTENTION ! X **N'EST PAS UN NOMBRE!** On ne dit pas « Posons $X = 1$ », mais « Évaluons en 1 ».

5 – Méthode algorithmique de Hörner pour l'évaluation des polynômes

La méthode de Hörner est un algorithme permettant de calculer plus rapidement la valeur d'une fonction polynomiale en un point donné que la méthode naïve.

Par exemple, si f est la fonction, définie sur $\mathbb{R}$, $x \mapsto 10x^4 - 7x^3 + 5x^2 + 3x - 13$ et que l'on veut calculer à l'aide d'un programme python $f(a)$ où a est un réel, on peut utiliser le script suivant :

```
1 def f(x:float)->float:
2     valeur = 10*(x**4)-7*(x**3)+5*(x**2)+3*x-13
3     return valeur
4 a=3.1415
5 print(f(a))
```

Cela nécessite 10 multiplications et 4 additions/soustractions. En fait, en généralisant cette méthode à un polynôme quelconque, on arrive à une complexité en $\mathcal{O}(n^2)$ où n est le degré du polynôme.

Idée : La méthode de Hörner est basée sur un constat, si l'on réécrit la fonction f de la manière suivante :

$$f(a) = (((10 \times a - 7) \times a + 5) \times a + 3) \times a - 13.$$

Ici, il n'y a que 4 multiplications et 4 additions.

Méthode 19.21 –
On peut généraliser cette idée.
Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme réel de degré n et f la fonction polynomiale associée. Pour calculer $f(\alpha)$ où α est un réel quelconque, on effectue le calcul

$$(\ldots(((a_n \times \alpha + a_{n-1}) \times \alpha + a_{n-2}) \times \alpha + a_{n-3}) \times \ldots) \times \alpha + a_0,$$

qui ne nécessite que n additions et n multiplications.

Si l'on représente les polynômes en python par la liste (selon le degré décroissant) de leurs coefficients, on peut écrire le code suivant :

```
def Evaluation_Horner(P:list,a:float)->float:
    """ Entrée: P polynôme (liste des coefficients par deg décroissant), a float
    Sortie: Valeur de P(a)"""
    valeur = P[0]
    degre = len(P)-1
    for i in range(1,degre+1):
        valeur = a*valeur+P[i]
    return valeur
```

Remarque 19.22 – Bien sûr, tout ce qui a été fait ici avec une fonction polynomiale réelle se généralise à une fonction polynomiale complexe.

III – Dérivée d'un polynôme

1 – Définition et généralités

Définition 19.23 – Pour tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ où $n \in \mathbb{N}$, et $a_0, a_1, \ldots, a_n \in \mathbb{K}$, on définit son **polynôme dérivé** par

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

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

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

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

On peut évidemment itérer le processus de dérivation. Comme dans le cas des fonctions, on utilise alors les notations P'', P''' et $P^{(\ell)}$ pour désigner respectivement les dérivées seconde, troisième et ℓ-ième de P. On note aussi $P^{(0)}$ le polynôme P.

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

Proposition 19.24 – Degré du polynôme dérivé

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

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

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

Exemple 19.25 – $P = X^3 + X + 1$ $\quad P' = 3X^2 + 1$ $\quad P^{(2)} = 6X$ $\quad P^{(3)} = 6$ et $\forall \ell \geqslant 4,\ P^{(\ell)} = 0$.

Démonstration. Le premier point est évident avec la définition.

On suppose que P n'est pas nul.

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

- ▷ $\mathcal{H}_0$ est clairement vérifiée.
- ▷ Soit $\ell \in [\![0; \deg(P) - 1]\!]$. On suppose que la propriété $\mathcal{H}_\ell$ est vraie. Le polynôme $P^{(\ell)}$ a pour degré $\deg(P) - \ell \geqslant 1$ donc il n'est pas constant et l'on a
$$\deg(P^{(\ell+1)}) = \deg\left(\left(P^{\ell}\right)'\right) = \deg(P^{(\ell)}) - 1 = \deg(P) - (\ell + 1)$$
donc la propriété $\mathcal{H}_{\ell+1}$ est vraie.

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

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

Proposition 19.26 – Dérivées du polynôme X^n

Soit $n \in \mathbb{N}$. Pour tout $\ell \in [\![0; n]\!]$,
$$\begin{aligned}(X^n)^{(\ell)} &= \frac{n!}{(n-l)!} X^{n-\ell} \\ &= n(n-1)\dots(n-\ell+1)X^{n-\ell} \qquad \text{si } \ell \geqslant 1\end{aligned}$$
et pour tout $\ell \geqslant n+1$, $(X^n)^{(\ell)} = 0$.

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

- ▷ La propriété $\mathcal{P}_0$ est vraie (facile).
- ▷ Soit $\ell \in [\![0; \underline{n-1}]\!]$. On suppose que la propriété $\mathcal{P}_\ell$ est vraie. Alors
$$(X^n)^{(\ell+1)} = \left((X^n)^{(\ell)}\right)' = \left(\frac{n!}{(n-\ell)!} X^{n-\ell}\right)' = \frac{n!}{(n-\ell)!}(n-\ell)X^{n-(\ell+1)} = \frac{n!}{(n-(\ell+1))!} X^{n-(\ell+1)}$$
ce qui prouve que $\mathcal{P}_{\ell+1}$ est vraie.

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

Proposition 19.27 – Formule de Leibniz

Pour tous polynômes P et Q de $\mathbb{K}[X]$ et tout entier naturel n, on a
$$(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Même démonstration que celle qui a été faite dans le chapitre « Dérivabilité des fonctions d'une variable réelle ».

Proposition 19.28 – Dérivée d'un polnyôme composé

Pour tous polynômes P et Q de $\mathbb{K}[X]$, on a
$$(P \circ Q)' = Q' \times (P' \circ Q).$$

Corollaire 19.29 – Dérivées du polynôme $(X-\alpha)^n$

Soit $n \in \mathbb{N}$ et $\alpha \in \mathbb{K}$. Pour tout $\ell \in [\![0; n]\!]$,
$$((X-\alpha)^n)^{(\ell)} = \frac{n!}{(n-l)!}(X-\alpha)^{n-\ell}$$
et pour tout $\ell \geqslant n+1$, $((X-\alpha)^n)^{(\ell)} = 0$.

2 – Formule de Taylor

Théorème 19.30 – Théorème de Taylor

Soit $n \in \mathbb{N}$ et $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}_n[X]$ un polynôme de degré au plus n.

$$P = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(0)}{k!} X^k \quad \text{(Formule de Taylor en 0)}$$

$$P = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k \quad \text{(Formule de Taylor en } a \in \mathbb{K}\text{)}$$

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

$$P^{(\ell)} = \left(\sum_{k=0}^{n} a_k X^k\right)^{(\ell)} = \sum_{k=0}^{n} a_k \left(X^k\right)^{(\ell)} = \sum_{k=\ell}^{n} a_k \frac{k!}{(k-\ell)!} X^{k-\ell} \text{ car } \left(X^k\right)^{(\ell)} = \begin{cases} 0 & \text{si} \quad k < \ell \\ \dfrac{k!}{(k-\ell)!} X^{k-\ell} & \text{si} \quad k \geqslant \ell \end{cases}$$

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

$$= a_\ell \frac{\ell!}{(\ell-\ell)!} = a_\ell \, \ell!$$

$$\text{donc } a_\ell = \frac{\widetilde{P^{(\ell)}}(0)}{\ell!} \text{ et donc } P = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(0)}{k!} X^k.$$

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

$$Q = \sum_{k=0}^{n} \frac{\widetilde{Q^{(k)}}(0)}{k!} X^k = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} X^k \quad \text{or } P = Q(X-a) \text{ donc } P = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k. \qquad \square$$

Corollaire 19.31 – Expression des coefficients par les dérivées

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. Alors, on a : $\forall k \in [\![0, n]\!], \; a_k = \dfrac{\widetilde{P}^{(k)}(0)}{k!}$.

IV – Arithmétique des polynômes

1 – Diviseurs et multiples

Définition 19.32 – Soient A et B deux polynômes. On dit que A est un **diviseur** de B ou que A **divise** B ou encore que A est un **multiple** de B si et seulement si il existe un polynôme K tel que $B = KA$.
On note alors $A \mid B$.

Exemple 19.33 –

1. Pour tout $P \in \mathbb{K}[X]$, $P \mid 0$ et $1 \mid P$.
2. Si $0 \mid P$, alors $P = 0$
3. Pour tout $\lambda \in \mathbb{K}^*$, on a $\lambda \mid P$

Exemple 19.34 – $X - 1 \mid X^2 - 1$ car $X^2 - 1 = (X-1)(X+1)$
$2X^2 - 2 \mid X^2 - 1$ car $X^2 - 1 = \dfrac{1}{2}(2X^2 - 2)$

Exemple 19.35 – Soit $n \in \mathbb{N}^*$. Montrer que $X-1$ divise X^n-1.
On peut montrer la relation suivante :

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

En effet, développons le terme de droite, on obtient :

$$\begin{aligned}(X-1)\sum_{k=0}^{n-1} X^k &= \sum_{k=0}^{n-1}(X-1)X^k = \sum_{k=0}^{n-1}(X^{k+1}-X^k)\\ &= \sum_{k=0}^{n-1} X^{k+1} - \sum_{k=0}^{n-1} X^k \quad \text{par linéarité de la somme}\\ &= \sum_{i=1}^{n} X^i - \sum_{k=0}^{n-1} X^k \quad \text{en posant dans la 1ère somme } i = k+1\\ &= X^n + \sum_{i=1}^{n} X^i - - \sum_{k=1}^{n-1} X^k - X^0\\ &= X^n - 1.\end{aligned}$$

Remarquons que $\sum_{k=0}^{n-1} X^k \in \mathbb{K}[X]$, ainsi on a montré que $X^n-1 = (X-1)Q$ où $Q = \sum_{k=0}^{n-1} X^k$.
Autrement dit, $X-1$ divise X^n-1.

Rappel : Soient P et Q deux polynômes. $PQ = 1 \Longrightarrow \deg(P) = \deg(Q) = 0$
Autrement dit, les polynômes inversibles sont les polynômes constants non nuls.

Proposition 19.36

La relation de divisibilité est réflexive et transitive sur $\mathbb{K}[X]$, c'est même une relation d'ordre sur l'ensemble des polynômes UNITAIRES OU NULS de $\mathbb{K}[X]$. Soient $P, Q, R \in \mathbb{K}[X]$.

1. **Réflexivité :** $P \mid P$.
2. **Transitivité :** Si $P \mid Q$ et $Q \mid R$, alors $P \mid R$.
3. **Pseudo Anti-symétrie :** ($P \mid Q$ et $Q \mid P$) $\iff \exists k \in \mathbb{K}^*$ tel que $P = kQ$ On dit alors que P et Q sont **associés** (sur $\mathbb{K}$).

Démonstration.

1. $P = 1 \times P$
2. Si $P \mid Q$ et $Q \mid R$, alors il existe A, B des polynômes tels que $Q = AP$ et $R = BQ$, donc on a $R = ABP$ et $P \mid R$.
3. Si $P \mid Q$ et $Q \mid P$, alors il existe K_1 et K_2 dans $\mathbb{K}[X]$ tels que $Q = K_1P$ et $P = K_2Q$. Donc $Q = K_1K_2Q$.
   Si $Q = 0$, alors $P = K_2Q = 0$ et la propriété est vraie.
   Si $Q \neq 0$, alors $K_1K_2 = 1$ et donc K_1 et K_2 sont des polynômes constants non-nuls, donc il existe $k \in \mathbb{K}^*$ tel que $K_2 = k$ et $P = kQ$. Le sens réciproque est évident.

□

Proposition 19.37 – Combinaisons linéaires et produits

Soient P, Q, R, S, T cinq polynômes.

1. $T \mid R$ et $T \mid S \Longrightarrow T \mid PR + QS$.

2. Si $P \neq 0$ alors $R \mid S \iff RP \mid SP$.

Démonstration.

1. Si $T \mid R$ et $T \mid S$, alors $R = AT$ et $S = BT$ avec A et B des polynômes, donc $PR + QS = (PA + QB)T$.
2. $RP \mid SP \iff \exists K \in \mathbb{K}[X],\ SP = RPK \iff \exists K \in \mathbb{K}[X],\ S = RK$ (car P est non-nul) $\iff R \mid S$.

□

Proposition 19.38 – Divisibilité et degré

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

Démonstration. Si $P \mid Q$, alors il existe $K \in \mathbb{K}[X]$ tel que $PK = Q$. Donc $\deg(PK) = \deg(Q)$.
Donc $\deg(P) + \deg(K) = \deg(Q)$.
Comme Q est non-nul, K est non-nul donc $\deg(K) \geqslant 0$ et donc $\deg(P) \leqslant \deg(Q)$. □

2 – Division euclidienne de deux polynômes

Théorème 19.39 – Théorème de la division euclidienne pour les polynômes

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$.
Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = QB + R$ **ET** $\deg(R) < \deg(B)$.

Exemple 19.40 – On peut écrire la division euclidienne du polynôme $A = X^2 + X + 1$ par le polynôme $B = X$:

$$A = X^2 + X + 1 = X(X+1) + 1 = BQ + R$$

le quotient est donc $Q = X + 1$ et le reste $R = 1$ est de degré $0 < 1$.

Démonstration. **Existence :** Si B est constant égal à $\lambda \in \mathbb{K}^*$, on peut prendre $R = 0$ et $Q = \frac{1}{\lambda}A$. on suppose désormais que B n'est pas constant et donc $\deg(B) \geqslant 1$.

On va procéder par récurrence sur le degré de A. Pour tout $d \in \mathbb{N}$, on pose H_d : « Pour tout polynôme A de degré inférieur ou égal à d, alors il existe un couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = QB + R$ et $deg(R) < deg(B)$. »
Si $\deg(A) < \deg(B)$, on peut prendre $Q = 0$ et $R = A$. On a bien $\deg(R) = \deg(A) < \deg(B)$.
Soit $d \in \mathbb{N}$ fixé, $d \geqslant \deg(B) - 1$. On suppose que H_d est vraie.
Soit A de degré $d+1$. Alors, $A = \sum_{k=0}^{d+1} a_k X^k$ avec $a_{d+1} \neq 0$. On note également $B = \sum_{k=0}^{q} b_k X^k$ avec $b_q \neq 0$.
On définit $Q_1 = \frac{a_{d+1}}{b_q} X^{d+1-q}$. Alors, A et $-Q_1 B$ sont de même degré et de coefficients dominants opposés. Donc $A - Q_1 B$ est de degré inférieur ou égal à d. Par hypothèse de récurrence, il existe Q_2 et R des polynômes tels que

$$A - Q_1 B = Q_2 B + R, \qquad \deg(R) < \deg(B)$$

On a donc $A = (Q_1 + Q_2)B + R, \qquad \deg(R) < \deg(B)$.
Donc H_{d+1} est vraie.
Par récurrence, pour tout polynôme A, il est possible d'effectuer une division euclidienne par B.
Unicité : Supposons que (Q_1, R_1) et (Q_2, R_2) soient deux couples convenant : $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$, avec $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$. On trouve par soustraction : $B(Q_1 - Q_2) = R_2 - R_1$.
Par propriétés du degré, on obtient alors :

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

Or le degré est à valeurs dans $\mathbb{N} \cup \{-\infty\}$. Donc $\deg(Q_1 - Q_2) = -\infty$ et $Q_1 = Q_2$. Donc $R_1 = R_2$, ce qui termine la preuve de l'unicité. □

Proposition 19.41 – Divisibilité et division euclidienne

Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$.

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

où R est le reste de la division euclidienne de A par B.

Démonstration. Le sens réciproque est évident.
Pour le sens direct, on suppose que $B \mid A$, c'est-à-dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + 0$. Comme $\deg(0) < \deg(B)$, l'écriture obtenue est une division euclidienne de A par B. Or celle-ci est unique, donc le reste de la division euclidienne de A par B est 0. □

Méthode 19.42 –
On peut poser la division en faisant disparaître les monômes de plus haut degré successivement. Par exemple, considérons $A = X^4 + 3X^2 - 5X + 1$ et $B = X^2 - 3X$ et détaillons le calcul.

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

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

   On note $A_1 = 3X^3 + 3X^2 - 5X + 1$ le nouveau polynôme obtenu.

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

$$\begin{array}{rrrrr|l} X^4 & & +3X^2 & -5X & +1 & X^2-3X \\ \cline{6-6} -(X^4 & -3X^3) & & & & X^2+3X \\ \cline{1-4} & 3X^3 & +3X^2 & -5X & +1 & \\ & -(3X^3 & -9X^2) & & & \\ \cline{2-4} & & 12X^2 & -5X & +1 & \end{array}$$

   On note $A_2 = 12X^2 - 5X + 1$ le nouveau polynôme obtenu.

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

$$\begin{array}{rrrrr|l} X^4 & & +3X^2 & -5X & +1 & X^2-3X \\ \cline{6-6} -(X^4 & -3X^3) & & & & X^2+3X+12 \\ \cline{1-4} & 3X^3 & +3X^2 & -5X & +1 & \\ & -(3X^3 & -9X^2) & & & \\ \cline{2-4} & & 12X^2 & -5X & +1 & \\ & & -(12X^2 & -36X) & & \\ \cline{3-4} & & & 31X & +1 & \end{array}$$

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

Exemple 19.43 – Effectuons la division euclidienne de $X^3 + 3X - 2$ par $X^2 + X$.

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

Donc $X^3 + 3X^2 - 2 = (X^2 + X)(X + 2) - (2X + 2)$.

Exemple 19.44 – Effectuer la division euclidienne de $A = 2X^4 - 3X^2 + 5$ par $B = X^2 - 2X + 3$.

$$\begin{array}{rrrrrr|l} X^4 & & -3X^2 & & +5 & X^2-2X+3 \\ \cline{6-6} -(X^4 & -43X^3 & +6X^2) & & & 2X^2+4X-1 \\ \cline{1-4} & 4X^3 & -9X^2 & & +5 & \\ & -(4X^3 & -8X^2 & +12X) & & \\ \cline{2-4} & & -X^2 & -12X & +5 & \\ & & -(-X^2 & +2X & -3) & \\ \cline{3-5} & & & -14X & +8 & \end{array}$$

Donc $A = (2X^2 + 4X - 1)B - 14X + 8$.

V – Racines d'un polynôme

1 – Définition

Définition 19.45 – Soit $P \in \mathbb{K}[X]$. On dit que le réel α est une **racine** du polynôme P lorsque $\widetilde{P}(\alpha) = 0$.

Remarque 19.46 – Le polynôme nul a une infinité de racines (et c'est le seul dans ce cas !).

Exemple 19.47 –

- Soit le polynôme $P = (X-5)(2X+1)(8-2X)$.
  Les réels 5, $-\frac{1}{2}$ et 4 sont ses trois racines.
- Soit le polynôme $Q = X^3 - 2X + 1$.
  Q admet 1 pour racine **évidente**.
- Soit le polynôme $R = X^4 + 1$.
  Ce polynôme n'a pas de racine dans $\mathbb{R}$ car $\forall x \in \mathbb{R} \quad x^4 + 1 \geqslant 1 > 0$.

2 – Racines et divisibilité

Théorème 19.48

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Alors α est une racine de P ssi le polynôme $X - \alpha$ divise P. Autrement dit, ssi il existe un polynôme Q non nul tel que $P(X) = (X-\alpha)Q(X)$.

Démonstration. On montre cette équivalence par double implication.
($\Longleftarrow$) Si $(X-\alpha)$ divise P, il existe un polynôme Q tel que $P(X) = (X-\alpha)Q(X)$. Alors en évaluant les fonctions polynomiales associées en $x = \alpha$, on obtient : $\widetilde{P}(\alpha) = (\alpha - \alpha)\widetilde{Q}(\alpha) = 0$ d'où α est racine du polynôme de P.
($\Longrightarrow$) Supposons α racine de P. La division euclidienne de P par $(X-\alpha)$ donne l'existence d'un unique couple de polynômes (Q, R) tel que,

$$P(X) = Q(X)(X-\alpha) + R(X) \tag{19.1}$$

avec $R = 0$ ou $\deg(R) < \deg(x-\alpha) = 1$.
Donc R est un polynôme constant et s'écrit $R : x \mapsto c$. Il nous reste alors à montrer que $c = 0$.
Évaluons les fonctions polynomiales associées en $x = \alpha$ dans l'égalité 19.1. Cela donne $\widetilde{P}(\alpha) = 0 + c$ donc $c = 0$. □

Exemple 19.49 – 1 est racine de $X^n - 1$ et donc $X - 1$ divise $X^n - 1$.

Théorème 19.50

Soit $p \in \mathbb{N}^*$ et $\alpha_1, \ldots, \alpha_p$, p réels 2 à 2 distincts. Alors $\alpha_1, \ldots, \alpha_p$ sont p racines de P ssi le polynôme $(X-\alpha_1)(X-\alpha_2)\ldots\left(X-\alpha_p\right)$ divise P.

Démonstration. La réciproque est évidente, il suffit donc de montrer le sens direct.
On suppose que $r_1, r_2, \ldots r_p$ sont des racines de P, et on va montrer par récurrence que $(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_p)$ divise P.
Pour cela, on pose $\forall k \in [\![1, p]\!]$,

$$\mathcal{H}(k) : \quad \text{«}(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_k) \text{ divise } P\text{»}.$$

Initialisation ($k = 1$) Directement vérifiée en appliquant le Théorème 19.48. Ainsi $\mathcal{H}(1)$ est vraie.

Hérédité Soit $k \in [\![1, p-1]\!]$. On suppose que $\mathcal{H}(k)$ est vraie, montrons que $\mathcal{H}(k+1)$ est vraie.
$\mathcal{H}(k)$ étant vraie, il existe $A \in \mathbb{K}[x]$ tel que

$$P(X) = (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_k)A(X).$$

Comme $k+1 \leqslant p$, alors α_{k+1} est racine de P et $\widetilde{P}(\alpha_{k+1}) = 0$. Mais comme les r_i sont supposés distincts deux à deux $(\alpha_{k+1}-\alpha_1)(\alpha_{k+1}-\alpha_2)\ldots(\alpha_{k+1}-\alpha_k) \neq 0$. Donc nécessairement $\widetilde{A}(\alpha_{k+1}) = 0$ et α_{k+1} est racine de A. Par le Théorème 19.48, il existe alors $C \in \mathbb{K}[x]$ tel que $A(X) = (X-\alpha_{k+1})C(x)$. Donc

$$P(X) = (X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_k)(X-\alpha_{k+1})C(X).$$

Ce qui montre $\mathcal{H}(k+1)$.

Conclusion La propriété étant initialisée et héréditaire, d'après le principe de récurrence, $\forall k \in [\![1, p]\!]$, $\mathcal{H}(k)$ est vraie. En particulier $\mathcal{H}(p)$ est vraie, ce qui termine la preuve.

□

Proposition 19.51

Un polynôme de degré inférieur ou égal à n et qui possède au moins $n+1$ racines distinctes est le polynôme nul.

Remarque 19.52 –

- Par contraposée, tout polynôme non nul de degré n admet au plus n racines.
- En particulier, tout polynôme qui admet une infinité de racines est le polynôme nul.

Démonstration. Soit P un polynôme de degré inférieur ou égal à n. Si P admet $r_1, r_2, \dots, r_{n+1}$ comme racines distinctes, le corollaire précédent donne l'existence d'un polynôme Q tel que :

$$P(X) = (X - r_1)(X - r_2)\dots(X - r_{n+1})Q(X).$$

Par propriétés du degré, cela donne $\deg(P) = n + 1 + \deg(Q)$. Comme par hypothèse, $\deg(P) \leqslant n$, cela implique que $Q = 0$, et donc $P = 0$. □

3 – Ordre de multiplicité d'une racine

Définition 19.53 – Soit $P \in \mathbb{K}[x]$ et $\alpha \in \mathbb{K}$. On dit que α est une racine d'ordre de multiplicité $k \in \mathbb{N}^*$ de P si $\widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = \dots = \widetilde{P}^{(k-1)}(\alpha) = 0$ et $\widetilde{P}^{(k)}(\alpha) \neq 0$.

Remarque 19.54 –

- En particulier α est racine **simple** de P si $\widetilde{P}(\alpha) = 0$ et $\widetilde{P}'(\alpha) \neq 0$
- α est racine **double** de P si $\widetilde{P}(\alpha) = 0$, $\widetilde{P}'(\alpha) = 0$ et $\widetilde{P}''(\alpha) \neq 0$.
- L'ordre de multiplicité d'une racine est inférieure au degré du polynôme.

Exemple 19.55 – On considère $P(X) = X^4 - 2X^3 + 3X^2 - 4X + 2$. Est-ce que 1 est racine, et si oui avec quelle multiplicité ?
$\widetilde{P}(1) = 1 - 2 + 3 - 4 + 2 = 0$, donc 1 est racine. On calcule la dérivée :

$$\widetilde{P}'(x) = 4x^3 - 6x^2 + 6x - 4.$$

$\widetilde{P}'(1) = 4 - 6 + 6 - 4 = 0$, donc 1 est racine d'ordre au moins 2. On calcule la dérivée seconde :

$$\widetilde{P}''(x) = 12x^2 - 12x + 6.$$

$\widetilde{P}''(1) = 12 - 12 + 6 = 6 \neq 0$. Donc 1 est racine d'ordre 2 de P.

Théorème 19.56

Soit $P \in \mathbb{K}[x]$, $\alpha \in \mathbb{K}$, et $k \in \mathbb{N}^*$.
Alors α est racine d'ordre k de P ssi il existe $Q \in \mathbb{K}[X]$ tel que :

$$P(X) = (X - \alpha)^k Q(X)$$

avec $\widetilde{Q}(\alpha) \neq 0$. Autrement dit ssi $(X - \alpha)^k$ divise P, mais $(X - \alpha)^{k+1}$ ne divise plus P.

Remarque 19.57 – En particulier, α est racine **double** si $(X - \alpha)^2$ divise P mais que $(X - \alpha)^3$ ne divise pas P.

Démonstration. Montrons l'équivalence par double inclusion.
($\Longrightarrow$) Supposons que $\alpha \in \mathbb{K}$ soit une racine d'ordre k de P i.e.

$$\widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = \dots = \widetilde{P}^{(k-1)}(\alpha) = 0 \text{ Et } \widetilde{P}^{(k)}(\alpha) \neq 0,$$

alors en utilisant la formule de Taylor pour P, on obtient (avec n le degré de P) :

$$P(X)=\sum_{j=0}^{n}\frac{\widetilde{P}^{(j)}(\alpha)}{j!}(X-\alpha)^j=\sum_{j=k}^{n}\frac{\widetilde{P}^{(j)}(\alpha)}{j!}(X-\alpha)^j=(X-\alpha)^k\left[\sum_{j=k}^{n}\frac{\widetilde{P}^{(j)}(\alpha)}{j!}(X-\alpha)^{j-k}\right]=(X-\alpha)^kQ(X)$$

en posant $Q(X)=\sum_{j=k}^{n}\frac{\widetilde{P}^{(j)}(\alpha)}{j!}(X-\alpha)^{j-k}\in\mathbb{K}[X]$. Il reste alors à vérifier que $\widetilde{Q}(\alpha)=\frac{\widetilde{P}^{(k)}(\alpha)}{k!}+0\neq 0$ pour conclure.

($\Longleftarrow$) Soit P un polynôme. Montrons le résultat par récurrence.

Soit $k\in\mathbb{N}^*$, on pose la propriété $\mathcal{H}(k)$: « si il existe $Q\in\mathbb{K}[X]$ tel que, $P(X)=(X-\alpha)^kQ(X)$ avec $Q(\alpha)\neq 0$ alors $\widetilde{P}(\alpha)=\widetilde{P}'(\alpha)=\ldots=\widetilde{P}^{(k-1)}(\alpha)=0$ et $\widetilde{P}^{(k)}(\alpha)\neq 0$ ».

Intialisation ($k=1$) Si il existe $Q\in\mathbb{K}[X]$ tel que, $P(X)=(X-\alpha)Q(X)$ avec $\widetilde{Q}(\alpha)\neq 0$, alors $\widetilde{P}(\alpha)=0$. De plus, $P'(X)=Q(X)+(X-\alpha)Q'(X)$ donc $\widetilde{P}'(\alpha)=\widetilde{Q}(\alpha)+0\neq 0$.
Ainsi $\mathcal{H}(1)$ est vraie et la propriété est initialisée.

Hérédité Soit $k\in\mathbb{N}^*$. Supposons maintenant que la propriété $\mathcal{H}(k)$ est vraie, et montrons la propriété que la propriété $\mathcal{H}(k)$ est vraie.
On part donc de l'existence de $Q\in\mathbb{K}[X]$ tel que, $P(X)=(X-\alpha)^{k+1}Q(X)$ avec $\widetilde{Q}(\alpha)\neq 0$. L'astuce ici est d'appliquer l'hypothèse de récurrence au polynôme P'.
On a alors,

$$P'(X)=(k+1)(X-\alpha)^kQ(X)+(X-\alpha)^{k+1}Q'(X)=(X-\alpha)^k\hat{Q}(X)$$

où l'on a posé $\hat{Q}(X)=(k+1)Q(X)+(X-\alpha)Q'(X)$.
Comme $\widetilde{\hat{Q}}(\alpha)=(k+1)\widetilde{Q}(\alpha)+0\neq 0$, on peut appliquer l'hypothèse de récurrence à P'.
On en déduit donc que $\widetilde{P}'(\alpha)=0=\left(\widetilde{P}'\right)'(\alpha)=\ldots=\left(\widetilde{P}'\right)^{(k-1)}(\alpha)$ et $\left(\widetilde{P}'\right)^{(k)}(\alpha)\neq 0$. C'est-à-dire $\widetilde{P}'(\alpha)=0=\widetilde{P}''(\alpha)=\ldots=\widetilde{P}^{(k)}(\alpha)$ et $\widetilde{P}^{(k+1)}(\alpha)\neq 0$.
Comme de plus, $\widetilde{P}(\alpha)=0$, on en déduit le résultat voulu, $\mathcal{H}(k+1)$ est vraie et la propriété est héréditaire.

Conclusion La propriété étant initialisée et héréditaire, d'après le principe de récurrence, $\mathcal{H}(k)$ est vraie pour tout $k\in\mathbb{N}^*$.

□

4 – Nombre de racines d'un polynôme

Théorème 19.58 – Factorisation «par les racines»

Soient $P\in\mathbb{K}[X]$ **NON NUL** et $\lambda_1,\ldots,\lambda_r$ des racines distinctes de P de multiplicités respectives $m_1,\ldots,m_r$. Alors $(X-\lambda_1)^{m_1}\ldots(X-\lambda_r)^{m_r}$ divise P. En particulier $m_1+\ldots+m_r\leqslant\deg(P)$.

Démonstration. Montrons par récurrence que pour tout $k\in[\![1,r]\!]$, $(X-\lambda_1)^{m_1}\ldots(X-\lambda_k)^{m_k}$ divise P.

Initialisation : λ_1 est racine de P de multiplicité m_1, donc $(X-\lambda_1)^{m_1}$ divise P.

Hérédité : Soit $k\in[\![1,r-1]\!]$. Faisons l'hypothèse que $(X-\lambda_1)^{m_1}\ldots(X-\lambda_k)^{m_k}$ divise P.

- Dans ces conditions : $P=(X-\lambda_1)^{m_1}\ldots(X-\lambda_k)^{m_k}A$ pour un certain $A\in\mathbb{K}[X]$.
- En notant α la multiplicité de λ_{k+1} dans A : $A=(X-\lambda_{k+1})^{\alpha}B$ pour un certain $B\in\mathbb{K}[X]$ avec $B(\lambda_{k+1})\neq 0$. En outre, $(X-\lambda_{k+1})^{\alpha}$ divise A, donc P, donc $\alpha\leqslant m_{k+1}$.
- Enfin : $P=(X-\lambda_{k+1})^{m_{k+1}}C$ pour un certain $C\in\mathbb{K}[X]$ avec $C(\lambda_{k+1})\neq 0$.

Il découle de ces trois points que : $(X-\lambda_1)^{m_1}\ldots(X-\lambda_k)^{m_k}(X-\lambda_{k+1})^{\alpha}B=(X-\lambda_{k+1})^{m_{k+1}}C$. Divisons cette égalité par $(X-\lambda_{k+1})^{\alpha}$ grâce à l'intégrité de $\mathbb{K}[X]$: $(X-\lambda_1)^{m_1}\ldots(X-\lambda_k)^{m_k}B=(X-\lambda_{k+1})^{m_{k+1}-\alpha}C$. Le polynôme de gauche n'admet pas λ_{k+1} pour racine, donc celui de droite non plus, donc $\alpha=m_{k+1}$.
Conclusion : $(X-\lambda_{k+1})^{m_{k+1}}$ divise A, donc $(X-\lambda_1)^{m_1}\ldots(X-\lambda_{k+1})^{m_{k+1}}$ divise P.

□

Exemple 19.59 – Le polynôme $(X-1)^4X^2(X+2)$ possède en tout trois racines distinctes : 1 de multiplicité 4,0 double et -2 simple. On dit en revanche qu'il possède $\boxed{7}$ **RACINES COMPTÉES AVEC MULTIPLICITÉ** , car $7=4+2+1$.

Exemple 19.60 – Soit $P=2X^4-7X^3+6X^2+X-2$. Calculer $P(1)$, $P'(1)$, $P(2)$ et $P(\frac{-1}{2})$ et en déduire une factorisation de P.
$P(1)=P(2)=P(\frac{-1}{2})=0$.

$P' = 8X^3 - 21X^2 + 12X + 1$ et $P'(1) = 0$.
On en déduit que 1 est racine de multiplicité au moins 2 de P et que 2 et $\frac{-1}{2}$ sont racines de multiplicité au moins 1. Cela fait au minimum une somme de multiplicités de 4. Or, P est de degré 4, donc il ne peut pas avoir d'autres racines et les multiplicités de 1 et 2 et $\frac{-1}{2}$ ne peuvent pas dépasser respectivement 2, 1 et 1. Enfin, le coefficient dominant de P est 2, donc

$$P = 2(X-1)^2(X-2)(X+\frac{1}{2}).$$

Théorème 19.61 – Nombre maximal de racines comptées avec multiplicité

- Un polynôme **NON NUL** P possède au plus $\deg(P)$ racines **COMPTÉES AVEC MULTIPLICITÉ.**
- En particulier, seul le polynôme nul possède une infinité de racines.

ATTENTION ! En dépit des apparences, ce théorème est l'un des plus importants du chapitre !

Un polynôme de degré n ne possède pas forcément n racines comptées avec multiplicité. Nous verrons au prochain paragraphe que c'est le cas si $\mathbb{K} = \mathbb{C}$, mais pas si $\mathbb{K} = \mathbb{R}$. Par exemple, $X^2 + 1$ est réel de degré 2 mais n'a pas de racine réelle.

Exemple 19.62 – Soit $P \in \mathbb{R}[X]$. On suppose que $P(n) = n^3 - n^2 + 1$ pour tout $n \in \mathbb{N}$. Alors $P = X^3 - X^2 + 1$, donc en fait $P(z) = z^3 - z^2 + 1$ pour tout $z \in \mathbb{C}$!

Démonstration. On connait ici P **SEULEMENT** en les entiers naturels et cela ne nous permet pas a priori d'affirmer que $P = X^3 - X^2 + 1$, ni que $P(z) = z^3 - z^2 + 1$ pour tout $z \in \mathbb{C}$. Il est pourtant facile d'obtenir ces résultats grâce à la notion de racine. En effet, le polynôme $P - X^3 + X^2 - 1$ admet par hypothèse tout entier naturel pour racine, donc possède une infinité de racines, donc est nul. Comme voulu $P = X^3 - X^2 + 1$. □

Exemple 19.63 – Soit $P \in \mathbb{R}[X]$. On suppose que P est de degré n entier et que $P(k) = \frac{1}{k}$ pour tout $k \in [\![1, n+1]\!]$.
Dans ces conditions : $P(-1) = n+1$.

Démonstration.

- **Analyse des hypothèses :** Le polynôme $XP(X)-1$ admet $1, 2, \dots, n+1$ pour racines, soit déjà $n+1$ racines distinctes, or il est justement de degré $n+1$, donc $XP(X) - 1 = \lambda \prod_{k=1}^{n+1}(X-k)$ pour un certain $\lambda \in \mathbb{R}^*$.
  Évaluons en 0 : $-1 = \lambda \prod_{k=1}^{n+1}(-k)$, i.e. $\lambda = \frac{(-1)^n}{(n+1)!}$.
  Enfin : $XP(X) = 1 + \frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(X-k)$.
- **Calcul de** $P(-1)$: Évaluons simplement ce résultat en -1 :

$$-P(-1) = 1 + \frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(-(k+1)) = 1 + \frac{(-1)^n}{(n+1)!} \times (-1)^{n+1}(n+2)! = 1 - (n+2), \quad \text{donc } P(-1) = n+1$$

□

Corollaire 19.64 – Identification polynôme/fonction polynomiale

Pour tous $P, Q \in \mathbb{K}[X]$, si les fonctions polynomiales $\widetilde{P}$ et $\widetilde{Q}$ sont égales, alors les polynômes P et Q le sont aussi. Autrement dit, les coefficients de P et Q sont égaux.

Démonstration. Il s'agit de montrer que l'application $\Phi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{FP}(\mathbb{K}) \\ P & \mapsto & \widetilde{P} \end{array}$ est bijective, ou $\mathcal{FP}(\mathbb{K})$ est l'ensemble des fonctions polynomiales de $\mathbb{K}$ dans $\mathbb{K}$.

Φ est facilement surjective : L'antécédent d'une fonction $x \mapsto \sum_{k=0}^{n} a_k x^k$ est le polynôme $\sum_{k=0}^{n} a_k X^k$.

Soient P_1 et P_2 deux polynômes tels que $\Phi(P_1) = \Phi(P_2)$. Alors, $x \mapsto \widetilde{P_1}(x) - \widetilde{P_2}(x)$ est la fonction nulle, ce qui signifie que $P_1 - P_2$ a une infinité de racines, donc est le polynôme nul. D'où $P_1 = P_2$.

Ainsi, Φ est injective. □

Définition 19.65 – Soit $P \in \mathbb{K}[X]$ non nul. On dit que P est **scindé** si et seulement si

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

Proposition 19.66 – Nombre de racines d'un pôlynôme scindé

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

VI – Polynômes scindés et factorisation dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

1 – Polynôme scindé

Définition 19.67 (Polynôme scindé) – Soit $P \in \mathbb{K}[X]$. On dit que P est scindé (sur $\mathbb{K}$) s'il **N** 'est **PAS** constant, et possède exactement $\deg(P)$ racines (dans $\mathbb{K}$) comptées avec multiplicité.

Dire que P est scindé sur $\mathbb{K}$ revient donc à dire que P est de la forme $P = A \prod_{k=1}^{r} (X - \lambda_k)^{m_k}$, où $\lambda_1, ..., \lambda_r$ sont les racines distinctes de P dans $\mathbb{K}$, de multiplicités respectives $m_1, ..., m_r$, et où A est son coefficient dominant.

ATTENTION ! La précision «scindé **SUR** $\mathbb{K}$ » n'est pas superflue, car un polynôme peut avoir des racines complexes mais aucune réelle. Le polynôme $X^2 + 1 = (X + i)(X - i)$ est ainsi scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

Exemple 19.68 – Le polynôme $X^3 + 27$ est scindé sur $\mathbb{C}$ et sa forme scindée vaut : $X^3 + 27 = (x-3)\left(x - 3\,e^{\frac{i\pi}{3}}\right)\left(x - 3\,e^{-\frac{i\pi}{3}}\right)$.

Exemple 19.69 – Pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$: $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$.

Démonstration. Le polynôme $X^n - 1$ n'est pas constant et admet les n nombres $e^{\frac{2ik\pi}{n}}$ pour racines distinctes, k décrivant $[\![0, n-1]\!]$. Comme il possède au plus n racines comptées avec multiplicité, il en possède forcément exactement n, donc est scindé sur $\mathbb{C}$. □

2 – Factorisation dans $\mathbb{C}[X]$

Tout polynôme possède-t-il une racine? Question essentielle s'il en est, mais à laquelle nous n'avons encore jamais répondu. La réponse affirmative suivante est un théorème majeur des mathématiques, appelé parfois « théorème fondamental de l'algèbre ».

Théorème 19.70 – Théorème de D'Alembert-Gauss

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

Démonstration. ADMIS. (Difficile) □

ATTENTION ! Le théorème est faux sur $\mathbb{R}$ - un polynôme non constant de $\mathbb{R}[X]$ peut ne pas avoir de racine **RÉELLE** , par exemple le polynôme $X^2 + 1$.

Remarque 19.71 – Ainsi, l'équation $z^6+z^4+1=0$ admet au moins une solutions dans $\mathbb{C}$. Cependant, le théorème ne fournit aucun procédé pour l'obtenir et en fait, personne n'est capable d'en déterminer une valeur exacte !

Au degré 2, on dispose d'une méthode de résolution systématique (à l'aide du discriminant).

Aux degrés 3 et 4, d'autres techniques existent également : les méthodes (respectivement) de Cardan et de Ferrari.

A partir du degré 5, il a été démontré (par Abel et par Galois) qu'il est impossible d'obtenir de telles méthodes de résolutions exactes.

Corollaire 19.72 – Nombre de racines d'un polynôme complexe

Soit $P\in\mathbb{C}[X]$ de degré $n\geqslant 1$ (non constant).

P possède n racines comptées avec leur multiplicité. Autrement dit, P est scindé.

Démonstration. Pour tout $k\in\mathbb{N}^*$, on note H_k la propriété : « P a au moins k racines ».

Initialisation : H_1 est vraie d'après le théorème de D'Alembert-Gauss.

Hérédité : Soit $k\in[\![1,n-1]\!]$. On suppose que H_k est vraie.

P possède au moins k racines, notées $\alpha_1,...,\alpha_k\in\mathbb{C}$.

On sait que $\prod_{j=1}^{k}(X-\alpha_j)\mid P$ donc il existe $Q\in\mathbb{C}[X]$ tel que $P=\prod_{j=1}^{k}(X-\alpha_j)\times Q$.

Donc $n=\deg(P)=\deg(\prod_{j=1}^{k}(X-\alpha_j))+\deg(Q)$ donc $\deg(Q)=n-k\geqslant 1$.

Ainsi, d'après le théorème de D'Alembert-Gauss, Q possède une racine complexe notée α_{k+1}. Il est évident que α_{k+1} est également une racine de P donc P possède au moins $k+1$ racines donc H_{k+1} est vraie.

Ccl. Pour tout $k\in[\![1,n]\!]$, H_k est vraie donc en particulier H_n.

P a donc au moins n racines, or il est de degré n donc P a exactement n racines. □

Théorème 19.73 – Décomposition dans $\mathbb{C}[X]$

Soit $P\in\mathbb{C}[X]$ non-constant. P se décompose de manière unique à l'ordre près des facteurs sous la forme

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

avec

- λ le coefficient dominant de P et r un entier.
- $\alpha_1,...,\alpha_r$ les racines de P de multiplicités respectives $m_1,...,m_r$.

3 – Factorisation dans $\mathbb{R}[X]$

Corollaire 19.74 – Nombre maximal de racines d'un polynôme réel

Soit $P\in\mathbb{R}[X]$ de degré $n\geqslant 1$ (non constant).

P possède **au maximum** n racines (réelles ou complexes) comptées avec leur multiplicité.

Proposition 19.75 – Racines complexes de polynômes réels

Soient $P\in\mathbb{R}[X]$, $\alpha\in\mathbb{C}$ et $m\in\mathbb{N}^*$.

Si α est une racine de multiplicité m de P, alors $\overline{\alpha}$ est une racine de multiplicité m de P.

Démonstration. Soit $Q\in\mathbb{R}[X]$ et $z\in\mathbb{C}$. On a $\widetilde{Q}(\overline{z})=\overline{\widetilde{Q}(z)}$.

En effet, $Q=\sum_{k=0}^{n}a_kX^k$ donc $\overline{\widetilde{Q}(z)}=\overline{\sum_{k=0}^{n}a_kz^k}=\sum_{k=0}^{n}\overline{a_k}\,\overline{z}^k=\sum_{k=0}^{n}a_k\overline{z}^k=\widetilde{Q}(\overline{z})$.

On suppose que α est une racine de P de multiplicité m donc

$$\begin{cases}\widetilde{P}(\alpha)=\widetilde{P}'(\alpha)=...=\widetilde{P}^{(m-1)}(\alpha)=0\\ \widetilde{P}^{(m)}(\alpha)\neq 0\end{cases}\quad\text{donc}\quad\begin{cases}\overline{\widetilde{P}(\alpha)}=\overline{\widetilde{P}'(\alpha)}=...=\overline{\widetilde{P}^{(m-1)}(\alpha)}=0\\ \overline{\widetilde{P}^{(m)}(\alpha)}\neq 0\end{cases}$$

donc $\begin{cases} \widetilde{P}(\alpha) = \widetilde{P}'(\alpha) = \ldots = \widetilde{P}^{(m-1)}(\alpha) = 0 \\ \widetilde{P}^{(m)}(\alpha) \neq 0 \end{cases}$ donc $\overline{\alpha}$ est une racine de multiplicité m de P. □

Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. On a également $P \in \mathbb{C}[X]$ donc on peut décomposer P dans $\mathbb{C}[X]$.

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

avec λ le coefficient dominant de P et $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ les racines de P de multiplicités respectives $m_1, \ldots, m_r \in \mathbb{N}^*$.

On numérote les racines de telle sorte que $\alpha_1, \ldots, \alpha_s \in \mathbb{R}$ et $\alpha_{s+1}, \ldots, \alpha_r \in \mathbb{C} \setminus \mathbb{R}$. De plus, d'après la proposition précédente, les racines non-réelles vont « par paire » avec leur conjugué. On numérote donc les racines non-réelles de telle sorte que $(\alpha_{s+1}, \ldots, \alpha_r) = (\alpha_{s+1}, \ldots, \alpha_t, \overline{\alpha_{s+1}}, \ldots \overline{\alpha_t})$. Ainsi,

$$\begin{aligned} P &= \lambda \prod_{k=1}^{s} (X - \alpha_k)^{m_k} \times \prod_{j=s+1}^{t} (X - \alpha_j)^{m_j} (X - \overline{\alpha_j})^{m_j} \\ &= \lambda \prod_{k=1}^{s} (X - \alpha_k)^{m_k} \times \prod_{j=s+1}^{t} \left(X^2 - 2\mathrm{Re}(\alpha_j) X + |\alpha_j|^2\right)^{m_j} \end{aligned}$$

On en déduit donc le résultat suivant :

Théorème 19.76 – Décomposition dans $\mathbb{R}[X]$

Tout polynôme de $\mathbb{R}[X]$ peut s'écrire comme produit d'un réel, de polynômes de degré 1 et de polynômes de degré 2 n'ayant pas de racine réelle.
Autrement dit, tout polynôme $P \in \mathbb{R}[x]$ peut se décomposer sous la forme suivante :

$$P(X) = a_n \prod_{i=1}^{k} (X - \alpha_i)^{r_i} \prod_{j=1}^{l} (X^2 + b_j X + c_j)$$

où

- a_n est le coefficient dominant de P ;
- les α_i sont les racines réelles de P, de multiplicités respectives $r_i \in \mathbb{N}^*$;
- les trinômes $X^2 + b_j X + c_j$ sont de discriminant strictement négatif.

Exemple 19.77 – Décomposer $P = X^4 - 2X^3 + 5X^2 - 8X + 4$ dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.
On remarque que $\widetilde{P}(1) = 0$ donc 1 est une racine de P.
$P' = 4X^3 - 6X^2 + 4X - 2$
$\widetilde{P}'(1) = 4 - 6 + 4 - 2 = 0$ donc 1 est une racine au moins double de P.
Ainsi, il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-1)^2 Q$.
Après une division euclidienne, on a $P = (X-1)^2(X^2+4)$.
$X^2 + 4$ est un polynôme de second degré et ne possède pas de racines réelles donc il s'agit de la décomposition de P dans $\mathbb{R}[X]$.
La décomposition dans $\mathbb{C}[X]$ est $P = (X-1)^2(X-2i)(X+2i)$.

4 – Polynômes irréductibles

Définition 19.78 – Soit $P \in \mathbb{K}[X]$. On dit que P est **irréductible** s'il est de degré supérieur ou égal à 1 et les seuls diviseurs de P sont les polynômes constants non nuls et les polynômes de la forme λP avec $\lambda \in \mathbb{K}^*$.

Il faut penser aux polynômes irréductibles comme les analogues des nombres premiers dans le monde des polynômes. Ce sont les éléments « de base », c'est-à-dire indécomposables (sauf de façon triviale) dont sont constitués les autres polynômes.

Proposition 19.79 – Polynômes irréductibles dans $\mathbb{R}$ et $\mathbb{C}$

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

Démonstration.

1. Soit $P \in \mathbb{K}[X]$ et $\deg(P) = 1$: Si $P = QR$ avec Q et R des polynômes, alors, en observant les degrés, on voit que l'un des deux polynômes Q et R est constant. Ainsi, les polynômes de degré 1 sont irréductibles.
2. Dans $\mathbb{C}[X]$, le théorème de décomposition assure que tout polynôme de degré supérieur ou égal à 2 est divisible par un polynôme de degré 1, donc n'est pas irréductible.
3. Dans $\mathbb{R}[X]$, le théorème de décomposition assure que tout polynôme de degré supérieur ou égal à 2 est divisible par un polynôme de degré 1 ou 2, donc n'est pas irréductible. De même un polynôme réel de degré 2 ayant deux racines réelles se factorise comme produit de facteurs de degré 1, donc n'est pas irréductible.
4. Si P est un polynôme réel de degré 2 sans racine réelle : Supposons que $P = AB$ où ni A ni B ne sont des polynômes constants : Alors, ce sont des polynômes de degré 1, qui admettent donc une racine réelle, ce qui est absurde. Donc P est irréductible.

□

On peut alors rassembler les résultats obtenus dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$ en le théorème suivant :

Théorème 19.80 – Décomposition dans $\mathbb{K}[X]$

Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique à l'ordre près des facteurs en produit de polynômes irréductibles de $\mathbb{K}[X]$.

Ce théorème est l'équivalent de l'existence et de l'unicité de la décomposition de tout nombre entier en produit de nombres premiers.

VII – Relations coefficients-racines

Le prochain théorème est rebutant au premier abord, commençons par deux cas simples. On travaille ci-dessous avec des polynômes non constants de $\mathbb{C}[X]$, donc avec des polynômes scindés sur $\mathbb{C}$ d'après le théorème de d'Alembert-Gauss.

- **Polynômes de degré 2 :** Soit $P = a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$ de racines λ_1 et λ_2 comptées avec multiplicité. Alors : $P = a_2(X-\lambda_1)(X-\lambda_2) = a_2X^2 - a_2(\lambda_1+\lambda_2)X + a_2\lambda_1\lambda_2$, donc après identification : $\lambda_1+\lambda_2 = -\dfrac{a_1}{a_2}$ (somme des racines) et $\lambda_1\lambda_2 = \dfrac{a_0}{a_2}$ (produit des racines).
- **Polynômes de degré 3 :** Soit $P = a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$ de racines $\lambda_1, \lambda_2, \lambda_3$ comptées avec multiplicité. Alors : $P = a_3(X-\lambda_1)(X-\lambda_2)(X-\lambda_3) = a_3X^3 - a_3(\lambda_1+\lambda_2+\lambda_3)X^2 + a_3(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3)X - a_3\lambda_1\lambda_2\lambda_3$, donc après identification : $\lambda_1+\lambda_2+\lambda_3 = -\dfrac{a_2}{a_3}$ (somme des racines), $\lambda_1\lambda_2\lambda_3 = -\dfrac{a_0}{a_3}$ (produit des racines) et $\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3 = \dfrac{a_1}{a_3}$.

Théorème 19.81 – Relations coefficients-racines

Soit $P = \sum_{k=0}^{n} a_kX^K \in \mathbb{C}[X]$ de degré $n \in \mathbb{N}^*$. On note $\lambda_1, \dots, \lambda_n$ les racines de P comptées avec multiplicité.

Pour tout $k \in [\![1, n]\!]$, si on pose $\sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \lambda_{i_1} \dots \lambda_{i_k}$, alors $\sigma_k = (-1)^k \dfrac{a_{n-k}}{a_n}$.

Autre manière de dire les choses : $P = a_n \prod_{i=1}^{n} (X-\lambda_i) = a_n\left(X^n - \sigma_1X^{n-1} + \sigma_2X^{n-2} - \sigma_3X^{n-3} + \dots + (-1)^n\sigma_n\right)$.

Ce théorème ne nous permet pas de calculer les racines de P à partir de ses coefficients - ce serait trop beau - mais il nous permet de le faire pour certaines fonctions $\sigma_1, \dots, \sigma_n$ des racines, appelées les fonctions symétriques élémentaires de $\lambda_1, \dots, \lambda_n$ - symétriques parce qu'elles ne dépendent pas de l'ordre dans lequel on a rangé $\lambda_1, \dots, \lambda_n$. Deux d'entre elles sont plus simples et plus utilisées que les autres :

$$\sigma_1 = \sum_{k=1}^{n} \lambda_k \quad \text{(somme des racines)} \quad \text{et} \quad \sigma_n = \prod_{k=1}^{n} \lambda_k \quad \text{(produit des racines).}$$

Pour que tout soit bien clair, détaillons $\sigma_1,\sigma_2,\sigma_3$ et σ_4 dans le cas où $n=4$: $\sigma_1=\lambda_1+\lambda_2+\lambda_3+\lambda_4$,

$$\sigma_2=\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_1\lambda_4+\lambda_2\lambda_3+\lambda_2\lambda_4+\lambda_3\lambda_4,\quad \sigma_3=\lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_4+\lambda_1\lambda_3\lambda_4+\lambda_2\lambda_3\lambda_4 \quad\text{et}\quad \sigma_4=\lambda_1\lambda_2\lambda_3\lambda_4.$$

Exemple 19.82 – Pour tout $n\geqslant 2$: $\displaystyle\sum_{k=0}^{n-1}\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}=\sum_{\omega\in\mathrm{U}_n}\omega=0$ et $\displaystyle\prod_{k=0}^{n-1}\mathrm{e}^{2\mathrm{i}k\pi}=\prod_{\omega\in\mathrm{U}_n}\omega=(-1)^{n+1}$.

Démonstration. Dans le contexte du polynôme scindé X^n-1 : $\sigma_1=\displaystyle\sum_{\omega\in\mathrm{U}_n}\omega$ et $\sigma_n=\prod_{\omega\in\mathrm{U}_n}\omega$.

Comme le coefficient de degré $n-1$ de X^n-1 vaut 0 : $\sigma_1=(-1)^1\dfrac{0}{1}=0$, et comme son coefficient de degré 0 vaut -1 : $\sigma_n=(-1)^n\dfrac{-1}{1}=(-1)^{n+1}$. □

Exemple 19.83 – Le polynôme non constant X^3-2X+5 est scindé sur $\mathbb{C}$ d'après le théorème de d'Alembert-Gauss - mais pas forcément sur $\mathbb{R}$ - et nous pouvons noter x,y et z ses trois racines complexes comptées avec multiplicité. L'unique polynôme unitaire de degré 3 dont les racines sont x^2,y^2 et z^2 est alors le polynôme $X^3-4X^2+4X-25$. Remarquez bien qu'on arrive au résultat sans jamais avoir eu la moindre idée de ce que valent x,y et z!

Démonstration. Nous devons calculer explicitement les coefficients du polynôme $\left(X-x^2\right)\left(X-y^2\right)\left(X-z^2\right)$:

$$\left(X-x^2\right)\left(X-y^2\right)\left(X-z^2\right)=X^3-\left(x^2+y^2+z^2\right)X^2+\left(x^2y^2+y^2z^2+z^2x^2\right)X-x^2y^2z^2.$$

Posons : $\sigma_1=x+y+z$, $\sigma_2=xy+yz+zx$ et $\sigma_3=xyz$. Les relations coefficients-racines du polynôme X^3-2X+5 s'écrivent : $\sigma_1=0,\sigma_2=-2$ et $\sigma_3=-5$.
Or : $x^2+y^2+z^2=(x+y+z)^2-2(xy+yz+zx)=\sigma_1^2-2\sigma_2=4$, $x^2y^2z^2=(xyz)^2=\sigma_3^2=25$
et $x^2y^2+y^2z^2+z^2x^2=(xy+yz+zx)^2-2(xy\times yz+yz\times zx+zx\times xy)=\sigma_2^2-2xyz(x+y+z)=\sigma_2^2-2\sigma_1\sigma_3=4$.
Comme annoncé : $\left(X-x^2\right)\left(X-y^2\right)\left(X-z^2\right)=X^3-4X^2+4X-25$. □

VIII – Polynômes d'interpolation de Lagrange

Étant donnés des points $x_1,\dots,x_n\in\mathbb{R}$ pour lesquels $x_1<\dots<x_n$ et des réels $y_1,\dots,y_n\in\mathbb{R}$ quelconques, le problème de l'interpolation consiste à construire des fonctions $f:[x_1,x_n]\longrightarrow\mathbb{R}$ pour lesquelles $f(x_i)=y_i$ pour tout $i\in[\![1,n]\!]$. Il existe bien sûr beaucoup de telles fonctions f, on peut par exemple en construire une en reliant linéairement les points de coordonnées $(x_1,y_1),\dots,(x_n,y_n)$. La méthode d'interpolation de Lagrange étudiée dans ce paragraphe est une autre approche du même problème.

Définition 19.84 – Soient $x_1,\dots,x_n\in\mathbb{K}$ distincts. Pour tout $i\in[\![1,n]\!]$, on pose $L_i=\displaystyle\prod_{\substack{1\leqslant k\leqslant n\\ k\neq i}}\frac{X-x_k}{x_i-x_k}$. Les polynômes $L_1,\dots,L_n$ sont appelés les **polynômes de Lagrange** de $x_1,\dots,x_n$.

Pour $n=3$: $L_1=\dfrac{(X-x_2)(X-x_3)}{(x_1-x_2)(x_1-x_3)}$, $L_2=\dfrac{(X-x_1)(X-x_3)}{(x_2-x_1)(x_2-x_3)}$ et $L_3=\dfrac{(X-x_1)(X-x_2)}{(x_3-x_1)(x_3-x_2)}$.

Proposition 19.85 – Propriété fondamentale

Pour tous $i,j\in[\![1,n]\!]$: $L_i\left(x_j\right)=\delta_{ij}$.
En particulier, L_i admet $x_1,\dots,x_{i-1},x_{i+1},\dots,x_n$ pour racines.

Théorème 19.86 – Polynôme d'interpolation de Lagrange de degré minimal

Soient $x_1,\dots,x_n\in\mathbb{K}$ **DISTINCTS** et $y_1,\dots,y_n\in\mathbb{K}$ quelconques. On reprend les notations précédentes $L_1,\dots,L_n$. Le polynôme $\displaystyle\sum_{i=1}^{n}y_iL_i$ est alors le seul et unique polynôme $P\in\mathbb{K}[X]$ **DE DEGRÉ INFÉRIEUR OU ÉGAL À** $n-1$ pour lequel $P(x_i)=y_i$ pour tout $i\in[\![1,n]\!]$.

Démonstration.

Existence : Posons $P = \sum_{i=1} y_i L_i$. Par définition, $L_1, \dots, L_n$ sont de degrés inférieurs ou égaux à $n-1$, donc P aussi. Ensuite, pour tout $j \in [\![1, n]\!]$: $P(x_j) = \sum_{i=1}^{n} y_i L_i(x_j) = \sum_{i=1}^{n} y_i \delta_{ij} = y_j$.

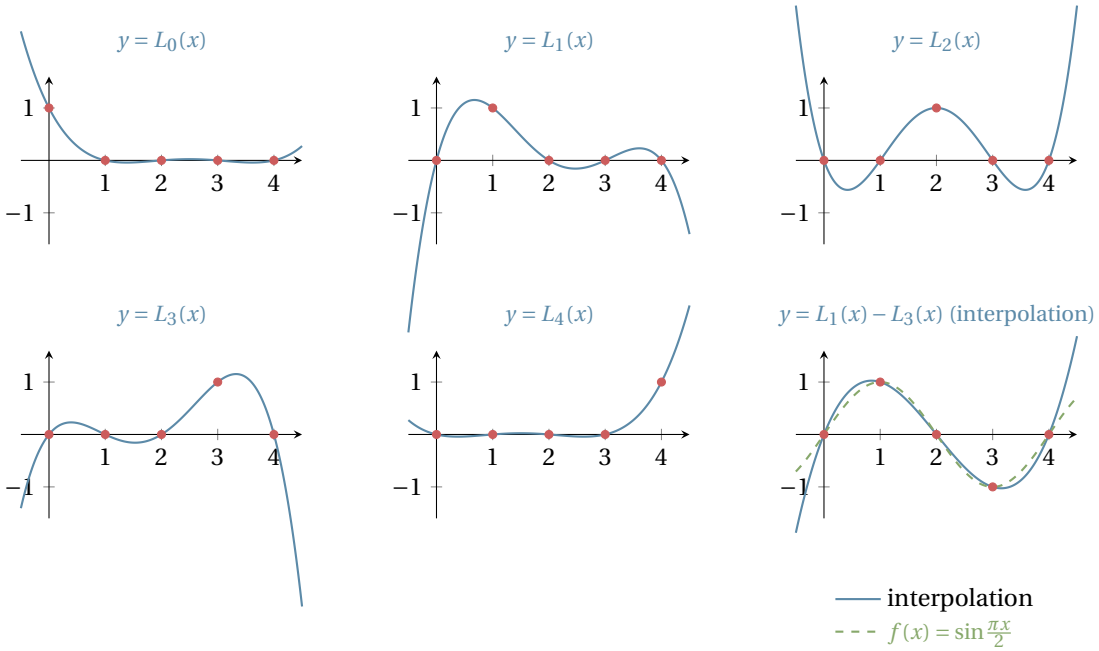
Unicité : Soient $P, Q \in \mathbb{K}[X]$ deux polynômes de degré inférieurs ou égaux à $n-1$ pour lesquels pour tout $i \in [\![1, n]\!]$: $P(x_i) = Q(x_i) = y_i$. Le polynôme $P - Q$ admet $x_1, \dots, x_n$ pour racines, donc au moins n racines comptées avec multiplicité. Comme $\deg(P-Q) \leqslant n-1$, forcément $P - Q = 0$, i.e $P = Q$.

□

Exemple 19.87 – Notons f la fonction $x \longmapsto \sin \frac{x\pi}{2}$ sur $[0,4]$, pour laquelle : $f(0) = f(2) = f(4) = 0$, $f(1) = 1$ et $f(3) = -1$. Déterminer le polynôme d'interpolation de Lagrange de f aux points $0, \dots, 4$.
Notons $L_0, \dots, L_4$ les cinq polynômes de Lagrange de $0, \dots, 4$. Le polynôme d'interpolation de Lagrange de f aux points $0, \dots, 4$ est alors en vertu du théorème précédent le polynôme $\sum_{i=0}^{4} f(i) L_i = L_1 - L_3$. Or :

$$L_1 = -\frac{X(X-2)(X-3)(X-4)}{6} \quad \text{et} \quad L_3 = -\frac{X(X-1)(X-2)(X-4)}{6}$$

$$\text{donc :} \quad L_1 - L_3 = -\frac{X(X-2)(X-3)(X-4)}{6} + \frac{X(X-1)(X-2)(X-4)}{6} = \frac{X(X-2)(X-4)}{3}.$$



Théorème 19.88

On reprend les notations précédentes et on note Y le polynôme $\sum_{i=1}^{n} y_i L_i$. Les polynômes P pour lesquels $P(x_i) = y_i$ pour tout $i \in [\![1, n]\!]$ sont exactement tous les polynômes de la forme $Y + Q \prod_{k=1}^{n} (X - x_k)$, Q décrivant $\mathbb{K}[X]$.

Démonstration. Pour tout $P \in \mathbb{K}[X]$: $\forall i \in [\![1, n]\!], \quad P(x_i) = y_i \iff \forall i \in [\![1, n]\!], \quad P(x_i) = Y(x_i)$

$$\iff P - Y \text{ admet } x_1, \dots, x_n \text{ pour racines} \iff \prod_{k=1}^{n} (X - x_k) \text{ divise } P - Y$$

$$\iff \exists Q \in \mathbb{K}[X], \quad P - Y = Q \prod_{k=1}^{n} (X - x_k)$$

□