Chapitre 15 - Polynômes

Dans tout ce chapitre, $\mathbb{K}$ désigne l'un des ensembles de nombres $\mathbb{R}$ ou $\mathbb{C}$.

1 Ensemble des polynômes à coefficients dans $\mathbb{K}$

1.1 Construction de $\mathbb{K}[X]$

Jusqu'à maintenant, vous voyiez un polynôme comme une fonction réelle (ou complexe) du lycée que l'on peut tracer. Cette vision n'est qu'une facette d'un objet mathématique qui est en fait algébrique.

Un polynôme est fondamentalement défini par la donnée de la liste de ses coefficients, par exemple le polynôme $4X^3 - 2X + 1$ est ainsi entièrement décrit par la liste $(1, -2, 0, 4)$.

La construction de l'ensemble des polynômes n'est pas au programme, mais nous nous appuierons sur la définition suivante :

Définition 1 - Polynôme à une indéterminée à coefficients dans $\mathbb{K}$.
On appelle *polynôme (à une indéterminée) à coefficients dans* $\mathbb{K}$ toute suite nulle à partir d'un certain rang d'éléments de $\mathbb{K}$, appelés coefficients. Si $(a_0, \dots, a_n, \dots)$ est une telle suite, on peut l'assimiler à la liste $(a_0, \dots, a_n)$, et on note

$$a_0 + a_1 X + \dots + a_n X^n = \sum_{k=0}^{n} a_k X^k.$$

le polynôme associé. On peut parler de *forme réduite et ordonnée*.

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 l'on choisit de noter X l'indéterminée.

Remarque 2 - Instant culturel.
La longueur de la liste des coefficients d'un polynôme peut être arbitrairement longue... d'où la vraie définition de l'ensemble des polynômes : il s'agit de l'ensemble des suites de $\mathbb{K}$ *nulles à partir d'un certain rang*. Plus délicat, on s'attend à pouvoir multiplier (et même composer des polynômes), et cela n'est pas si simple si on les voit comme des suites de coefficients, car alors, en réalisant que $(0, 1, 0, \dots) = X$ et $(0, 0, 1, 0, \dots) = X^2$, on doit alors définir un produit des suites tel que

$$(0, 1, 0, \dots) \times (0, 0, 1, 0, \dots) = (0, 0, 0, 1, 0, \dots),$$

ce qui n'est pas pratique visuellement.
On ne parlera donc pas beaucoup plus de cette approche constructive, qui n'est pas au programme.

Théorème 3 - Identification des coefficients. Deux polynômes sont égaux si et seulement si leurs coefficients le sont.

Définition 4 - Polynôme constant, polynôme nul, monoôme.

- On appelle *polynôme constant* de $\mathbb{K}[X]$ tout polynôme $(\lambda, 0, 0, \dots)$, avec $\lambda \in \mathbb{K}$, c'est-à-dire tout polynôme de la forme λX^0. Un tel polynôme sera simplement noté λ.
- Avec cette notation, le polynôme 0 est appelé *polynôme nul*.
- On appelle monôme un polynôme dont un seul des coefficients est non nul, donc un polynôme de la forme λX^p avec $\lambda \in \mathbb{K}$ et $p \in \mathbb{N}$.

Définition-théorème 5 - Addition et multiplication sur $\mathbb{K}[X]$. Soit $P=(a_k)_{k\in\mathbb{N}}, Q=(b_k)_{k\in\mathbb{N}}\in\mathbb{K}[X]$.

- Soient $\lambda\in\mathbb{K}$ et $\mu\in\mathbb{K}$, on appelle *somme de P et Q* le polynôme $(\lambda a_k+\mu b_k)_{k\in\mathbb{N}}$, noté $\lambda P+\mu Q$. On a en particulier
$$\lambda\left(\sum_{k=0}^{n}a_kX^k\right)+\mu\left(\sum_{k=0}^{n}b_kX^k\right)=\sum_{k=0}^{n}\left(\lambda a_k+\mu b_k\right)X^k$$
- On appelle *produit de P et Q* le polynôme $\left(\sum_{i=0}^{k}a_ib_{k-i}\right)_{k\in\mathbb{N}}$, noté $P\times Q$ ou PQ. On a en particulier
$$\left(\sum_{k=0}^{n}a_kX^k\right)\times\left(\sum_{k=0}^{n}b_kX^k\right)=\sum_{0\leqslant i,j\leqslant n}a_ib_jX^{i+j}=\sum_{k=0}^{2n}\overbrace{\left(\sum_{\substack{0\leqslant i,j\leqslant n\\ i+j=k}}a_ib_j\right)}^{\text{On regroupe les termes de même degré } k}X^k=\sum_{k=0}^{2n}\overbrace{\left(\sum_{i=0}^{k}a_ib_{k-i}\right)}^{\substack{\text{On élimine } j\\ \text{via la relation } j=k-i}}X^k,$$

✎ **En pratique** ✎ Attention, l'écriture $P=\sum_{k=0}^{n}a_kX^k$ ne sous-entend en aucune façon que $a_n\neq 0$! La définition du produit et la méthode proposée permet bien de faire le produit de n'importe quel polynôme. Nous verrons une méthode plus approprié lorsque nous aurons défini le degré.

On peut alors montrer que l'addition et la multiplication sont associatives et commutatives, que la multiplication est distributive sur l'addition, que le polynôme nul 0 est le neutre pour l'addition, *i.e.* $0+P=P+0=P$, et que le polynôme constant 1 est le neutre pour la multiplication, *i.e.* $1\times P=P\times 1=P$. Bref, les règles usuelles du calcul littéral que vous connaissez sont respectées.

Corollaire 6 - Formule du binôme. Pour tous $P,Q\in\mathbb{K}[X]$ et $n\in\mathbb{N}$, $\quad(P+Q)^n=\sum_{k=0}^{n}\binom{n}{k}P^kQ^{n-k}$.

Le temps de la notation polynomiale est enfin arrivée ! Conformément au programme, on peut oublier la construction qui précède. Le point de vue des suites presque nulles nous a seulement permis de définir proprement le monde des *polynômes formels* – qualifiés ainsi pour les distinguer des fonctions polynomiales, sur lesquelles nous reviendrons plus tard.

Terminons ce paragraphe avec une application classique du théorème 3 d'identification des coefficients de polynômes égaux.

Application 7 - Formule de Vandermonde. En étudiant l'égalité $(X+1)^{2n}=(X+1)^n\times(X+1)^n$, montrer que pour tout $n\in\mathbb{N}$, $\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

En effet, l'égalité $(X+1)^{2n}=(X+1)^n\times(X+1)^n$ s'écrit aussi
$$\sum_{k=0}^{2n}\binom{2n}{k}X^k=\sum_{i=0}^{n}\binom{n}{i}X^i\times\sum_{j=0}^{n}\binom{n}{j}X^j=\sum_{k=0}^{2n}\sum_{i=0}^{k}\binom{n}{i}\binom{n}{k-i}X^k.$$
Dans le membre de gauche, le coefficient de degré n vaut $\binom{2n}{n}$ et, dans le membre de droite, par définition du produit de deux polynômes, il vaut $\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}=\sum_{i=0}^{n}\binom{n}{i}^2$.

Définition-théorème 8 - Composition des polynômes. Soit $P = \sum_{k=0}^{n} a_k X^k, Q \in \mathbb{K}[X]$, avec $n \in \mathbb{N}$. On appelle *composée de Q suivie de P*, notée $P \circ Q$ ou $P(Q)$, le polynôme

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

Remarque 9

- Comme pour les puissances d'un nombre, pour tout $Q \in \mathbb{K}[X]$, $Q^0 = 1$, on a donc si $P = \sum_{k=0}^{n} a_k X^k$,
$$P \circ Q = a_n Q^n + \ldots + a_2 Q^2 + a_1 Q + a_0.$$
- Dans le cas particulier où $Q = X$, le polynôme $P(Q) = P(X)$ est égal à P, c'est pourquoi on utilise aussi bien l'écriture P que $P(X)$ pour désigner ce polynôme.
- On peut montrer sans difficulté que, pour tous $\lambda, \mu \in \mathbb{K}$ et $P, Q, R \in \mathbb{K}[X]$,
$$(\lambda P + \mu Q) \circ R = \lambda P \circ R + \mu Q \circ R \qquad \text{et} \qquad (PQ) \circ R = (P \circ R)(Q \circ R).$$

Exemple 10

- Un polynôme P est dit *pair* lorsque $P(-X) = P(X)$. Or si $P = \sum_{k=0}^{n} a_k X^k$, alors $P(-X) = \sum_{k=0}^{n} (-1)^k a_k X^k$. Ainsi P est pair si et seulement si, pour tout $k \in \mathbb{N}$, $a_{2k+1} = 0$, *i.e.* si et seulement si P est combinaison de puissances paires de X.
- Similairement, un polynôme P est dit *impair* lorsque $P(-X) = -P(X)$. Ainsi P est impair si et seulement s'il est combinaison de puissances impaires de X.

1.2 Degré d'un polynôme

Pour un polynôme $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ non nul, l'ensemble $D = \{k \in \mathbb{N} \mid a_k \neq 0\}$ est une partie non vide et majorée de $\mathbb{N}$, puisque la suite $(a_k)_{k\in\mathbb{N}}$ des coefficients est nul à partir d'un certain rang, D admet donc un plus grand élément, ce qui légitime la définition suivante.

Définition 11 - Degré d'un polynôme, coefficient dominant, polynôme unitaire.

- Soit $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ non nul. On appelle *degré de P*, noté $\deg P$, le plus grand indice k tel que $a_k \neq 0$. Le coefficient de degré $\deg P$ est appelé son *coefficient dominant* et, lorsque ce dernier est égal à 1, le polynôme P est dit *unitaire*.
- Par convention, le polynôme nul est de degré $-\infty$: $\deg 0 = -\infty$.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré INFÉRIEUR ou égal à n est noté $\mathbb{K}_n[X]$.

Exemple 12

- Le polynôme $P = 3X^2 - \sqrt{5}X + 2$ est de degré 2 et a pour coefficient dominant 3. Ainsi $P \in \mathbb{R}_2[X]$, mais on a aussi $P \in \mathbb{R}_{155}[X]$ par exemple, puisque $\deg P \leqslant 155$.
- Le polynôme $X^3 - 3X + 2$ est unitaire.

Exemple 13 Déterminer le degré et le coefficient dominant de $(X+2)^n - (X-2)^n$.

Remarque 14

- Un polynôme $\sum_{k=0}^{n} a_k X^k$ est de degré INFÉRIEUR ou égal à n. Et il est de degré n si et seulement si $a_n \neq 0$.
- Un polynôme est constant si et seulement s'il est nul ou de degré nul. Ainsi $\mathbb{K}_0[X]$ s'identifie à $\mathbb{K}$.

Théorème 15 - Degrés d'une somme et d'un produit. Soit $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

(i) Degré d'une somme. $\deg(P+Q) \leqslant \max\{\deg P, \deg Q\}$, avec égalité lorsque $\deg P \neq \deg Q$.

(ii) Degré d'un produit. $\deg(PQ) = \deg P + \deg Q$. En particulier, si $\lambda \neq 0$, $\deg(\lambda P) = \deg P$.

(iii) Degré d'une composée. Si Q n'est pas constant, alors $\deg(P \circ Q) = \deg P \times \deg Q$.

✎ **En pratique** ✎ On dispose désormais d'une formule pour calculer le produit de deux polynômes avec la notation polynomiale : Etant donnés deux polynômes P et Q de degrés respectifs n et m, on écrit

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{m} b_k X^k.$$

On a alors

$$PQ = \sum_{k=0}^{n+m} c_k X^k \quad \text{avec } c_k = \sum_{\substack{0\leqslant i\leqslant n\\ 0\leqslant j\leqslant m\\ i+j=k}} a_i b_j = \sum_{0\leqslant i\leqslant n} a_i b_{k-i}.$$

Exemple 16 - Effectuer les produits suivants :.

1. $X \times \left(\sum_{k=0}^{n} a_k X^k\right)$ **2.** $(X-1) \times \left(\sum_{k=0}^{n} X^k\right)$

Exemple 17 L'inégalité pour la somme est due à la situation suivante : soit $P = X^2+1$ et $Q = -X^2+X-2$, alors $P+Q = X-1$ et $\deg(P+Q) = 1 < \max\{\deg P, \deg Q\} = 2$.

Remarque 18 Pour tous $\lambda, \mu \in \mathbb{K}$ et $P, Q \in \mathbb{K}[X]$, $\deg(\lambda P + \mu Q) \leqslant \max\{\deg P, \deg Q\}$.

Le résultat précédent concernant le degré d'un produit permet d'établir le résultat suivant :

Théorème 19 - Intégrité de $\mathbb{K}[X]$. $\mathbb{K}[X]$ est *intègre*, *i.e.* vérifie

$$\forall P, Q \in \mathbb{K}[X], \quad (PQ = 0 \implies P = 0 \text{ ou } Q = 0).$$

Démonstration. Soit $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $\deg P + \deg Q = \deg(PQ) = -\infty$ et nécessairement $\deg P = -\infty$ ou $\deg Q = -\infty$, *i.e.* $P = 0$ ou $Q = 0$. ∎

Remarque 20 Cette propriété serait nettement plus difficile à prouver si l'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 rien ne nous garantit alors que l'une des deux s'annule tout le temps.

1.3 Dérivation des polynômes

Définition 21 - Dérivation des polynômes. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, avec $n \in \mathbb{N}$.

- Le polynôme $\sum_{k=0}^{n} k a_k X^{k-1}$ est appelé *polynôme dérivé de P* et noté P' – avec pour convention, pour $k=0$, $0 \times X^{-1} = 0$.
- On définit alors, pour tout $p \in \mathbb{N}$, le *p^e polynôme dérivé de P*, noté $P^{(p)}$, par récurrence :

$$\begin{cases} P^{(0)} = P, \\ P^{(p+1)} = \left(P^{(p)}\right)', \text{ pour tout } p \in \mathbb{N}. \end{cases}$$

Pour $n \in \{2, 3\}$, on préfère toutefois les notations P'' et P''' à $P^{(2)}$ et $P^{(3)}$.

Exemple 22 Pour $P = 8X^3 - 5X^2 + 3X + 1$, on a

$$P' = 24X^2 - 10X + 3, \qquad P'' = \left(P'\right)' = 48X - 10, \qquad P''' = \left(P''\right)' = 48, \qquad P^{(4)} = \left(P'''\right)' = 0$$

et donc $P^{(p)} = 0$, pour tout $p \geqslant 4$.

Exemple 23 Pour tous $n \in \mathbb{N}$ et $p \in [\![0\,,n]\!]$, $\left(X^n\right)^{(p)} = n(n-1)\cdots(n-p+1)X^{n-p} = p!\binom{n}{p}X^{n-p}$.

Les règles opératoires pour la dérivation des polynômes formelles sont identiques à celles pour les fonctions dérivables ! En revanche, dans le cadre des polynômes formelles, il est parfaitement hors de propos de s'intéresser à la dérivabilité.

Théorème 24 - Propriétés de la dérivation des polynômes. Soit $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $n \in \mathbb{N}$.

(i) Degré. $\begin{cases} \deg\left(P^{(n)}\right) = \deg P - n & \text{si } n \leqslant \deg P, \\ P^{(n)} = 0 & \text{sinon.} \end{cases}$ En particulier, P est constant si et seulement si $P' = 0$.

(ii) Linéarité. $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.

(iii) Produit. $(PQ)' = P'Q + PQ'$ et plus généralement

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)} \qquad \textit{(formule de Leibniz}^{\dagger}\textit{)}.$$

(iv) Composition. $(P \circ Q)' = Q' \times P' \circ Q$.

Exercice 25

Pour tous $n \in \mathbb{N}$ et $p \in [\![0\,,n]\!]$, $\left((aX+b)^n\right)^{(p)} = a^p\,(aX+b)^{n-p}$.

2 Divisibilité et division polynomiale

Les notions et résultats de cette section sont analogues à ceux que vous connaissez concernant les entiers relatifs.

2.1 Relation de divisibilité

Définition 26 - Divisibilité, diviseur, multiple. Soit $A, B \in \mathbb{K}[X]$.
On dit que A *divise* B, ou que A *est un diviseur de* B, ou que B est divisible par A ou encore que B *est un multiple de* A lorsqu'il existe $P \in \mathbb{K}[X]$ tel que $B = AP$. Cette relation se note $A \mid B$.

Exemple 27

- Le polynôme $X^2 + X - 6$ est divisible par $X + 3$ car $X^2 + X - 6 = (X+3)(X-2)$.
- Le polynôme nul est divisible par tous les polynômes mais il ne divise que lui-même.
- Si $A \mid B$ avec B non nul, alors $\deg B \geqslant \deg A$.

Théorème 28 - Propriétés de la relation de divisibilité. Soit $A, B, C, D \in \mathbb{K}[X]$

(i) $A \mid A$. **(ii)** $A \mid B$ et $B \mid C \implies A \mid C$. **(iii)** $A \mid B$ et $B \mid A \iff \exists \lambda \in \mathbb{K}^*,\ A = \lambda B$.

(iv) $D \mid A$ et $D \mid B \implies \forall U, V \in \mathbb{K}[X],\ D \mid (AU + BV)$.

(v) $A \mid B$ et $C \mid D \implies AC \mid BD$. En particulier, $A \mid B \implies \forall k \in \mathbb{N},\ A^k \mid B^k$.

†. Gottfried Wilhelm Leibniz (1646 à Leipzig – 1716 Hanovre), est un philosophe, scientifique, mathématicien, logicien, diplomate, juriste, bibliothécaire et philologue allemand. On lui attribue généralement, avec Isaac Newton, l'invention du calcul infinitésimal.

Démonstration.

(i) On a tout simplement $A = A \times 1$ et $1 \in \mathbb{K}[X]$.

(ii) Il existe $P, Q \in \mathbb{K}[X]$ tels que $B = AP$ et $C = BQ$, ainsi $C = APQ$ avec $PQ \in \mathbb{K}[X]$.

(iii) Si $A \mid B$ et $B \mid A$, alors il existe $P, Q \in \mathbb{K}[X]$ tels que $B = AP$ et $A = BQ$, ainsi $A = APQ$ avec $PQ \in \mathbb{K}[X]$.

- Si $A = 0$, alors $B = 0$ et donc $A = \lambda B$ avec $\lambda = 1$ par exemple.
- Si $A \neq 0$, alors $PQ = 1$, par intégrité de $\mathbb{K}[X]$, et en particulier P et Q sont non nuls et donc de degrés entiers. Or les inégalités $0 \leqslant \deg P \leqslant \deg(P) + \deg(Q) = \deg(PQ) = \deg(1) = 0$, montrent que $\deg P = 0$, *i.e.* $P \in \mathbb{K}^*$.

La réciproque est claire, dans la mesure où λ et $\dfrac{1}{\lambda}$ sont des éléments de $\mathbb{K}[X]$.

(iv) Il existe $P, Q \in \mathbb{K}[X]$ tels que $A = DP$ et $B = DQ$. Ainsi, pour tout $U, V \in \mathbb{K}[X]$, $AU + BV = D(UP + VQ)$ avec $(UP + VQ) \in \mathbb{K}[X]$.

(v) Il existe $P, Q \in \mathbb{K}[X]$ tels que $B = AP$ et $D = CQ$, alors $BD = ACPQ$ avec $PQ \in \mathbb{K}[X]$. Pour la seconde partie, il suffit de procéder par récurrence sur $k \in \mathbb{N}$.

■

2.2 Division euclidienne

Théorème 29 - Division euclidienne. Soit $A, B \in \mathbb{K}[X]$ avec B NON NUL.
Il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X]^2$ pour lequel $A = BQ + R$ et $\deg R < \deg B$. On appelle A le *dividende* de la division euclidienne de A par B, B le *diviseur*, Q le *quotient* et R le *reste*.

Démonstration.

- **Existence.** Si B divise A, il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$ et on pose $R = 0$.
  Supposons désormais que B ne divise pas A, notons b son degré et $\beta \neq 0$ son coefficient dominant. L'ensemble $\mathscr{D} = \{\deg(A - BP)\}_{P \in \mathbb{K}[X]}$ est alors une partie non vide de $\mathbb{N}$ (la valeur $-\infty$ étant exclue par hypothèse) et possède donc un plus petit élément r. Notons $Q \in \mathbb{K}[X]$ un polynôme tel que $\deg(A - BQ) = r$, posons $R = A - BQ$ $(R \neq 0)$ et notons ρ le coefficient dominant de R. Il reste à espérer que $\deg R < \deg B$.
  Par l'absurde, supposons que $r \geqslant b$. Alors $\deg\left(R - \dfrac{\rho}{\beta}X^{r-b}B\right) < r$, car la soustraction par $\dfrac{\rho}{\beta}X^{r-b}B$ annule le terme dominant ρX^r de R. Or $\deg\left(R - \dfrac{\rho}{\beta}X^{r-b}B\right) = \deg(A - BP) \in \mathscr{D}$ en posant $P = Q + \dfrac{\rho}{\beta}X^{r-b}B$, ce qui contredit la minimalité de r ! Ainsi $r \leqslant b$.
- **Unicité.** Soit (Q_1, R_1) et (Q_2, R_2) deux couples de la division euclidienne de A par B. Par définition, $B(Q_1 - Q_2) = R_1 - R_2$. Si $Q_1 \neq Q_2$, on a alors $\deg(Q_1 - Q_2) \geqslant 0$, donc $\deg(B(Q_1 - Q_2)) \geqslant \deg B$, alors que $\deg(R_1 - R_2) < \deg B$, par définition de R_1 et R_2 – contradiction ! Ainsi, $Q_1 = Q_2$ et aussitôt $R_1 = R_2$.

■

Remarque 30 Le polynôme B divise A si et seulement si le reste de la division de A par B est nul.

✎ **En pratique** ✎ Pour effectuer concrètement une division euclidienne, on pourra appliquer l'algorithme de la division euclidienne, avec des notations proches des petites classes, voir prise de notes en cours.

Exemple 31 La division euclidienne de $7X^5 + 4X^4 + 2X^3 - X + 5$ par $X^2 + 2$ donne après calculs :

$$7X^5 + 4X^4 + 2X^3 - X + 5 = \left(X^2 + 2\right) \underbrace{\left(7X^3 + 4X^2 - 12X - 8\right)}_{\text{quotient}} + \underbrace{23X + 21}_{\text{reste}}.$$

En particulier, $7X^5 + 4X^4 + 2X^3 - X + 5$ n'est pas divisible par $X^2 + 2$, puisque le reste de la division euclidienne entre ces deux polynômes n'est pas nul.

La division euclidienne est un outil puissant pour le calcul des primitives des fractions rationelles, car elle permet de se ramener à un degré moins élevé pour le numérateur. Nous reviendrons sur ce point plus tard.

3 Racines d'un polynôme

3.1 Lien avec les fonctions polynomiales

Définition-théorème 32 - Évaluation polynomiale, fonction polynomiale associée.

- Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, avec $n \in \mathbb{N}$, et $\lambda \in \mathbb{K}$. On pose $P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k$, élément de $\mathbb{K}$ appelé *évaluation de P en λ*.
- Pour tout $P \in \mathbb{K}[X]$, la fonction $\lambda \longmapsto P(\lambda)$ de $\mathbb{K}$ dans $\mathbb{K}$ est appelé la *fonction polynomiale associée à P*. On la note $\widetilde{P}$ lorsque l'on veut la distinguer proprement du polynôme P, mais on la note aussi souvent P, dans la mesure où l'on s'autorise à confondre un polynôme avec sa fonction polynomiale (cf. théorème 56).
- Pour tous $P, Q \in \mathbb{K}[X]$, $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ et $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$.
- Pour tous $P, Q \in \mathbb{R}[X]$, $\widetilde{P'} = \widetilde{P}'$.

Démonstration. Admis. ■

Les résultats des deux derniers points n'ont rien d'évidents. Nous disposons sur $\mathbb{R}[X]$ et $\mathbb{R}^{\mathbb{R}}$ de notions DIFFÉRENTES d'addition, multiplication, composition et dérivation. Par exemple, dans la formule « $\widetilde{P'} = \widetilde{P}'$ », la dérivée P' est une dérivée formelle (celle de la définition 21), alors que la dérivée $\widetilde{P}'$ est la dérivée d'une fonction définie comme limite d'un taux d'accroissement.

✖ ATTENTION ! ✖ X n'est pas un nombre ! On ne dit pas « Posons $X = 1$ », mais « Évaluons en 1 ».

Remarque 33 - Pourquoi cette différence ?. Msieur, msieur ! Ca fait 6 mois que vous nous criez dessus de ne pas confondre f et $f(x)$, et maintenant on peut écrire $P = P(X)$?
La différence entre la notion de polynôme formel et de fonction est profonde, elle vient du fait qu'un polynôme est uniquement déterminé par une liste finie de coefficients, alors qu'une fonction est plus complexe à définir. Si on pense en terme de programmation, on peut définir et manipuler des polynômes facilement en tant que liste, ce que l'on ne peut faire pour des fonctions réelles. Pour aller plus loin, un polynôme $P(X)$ peut être évalué en de nombreux objets différents, ce qui très intéressant tant en mathématique qu'en informatique (avec-vous entendu de la« programmation orienté objet » ?).

Un exemple d'application important sera lié aux matrices. Puisqu'on a définit le produit matriciel, on a aussi défini des puissances de matrices, et on peut donc évaluer un polynôme en une matrice $A \in M_n(\mathbb{K})$, avec la convention $A^0 = I_n$

Exemple 34 - Evaluation matricielle. Soit $P(X) = X^2 - 3X + 2$ et $A = \begin{pmatrix} 1 & 4 \\ 2 & -1 \end{pmatrix}$. Calculer $P(A)$.

La méthode de Horner Comment évaluer efficacement un polynôme $P = \sum_{k=0}^{n} a_k X^k$ en $\lambda \in \mathbb{K}$? Si on calcule froidement chaque puissance λ^k séparément, on effectue déjà $1 + \ldots + n = \frac{n(n-1)}{2}$ opérations, auxquelles s'ajoutent les multiplications par les coefficients a_k, puis la somme finale $\lambda_n a^n + \ldots + a_0$.

La méthode de Horner est un algorithme qui permet de diminuer la quantités d'opérations sans même avoir à stocker les valeurs successives des puissances de λ. Elle consiste à écrire

$$P(\lambda) = ((\ldots((a_n\lambda + a_{n-1}) + a_{n-2})\lambda + \ldots)\lambda + a_1)\lambda + a_0.$$

Cette écriture, sur laquelle on lit l'ordre de l'algorithme, est plus digeste si on part de la droite :

$$P(\lambda) = a_0 + \lambda(a_1 + \ldots).$$

Ainsi, on réalise $2n + 1$ opérations : des sommes et des multiplications successives, en commençant par former le produit $a_n\lambda$ puis la somme $a_n\lambda + a_{n-1}$, etc...

Voici l'algorithme en Python :

Algorithme 1 : Méthode d'Horner pour évaluer un polynôme $P = \sum_{k=0}^{n} a_k X^k$ en $\lambda \in \mathbb{K}$

Entrées : Un polynôme P de degré n, sous la forme d'une liste $[a_n, \dots, a_0]$ et un nombre $\lambda \in \mathbb{K}$.
Sorties : La valeur $P(\lambda)$

```
def horner(P,x) : ;
n=len(P) ;
valeur=0;
pour i in range(0,n) : faire
    valeur=valeur*lambda+P[i]
return valeur
```

3.2 Racines et multiplicités

Lemme 35 - Division euclidienne par $X - \lambda$. Soit $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Le reste de la division euclidienne de P par $X - \lambda$ est $P(\lambda)$.

Démonstration. Par division euclidienne, il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - \lambda)Q + R$ et $\deg R < 1$. Ainsi R est un polynôme constant. Il suffit alors d'évaluer en λ : $P(\lambda) = (\lambda - \lambda)Q(\lambda) + R(\lambda) = R$. ■

De ce résultat préliminaire découle la double définition suivante :

Définition 36 - Racine. Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On dit que λ est une *racine de P (dans $\mathbb{K}$)* lorsque l'une des deux assertions équivalentes suivantes est vérifiée :

(i) $P(\lambda) = 0$. **(ii)** P est divisible par $X - \lambda$.

✎ **En pratique** ✎ On retiendra :

$$P(\lambda) = 0 \iff \exists Q \in \mathbb{K}[X] \text{ non nul tel que } P(X) = (X - \lambda)Q.$$

Cette propriété est ESSENTIELLE car elle vous permet de factoriser un polynôme une fois que vous en avez trouvé une racine. Pour trouver Q, on peut effectuer une division euclidinne, ou encore chercher les coefficients de Q en identifiant ceux de $(X - \lambda)Q$ avec ceux de P.

Exemple 37 - Une factorisation. Soit $P(X) = X^4 + 3X^3 - X^2 + 2X - 5$. Calculer $P(1)$ puis factoriser P.

✖ **Attention !** ✖ La précision « racine dans $\mathbb{K}$ » n'est pas superflue. Par exemple, le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, alors qu'il en a deux dans $\mathbb{C}$, à savoir i et $-i$.

✎ **En pratique** ✎ Via la notion de racine, on ramène souvent les problèmes de divisibilité à des problèmes d'évaluation, et vice versa.

Exemple 38 Pour tout $n \in \mathbb{N}$, le reste de la division euclidienne de X^n par $X^2 - 3X + 2$ vaut $(2^n - 1)X - (2^n - 2)$.
En effet, pour tout $n \in \mathbb{N}$, la division euclidienne de X^n par $X^2 - 3X + 2$ s'écrit $X^n = (X - 1)(X - 2)Q + aX + b$, avec $Q \in \mathbb{K}[X]$ et $a, b \in \mathbb{R}$. Évaluons en 1 : $1 = a + b$, et en 2 : $2^n = 2a + b$, ce qui aboutit, après calculs, à $a = 2^n - 1$ et $b = 2 - 2^n$.

Définition-théorème 39 - Multiplicité d'une racine. Soit $P \in \mathbb{K}[X]$ NON NUL et $\lambda \in \mathbb{K}$.

- L'ensemble $\left\{k \in \mathbb{N} \,\middle|\, (X-\lambda)^k \text{ divise } P\right\}$ possède un plus grand élément m appelé la *multiplicité de λ dans P*. Pour résumer, on dit souvent que m est la plus grande puissance de $X-\lambda$ qui divise P.

  En particulier, dire que λ n'est pas une racine de P revient à dire que λ a pour multiplicité 0 dans P. Une racine est dite *simple* lorsqu'elle est de multiplicité 1, *double* lorsqu'elle est de multiplicité 2, etc.
- Plus concrètement, l'entier m est caractérisé par les deux assertions équivalentes suivantes :
  - **(i)** P est divisible par $(X-\lambda)^m$ mais PAS par $(X-\lambda)^{m+1}$.
  - **(ii)** Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\lambda)^m Q$ et $Q(\lambda) \neq 0$.

Exemple 40 - Exemples faciles. Donner les racines dans $\mathbb{R}$ et leurs multiplicités pour les polynômes suivants :

1. $(X+1)(X-1)^2$. **2.** $(X+2)^n$. **3.** $X^4+3X^3+3X^2+X$. **4.** $(X-1)(X^2+3)$. Et dans $\mathbb{C}$?

Théorème 41 - Formule de Taylor polynomiale. Pour tout $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, $\displaystyle P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k$.

En particulier, pour tout $k \in \mathbb{N}$, le coefficient de degré k de P est $\dfrac{P^{(k)}(0)}{k!}$.

Démonstration.

- **Cas $\lambda = 0$.** En notant $P = \displaystyle\sum_{i=0}^{+\infty} a_i X^i$, dérivons k fois, pour tout $k \in \mathbb{N}$, $P^{(k)} = \displaystyle\sum_{i=0}^{+\infty} a_i \frac{i!}{(i-k)!} X^{i-k}$, puis évaluons en 0, $P^{(k)}(0) = a_k k!$. Aussitôt $a_k = \dfrac{P^{(k)}(0)}{k!}$ et donc $P = \displaystyle\sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} X^k$.
- **Cas général.** Posons $Q = P(X+\lambda)$. Alors, pour tout $k \in \mathbb{N}$, $Q^{(k)} = P^{(k)}(X+\lambda)$. On en déduit que

$$Q = \sum_{k=0}^{+\infty} \frac{Q^{(k)}(0)}{k!} X^k = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} X^k$$

  et on termine en composant à droite par $X-\lambda$.

■

Remarque 42 Malgré les apparences, la somme $\displaystyle\sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k$ est finie puisque $P^{(k)}$ est nul, pour tout $k > \deg P$.

La formule de Taylor va nous permettre de caractériser la multiplicité d'une racine d'un polynôme par l'annulation des dérivées successives de ce polynôme en cette racine.

Théorème 43 - Multiplicité et dérivées successives. Soit $P \in \mathbb{K}[X]$ non nul, $\lambda \in \mathbb{K}$ et $m \in \mathbb{N}$.
λ est de multiplicité m dans P si et seulement si $P^{(k)}(\lambda) = 0$, pour tout $k \in [\![0, m-1]\!]$, ET $P^{(m)}(\lambda) \neq 0$.

Démonstration.

- Supposons λ de multiplicité m dans P. Dans ce cas, il existe d'une part $Q \in \mathbb{K}[X]$ tel que $P = (X-\lambda)^m Q$ et $Q(\lambda) \neq 0$. D'autre part, d'après la formule de Taylor

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = (X-\lambda)^m \sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m} + \underbrace{\sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k}_{\text{degré} < m}.$$

  Ainsi, par unicité du reste et du quotient dans la division euclidienne de P par $(X-\lambda)^m$:

⋆ $\sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = 0$, ce qui en composant à droite par $X+\lambda$ donne $\sum_{k=0}^{m-1} \frac{P^{(k)}(\lambda)}{k!}X^k = 0$ et en identifiant $P^{(k)}(\lambda) = 0$, pour tout $k \in [\![0, m-1]\!]$;

⋆ $Q = \sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m}$, ainsi $Q(\lambda) = \frac{P^{(m)}(\lambda)}{m!}$ et donc $P^{(m)}(\lambda) \neq 0$, puisque $Q(\lambda) \neq 0$.

- Supposons réciproquement que $P(\lambda) = P'(\lambda) = \ldots = P^{(m-1)}(\lambda) = 0$ et $P^{(m)}(\lambda) \neq 0$. Alors, d'après la formule de Taylor,

$$P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = \sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = (X-\lambda)^m \sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m} = (X-\lambda)^m Q,$$

avec $Q = \sum_{k=m}^{+\infty} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^{k-m}$. Or $Q(\lambda) = \frac{P^{(m)}(\lambda)}{m!} \neq 0$, par hypothèse, et λ est donc bien de multiplicité m dans P.

■

Exemple 44 La multiplicité de 1 dans $P = X^4 + 3X^3 - 3X^2 - 7X + 6$ est égale à 2.

En effet, déjà $P(1) = 1 + 3 - 3 - 7 + 6 = 0$. Ensuite, $P' = 4X^3 + 9X^2 - 6X - 7$ et $P'(1) = 4 + 9 - 6 - 7 = 0$. Enfin, $P'' = 12X^2 + 18X - 6$ et $P''(1) = 12 + 18 - 6 = 24 \neq 0$.

Exemple 45 Le trinôme du second degré $aX^2 + bX + c$, avec $a, b, c \in \mathbb{K}$ et $a \neq 0$, admet une racine double α si et seulement si $b^2 - 4ac = 0$ et, le cas échéant, $\alpha = -\frac{b}{2a}$.

En effet, posons $P = aX^2 + bX + c$.

$$P(\alpha) = P'(\alpha) = 0 \iff \begin{cases} a\alpha^2 + b\alpha + c = 0 \\ 2a\alpha + b = 0 \end{cases} \underset{a\neq 0}{\iff} \begin{cases} a \times \left(\frac{-b}{2a}\right)^2 + b \times \frac{-b}{2a} + c = 0 \\ \alpha = -\frac{b}{2a} \end{cases} \iff \begin{cases} \frac{4ac - b^2}{4a} = 0 \\ \alpha = -\frac{b}{2a} \end{cases}.$$

Théorème 46 - Racines complexes d'un polynôme réel.
Soit $P \in \mathbb{R}[X]$ non nul – à coefficients RÉELS donc – et $\lambda \in \mathbb{C}$. Alors λ et $\overline{\lambda}$ ont même multiplicité dans P.

Démonstration. P étant à coefficients réels, pour tout $k \in \mathbb{N}$, $P^{(k)}\left(\overline{\lambda}\right) = \overline{P^{(k)}(\lambda)}$, la conclusion provient alors du théorème 43. ■

Exemple 47 À quelle condition nécessaire et suffisante sur $n \in \mathbb{N}$ le polynôme $X^2 + 1$ divise-t-il $X^n + 1$?
Réponse : $n \equiv 2\ [4]$.

En effet, puisque $X^2 + 1 = (X - i)(X + i)$, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} X^2 + 1 \mid X^n + 1 &\iff i \text{ et } -i \text{ sont racines de } X^n + 1 \\ &\iff i \text{ est racine de } X^n + 1 \qquad \text{car } X^n + 1 \in \mathbb{R}[X] \\ &\iff i^n + 1 = 0 \\ &\iff \mathrm{e}^{\frac{ni\pi}{2}} = \mathrm{e}^{i\pi} \\ &\iff \frac{n\pi}{2} \equiv \pi\ [2\pi] \\ &\iff n \equiv 2\ [4]. \end{aligned}$$

✎ **En pratique** ✎ Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Nous avons déjà vu (cf. exemple 38) de quelle manière les racines de B peuvent être exploitées lorsque l'on veut déterminer le reste de la division euclidienne de A par B. Le théorème 43 permet de prendre en compte leurs multiplicités respectives.

- Si $B = X(X-1)(X+4)$, la division euclidienne de A par B s'écrit $A = X(X-1)(X+4)Q + aX^2 + bX + c$, avec $Q \in \mathbb{K}[X]$ et $a, b, c \in \mathbb{R}$, et l'évaluation de cette égalité en les racines 0, 1 et -4 fournit un système linéaire d'inconnue a, b, c aisé à résoudre.
- Si $B = (X-2)^3(X+1)$, la division euclidienne de A par B s'écrit $A = (X-2)^3(X+1)Q + aX^3 + bX^2 + cX + d$, avec $Q \in \mathbb{K}[X]$ et $a, b, c, d \in \mathbb{R}$. On n'obtient hélas que deux équations en évaluant en 2 et -1, mais on en obtient deux supplémentaires en exploitant la multiplicité de 2 dans B. En effet, $A'(2) = 12a + 4b + c$ et $A''(2) = 12a + 2b$.

Exemple 48 Pour tout $n \in \mathbb{N}^*$, le reste de la division euclidienne de X^n par $X(X-1)^2$ est $(n-1)X^2 - (n-2)X$.
En effet, ...

3.3 Nombre maximal de racines

Théorème 49 - Factorisation « par les racines ».
Soit $P \in \mathbb{K}[X]$ NON NUL et $\lambda_1, \dots, \lambda_r \in \mathbb{K}$ des racines distinctes de P de multiplicités respectives $m_1, \dots, m_r$. Alors $(X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}$ divise P. En particulier $\sum_{i=1}^{r} m_i \leqslant \deg P$.

Démonstration. Commençons par un lemme, en notant, pour tous $P \in \mathbb{K}[X]$ non nul et $\lambda \in \mathbb{K}$, $\text{mult}(P, \lambda)$ la multiplicité de λ dans P.

Lemme 50 Pour tous $P, Q \in \mathbb{K}[X]$ non nuls et $\lambda \in \mathbb{K}$, $\text{mult}(PQ, \lambda) = \text{mult}(P, \lambda) + \text{mult}(Q, \lambda)$.

Démonstration. Posons $m = \text{mult}(P, \lambda)$ et $n = \text{mult}(Q, \lambda)$.
Il existe alors $P_1, Q_1 \in \mathbb{K}[X]$ tels que $P = (X-\lambda)^m P_1$ et $P_1(\lambda) \neq 0$, et $Q = (X-\lambda)^n Q_1$ et $Q_1(\lambda) \neq 0$.
Alors $PQ = (X-\lambda)^m P_1 (X-\lambda)^n Q_1 = (X-\lambda)^{m+n} P_1 Q_1$ et $(P_1 Q_1)(\lambda) = P_1(\lambda) Q_1(\lambda) \neq 0$. Autrement dit, $\text{mult}(PQ, \lambda) = m + n$. ■

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

- **Initialisation.** λ_1 est racine de P de multiplicité m_1, ainsi $(X-\lambda_1)^{m_1}$ divise P.
- **Hérédité.** Soit $k \in [\![1, r-1]\!]$ et supposons que $(X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k}$ divise P. Il existe donc $A \in \mathbb{K}[X]$ tel que $P = (X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k} A$.
  Notons α la multiplicité de λ_{k+1} dans A, il existe alors $B \in \mathbb{K}[X]$ tel que $A = (X-\lambda_{k+1})^\alpha B$ et $B(\lambda_{k+1}) \neq 0$. Alors
  $$P = (X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k} (X-\lambda_{k+1})^\alpha B$$
  et donc
  $$\begin{aligned} m_{k+1} &= \text{mult}(P, \lambda) \\ &= \text{mult}\left((X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k}, \lambda_{k+1}\right) + \text{mult}\left((X-\lambda_{k+1})^\alpha, \lambda_{k+1}\right) + \text{mult}\left(B, \lambda_{k+1}\right) \\ &= 0 + \alpha + 0. \end{aligned}$$
  Ainsi $\alpha = m_{k+1}$ et donc $(X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k} (X-\lambda_{k+1})^{m_{k+1}}$ divise P.

■

Exemple 51 Le polynôme $(X-1)^4 X^2 (X+2)$ possède en tout trois racines distinctes (1 de multiplicité 4, 0 de multiplicité 2 et -2 de multiplicité 1). On dit en revanche qu'il possède sept *racines comptées avec multiplicité*, puisque $4 + 2 + 1 = 7$.

Corollaire 52 - 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.

Un polynôme de degré n ne possède pas nécessairement n racines comptées avec multiplicité. Nous verrons à la section 4 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 53 Soit $P \in \mathbb{R}[X]$. On suppose que, pour tout $n \in \mathbb{N}$, $P(n) = n^3 - n^2 + 1$. Alors $P = X^3 - X^2 + 1$ et, a fortiori, pour tout $z \in \mathbb{C}$, $P(z) = z^3 - z^2 + 1$.

En effet, le polynôme $P - X^3 + X^2 - 1$ admet, par hypothèse, tout entier naturel pour racine et en possède donc une infinité. Ainsi ce polynôme est nul.

✎ **En pratique** ✎ Comme l'illustre l'exemple précédent, le théorème 52 est un théorème de DÉS-ÉVALUATION. Évaluer consiste à passer d'une égalité polynomiale à une égalité de nombres réels ou complexes. Dés-évaluer, c'est le contraire : remonter d'une collection d'égalités de nombres à une égalité polynomiale. En d'autres termes, lorsqu'un polynôme P est défini par certaines de ses valeurs, il est souvent fructueux d'interpréter cette hypothèse sur les valeurs de P en termes de racines d'un nouveau polynôme Q. Quand ce polynôme Q a trop de racines, il est nécessairement nul et on en tire souvent de précieux renseignement sur P.

Exemple 54 Il n'existe pas de polynôme $P \in \mathbb{R}[X]$ tel que, pour tout $n \in \mathbb{N}$, $P(n) = \sqrt[3]{n^2+1}$.

En effet, supposons par l'absurde qu'un tel polynôme P existe. Le polynôme $P^3 - X^2 - 1$ admet alors une infinité de racines (tous les entiers naturels) et est donc nul, de sorte que $P^3 = X^2 + 1$. En particulier, $3\deg P = 2$, soit $\deg P = \dfrac{2}{3}$, ce qui est absurde.

Exemple 55 Soit $P \in \mathbb{R}[X]$ de degré n et tel que, pour tout $k \in [\![1, n+1]\!]$, $P(k) = \dfrac{1}{k}$. Alors $P(-1) = n + 1$.

En effet, Le polynôme $XP - 1$ admet $n+1$ racines (les éléments de $[\![1, n+1]\!]$), or il est de degré $n+1$, ainsi, il existe $\lambda \in \mathbb{R}^*$ tel que $XP - 1 = \lambda \prod_{k=1}^{n+1}(X - k)$. En évaluant en 0, on obtient alors :

$$-1 = \lambda \prod_{k=1}^{n+1}(-k) \iff \lambda = \frac{(-1)^n}{(n+1)!} \quad \text{et} \quad \text{ainsi} \quad XP = 1 + \frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(X-k).$$

Il reste alors à évaluer en -1 :

$$-P(-1) = 1 + \frac{(-1)^n}{(n+1)!}\prod_{k=1}^{n+1}(-(k+1)) = 1 + \frac{(-1)^n}{(n+1)!} \times (-1)^{n+1}(n+2)! = 1 - (n+2) = -n - 1.$$

Théorème 56 - 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 eux-mêmes, *i.e.* leurs coefficients.

Démonstration. Si $\widetilde{P} = \widetilde{Q}$, alors $\widetilde{P - Q}$ est nulle sur $\mathbb{K}$. Ainsi, tout élément de $\mathbb{K}$ est racine de $P - Q$, or $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$) est infini, $P - Q$ possède donc une infinité de racine et est par conséquent nul. ■

Définition-théorème 57 - Polynôme scindé. Un polynôme $P \in \mathbb{K}[X]$ est dit *scindé (sur $\mathbb{K}$)* lorsqu'il n'est pas constant et possède exactement $\deg P$ racines (dans $\mathbb{K}$) comptées avec multiplicité.

Dire que P est scindé sur $\mathbb{K}$ équivaut donc à dire que P est de la forme $\alpha \prod_{i=1}^{r}(X - \lambda_i)^{m_i}$, où $\lambda_1, \ldots, \lambda_r$ sont les racines distinctes de P dans $\mathbb{K}$, de multiplicités respectives $m_1, \ldots, m_r$, et où α est son coefficient dominant. On a de plus $m_1 = \ldots + m_r = \deg(P)$.

Démonstration. Si P est scindé sur $\mathbb{K}$, alors, en vertu du théorème 49, $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ divise P. Il existe donc $Q \in \mathbb{K}[X]$ tel que $P = Q\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$, or $\deg Q = \deg P - \deg\left(\prod_{i=1}^{r}(X-\lambda_i)^{m_i}\right) = 0$, ainsi $Q \in \mathbb{K}$ et comme $\prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ est unitaire Q est égal au coefficient dominant de P. ■

✖ **Attention !** ✖ La précision « scindé sur $\mathbb{K}$ » n'est pas superflue puisqu'un polynôme peut avoir des racines complexes mais aucune racine réelle, *e.g.* $X^2+1 = (X-i)(X+i)$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$.

Exemple 58 Les polynômes de degré 1 de $\mathbb{K}[X]$ sont scindés.

En effet, P est non constant de la forme $aX+b$, avec $a, b \in \mathbb{K}$ et $a \neq 0$, et admet $-\dfrac{b}{a}$ pour racine dans $\mathbb{K}$.

Exemple 59 Pour tout $n \in \mathbb{N}^*$, le polynôme X^n-1 est scindé sur $\mathbb{C}$. Précisément : $X^n - 1 = \prod_{k=0}^{n-1}\left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right)$.

En effet, le polynôme X^n-1 n'est pas constant et admet au plus n racines, étant de degré n. Or X^n-1 admet les n racines n^{es} de l'unité pour racines distinctes.

4 Factorisation irréductible sur $\mathbb{R}$ ou $\mathbb{C}$

Définition 60 - Polynômes irreductibles. Un polynôme $P \in \mathbb{K}[X]$ non constant est irreductible sur $\mathbb{K}$ lorsque

$$P = AB \text{ avec } (A,B) \in \mathbb{K}[X]^2 \implies A \text{ ou } B \text{ constant.}$$

Autrement dit, un polynôme est irreductible quand il n'a aucun diviseur autre que les polynômes constants et lui-même. Cela vous évoque-t-il quelque chose ?

La question liée est : un polynôme possède-t-il toujours une racine ? Le théorème majeur suivant apporte une réponse affirmative à cette question.

Théorème 61 - d'Alembert-Gauss†. Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine complexe.

Démonstration. Admis ■

✖ **Attention !** ✖ Ce théorème est naturellement faux sur $\mathbb{R}$, *e.g.* le polynôme X^2+1 n'a pas de racine réelle.

Théorème 62 - Factorisation irréductible dans $\mathbb{C}[X]$. Tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$, et les seuls polynômes irreductibles sont de degré 1.

Autrement dit, tout polynôme non constant de $\mathbb{C}[X]$ se factorise en un produit de polynômes de degré 1 qui coïncide avec sa forme scindée. En particulier, cette factorisation, dite *irréductible*, est unique, à l'ordre près des facteurs.

†. Jean Le Rond d'Alembert (1717 à Paris – 1783 à Paris) est un mathématicien, physicien, philosophe et encyclopédiste français qui a notamment dirigé avec Denis Diderot l'édition entre 1751 et 1772 de l'*Encyclopédie ou Dictionnaire raisonné des sciences, des arts et des métiers*, première encyclopédie française.

Johann Carl Friedrich Gauss (1777 à Brunswick – 1855 à Göttingen) est un mathématicien, astronome et physicien allemand, dont la contribution aux mathématiques est extraordinaire.

Démonstration. Procédons par récurrence sur le degré $n \in \mathbb{N}^*$ des éléments non constants de $\mathbb{C}[X]$.

- **Initialisation.** Si $P \in \mathbb{C}[X]$ est de degré 1, il est scindé (cf. 58).
- **Hérédité.** Soit $n \in \mathbb{N}^*$ et supposons que tous les polynômes de $\mathbb{C}[X]$ de degré n sont scindés. Soit $P \in \mathbb{C}[X]$ de degré $n+1$. D'après le théorème de d'Alembert-Gauss, P admet une racine λ dans $\mathbb{C}$, ainsi $X-\lambda$ divise P et il existe donc $Q \in \mathbb{C}[X]$ tel que $P = (X-\lambda)Q$. Or $\deg Q = \deg P - \deg(X-\lambda) = n$, ainsi Q est scindé par hypothèse de récurrence, *i.e.* de la forme $\alpha \prod_{i=1}^{n}(X-\lambda_i)$, où $\lambda_1, \dots, \lambda_n$ sont les n racines de Q dans $\mathbb{C}$ et α est son coefficient dominant. Alors $P = \alpha \prod_{i=1}^{n+1}(X-\lambda_i)$, avec $\lambda_{n+1} = \lambda$, admet exactement $n+1$ racines dans $\mathbb{C}$, donc est scindé.

■

✎ **En pratique** ✎ Factoriser un polynôme de $\mathbb{C}[X]$ revient à déterminer ses racines dans $\mathbb{C}$.

Théorème 63 - Factorisation irréductible dans $\mathbb{R}[X]$. Les polynômes non constants irreductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les trinômes de discriminant strictement négatif.
De plus, tout polynôme non constant admet la *factorisation irréductible* de P suivante :

$$P = \alpha \prod_{i=1}^{r}(X-\lambda_i)^{m_i} \times \prod_{j=1}^{s}\left(X^2+b_jX+c_j\right)^{n_j},$$

avec

- α le coefficient dominant de P ;
- $\lambda_1, \dots, \lambda_r$ les racines réelles distinctes de P, de multiplicités respectives $m_1, \dots, m_r$;
- $X^2+b_jX+c_j$ des polynômes de discriminant strictement négatif, pour tout $j \in [\![1\,,s]\!]$, distincts, et $n_j \in \mathbb{N}^*$.

Cette factorisation est unique à l'ordre près des facteurs.

Démonstration. Soit $P \in \mathbb{R}[X]$ non constant. P est scindé sur $\mathbb{C}$ et, puisqu'il est à coefficients réels, ses racines non réelles peuvent être regroupées par paires de conjuguées de mêmes multiplicités (théorème 46). Or le regroupement de deux facteurs $X-\lambda$ et $X-\overline{\lambda}$ donne un facteur $X^2 - 2\operatorname{Re}(\lambda)X + |\lambda|^2$, de discriminant strictement négatif. Enfin cette factorisation sur $\mathbb{R}$ est unique, car dans le cas contraire P aurait plusieurs formes scindées sur $\mathbb{C}$, ce qui est exclu. ■

✎ **En pratique** ✎ La factorisation irréductible sur $\mathbb{R}$ d'un polynôme de $\mathbb{R}[X]$ se déduit de sa forme scindée sur $\mathbb{C}$ par regroupement des racines non réelles par paires de conjuguées.

Exemple 64 Factoriser les polynômes suivants sur $\mathbb{C}[X]$ et $\mathbb{R}[X]$:

1. X^3-1. **2.** X^4-1. **3.** X^4+1.

Comme on le voit dans le dernier exemple, sur $\mathbb{R}$, avoir des racines et être factorisable n'est pas la même chose, puisque X^4+1 n'a pas de racines sur $\mathbb{R}$, mais n'est pas irreductible !

Exemple 65 Pour factoriser X^5+1 sur $\mathbb{R}$, on commence par le factoriser sur $\mathbb{C}$:

$$X^5+1 = \left(X-\mathrm{e}^{i\pi/5}\right)\left(X-\mathrm{e}^{3i\pi/5}\right)(X+1)\left(X-\mathrm{e}^{7i\pi/5}\right)\left(X-\mathrm{e}^{i9\pi/5}\right)$$

puis on regroupe les facteurs conjugués :

$$X^5+1 = (X+1)\left(\left(X-\mathrm{e}^{i\pi/5}\right)\left(X-\mathrm{e}^{i9\pi/5}\right)\right)\left(\left(X-\mathrm{e}^{3i\pi/5}\right)\left(X-\mathrm{e}^{7i\pi/5}\right)\right) = (X+1)\left(X^2-2\cos\frac{\pi}{5}X+1\right)\left(X^2-2\cos\frac{3\pi}{5}X+1\right).$$

✖ **Attention !** ✖ En dépit des apparences $(X+1)\left(X^2-3X+2\right)^2$ n'est pas la factorisation irréductible de ce polynôme sur $\mathbb{R}$, car $X^2-3X+2 = (X-1)(X-2)$ (ce trinôme n'est pas de discriminant strictement négatif).

Remarque 66 - Factorisation irréductible dans $\mathbb{R}[X]$. Tout comme on peut lire les diviseurs d'un nombre en faisant des combinaisons sur sa décomposition en facteurs premiers, on peut obtenir tout les diviseurs (dans $\mathbb{R}$ ou $\mathbb{C}$ d'un polynôme sur sa décomposition en facteurs irreductibles.
Ce point n'est pas vraiment au programme mais est d'application facile.

Somme et produit des racines On généralise les relations "somme et produit" des racines d'un polynôme de degré 2 vues au chapitre 4.

Proposition 67 - Somme et produit d'un polynôme scindé. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé sur $\mathbb{K}$ de degré n. Alors

- La somme des racines de P comptées avec multiplicités vaut $-\frac{a_{n-1}}{a_n}$.
- Le produit des racines de P comptées avec multiplicités vaut $(-1)^n \frac{a_0}{a_n}$.

Si on note s cette somme et p ce produit, dans le cas d'un polynôme de degré 2 unitaire scindé sur $\mathbb{K}$, on retrouve son expression $X^2 - sX + p$.

Exemple 68 Déterminer des racines entières évidentes (si c'est possible) pour les polynômes suivants, et essayer de les factoriser :

1. $X^3 - 6X^2 - 13X + 42$. **2.** $X^3 - 6X^2 + 12X - 8$. **3.** $X^2 - 8X + 6$ (on verra qu'il n'y a pas de racines entières).

5 Décomposition en éléments simples

Il s'agit d'une nouvelle technique de calcul algébrique qui permet de « développer » des fractions de polynômes, en particulier utile pour le calcul de primitives. Ne la tentez pas pour des fractions d'un autre type !

Vous avez déjà vu les tours de magie suivants :

$$\frac{x+1}{x-1} = 1 + \frac{2}{x-1} \quad \text{et} \quad \frac{1}{1-x^2} = \frac{1}{1+x} + \frac{1}{1-x},$$

clairs en mettant au même dénominateur, mais que vous n'auriez pas trouvés seuls. On va voir dans cette section comment devenir magicien soit même.

5.1 Les fractions rationnelles et leurs décompositions

Définition 69 On appelle fraction rationnelle une fonction de $\mathbb{R}$ dans $\mathbb{K}$ de la forme

$$F : x \mapsto \frac{P(x)}{Q(x)},$$

où P et Q sont deux polynômes à coefficients dans $\mathbb{K}$. On suppose que cette écriture est irreductible, c'est-à-dire que P et Q n'ont pas de facteurs communs dans leur décompositions en facteurs irreductibles (sinon, on simplifie la fraction).
Notons $\mathcal{R}$ les racines de Q, alors la fonction F est bien définie sur $\mathbb{R}\backslash\mathcal{R}$, et $\mathcal{R}$ est appelé l'ensemble des *pôles* de F (sur $\mathbb{K}$). La multiplicité d'un pôle est sa multiplicité en tant que racine de Q.
On définit le degré de F comme l'entier $\deg(P) - \deg(Q)$. Il peut être négatif !

Exemple 70 Voici des fractions rationnelles, écrites à l'aide d'une indeterminée. Quelles sont leurs pôles (sur $\mathbb{R}$, et sur $\mathbb{C}$), et leurs multiplicités ? Et le degré des fraction rationnelles ?

1. $\frac{2X+3}{X^2+1}$. **2.** $\frac{X^2}{(X-3)(X+1)}$. **3.** $\frac{X^5}{(X^2+X+1)(X-2)^2}$.

Proposition 71 Soit $F = \frac{P}{Q}$ une fraction rationnelle, alors il existe des polynômes E et P_1, uniques, tels que

$$F = E + \frac{P_1}{Q} \quad \text{avec } \deg(P_1) < \deg(Q).$$

De plus, E et P_1 sont le dividande et le reste de la division euclidienne de P par Q.

Ainsi on peux toujours se ramener à l'étude d'une fraction rationnelle avec un dénominateur de plus grand degré que le numérateur.

5.2 Forme des éléments simples

Le cas des poles simples Une racine ou un pôle est dit simple quand sa multiplicité vaut 1.

Voici le résultats à savoir :

Théorème 72 Soit $F = \frac{P}{Q}$ une fraction rationnelle, avec $\deg P < \deg Q$ (on peut toujours se ramener à ce cas avec la proposition précédente). Supposons que Q est scindé à racines simples, c'est à dire que F est de la forme

$$F = \frac{P}{\prod_{k=1}^{n}(X - \alpha_k)}$$

avec $(\alpha_k)_{k=1,\dots,n}$ des réels distincts deux à deux. Alors il existe des coefficients $(c_1, \dots, c_n)$ dans $\mathbb{K}$ tels que

$$F = \sum_{k=1}^{n} \frac{c_k}{X - \alpha_k} = \frac{c_1}{X - \alpha_1} + \dots + \frac{c_n}{X - \alpha_n}.$$

Les coefficients $(a_k)_{k=1,\dots,n}$ peuvent se calculer explicitement :

- On peut multiplier le tout par $(X - \alpha_k)$ et évaluer en α_k.
- On a la formule $c_k = \frac{P(\alpha_k)}{Q'(\alpha_k)}$.

Exemple 73 Décomposer en éléments simples les fractions rationnelles suivantes, et donner des primitives des fonctions associées.

1. $\frac{1}{X(X-1)(X+1)}$. **2.** $\frac{X^2}{(X-2)(X+1)}$ (division euclidienne déconseillée). **3.** $\frac{X^3}{(X+1)(X+3)}$ (division euclidienne conseillée).

Et pour d'autres facteurs au dénominateurs Le pogramme est clair : pour décomposer une fraction $\frac{P}{Q}$ où Q n'est pas scindé à racines simples, la forme de la décomposition doit être suggérée. Il vaut tout de même mieux avoir déjà vue les formes possibles, surtout que les techniques qui vont avec sont à savoir !

L'idée générale est facile : chaque facteur dans Q va créer un ou plusieurs termes dans la décomposition de $\frac{P}{Q}$. Voici les formes possibles

- Un facteur de la forme $(X - \alpha)$, avec α une racine de Q, va créer un terme de la forme $\frac{c}{X-\alpha}$. C'est le cas déjà vu, et les méthodes pour déterminer c restent d'actualité.
- Un facteur de la forme $(X^2 + \beta x + \gamma)$, irreductible, (donc de discriminant strictement négatif) va créer un terme de la forme $\frac{bX+c}{X^2+\beta x+\gamma}$. Il faudra trouver b et c (voir les techniques ci-dessous).
- Un facteur de la forme $(X - \alpha)^m$ avec $m \geqslant 2$ (pôle multiple), va créer plusieurs termes de la forme $\frac{\alpha_r}{(X-\alpha)^r}$, avec $1 \leqslant r \leqslant m$ et $\alpha_r \in \mathbb{K}$. C'est un cas difficile, il faudra trouver les coefficients α_r.
- Un facteur de la forme $(X^2 + \beta x + \gamma)^m$, où le trinôme $X^2 + \beta x + \gamma$ est irreductible, est éloigné du programme. Ils combinent les techniques des deux points précédents.

5.3 Les techniques de calculs

Voici maintenant les techniques générales, à adapter selon vos envies :

Multiplier par un facteur et évaluer Pour un facteur $X-\alpha$, on a déjà vu comment faire. S'il y a un facteur $(X-\alpha)^m$, ce facteur va générer des termes $\frac{a_1}{X-\alpha}+\ldots+\frac{a_m}{(X-\alpha)^m}$. Cette technique marche encore en multipliant par $(X-\alpha)^m$, pour obtenir le terme a_m.

Exemple 74 On cherche a et b tels que

$$\frac{X}{(X-1)^2(X+1)}=\frac{a_1}{X-1}+\frac{a_2}{(X-1)^2}+\frac{b}{X+1}.$$

Trouver avec la méthode a_2 et b. Il reste à trouver a_1 !

Pour un facteur de degré 2 de la forme $(X^2+\beta x+\gamma)$ on peut passer dans le complexes, soit en le factorisant dans le complexe pour faire apparaître des facteurs de degré 1 et appliquer la méthode (mais il faut au final repasser dans le réel), soit en multipliant par $(X^2+\beta x+\gamma)$ et en évaluant en une racine complexe du trinôme. Dans tous les cas, cette méthode demande un calcul de racines.

Exemple 75 On cherche a, b et c tels que

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

Montrer que $bi+c=\frac{1}{i-1}$, en déduire b et c.

Comme on le voit, cette méthode donne deux coefficients d'un coup ! et oui, une égalité de complexes c'est bien deux égalités de réels.

Analyse asymptotique en $+\infty$ De manière générale, on peut multiplier par des puissances de X bien choisies et faire tendre X vers $+\infty$. Cela donne des relations entre vos inconnues, et permet quoiqu'il arrive de diminuer le nombre de calculs à faire (ou de les vérifier).

Exemple 76

1. On cherche a et b tels que
$$\frac{X}{(X-1)(X+1)}=\frac{a}{X-1}+\frac{b}{X+1}.$$
Montrer, sans calculer a et b, que $a+b=1$. Calculer a et b.
2. On cherche a, b et c tels que
$$\frac{1}{(X-1)(X^2+X+1)}=\frac{a}{X-1}+\frac{bX+c}{X^2+X+1}.$$
Montrer, sans calculer les autres coefficients, que $a+b=0$, en déduire a et b. Il reste à trouver c !

Evaluer en une valeur (qui n'est un pôle) Cette méthode vous donne une relation entres les coefficients. Pratique si on a déjà bien travaillé.

Exemple 77

1. On cherche a et b tels que
$$\frac{1}{(X-1)(X^2+X+1)}=\frac{a}{X-1}+\frac{bX+c}{X^2+X+1}.$$
On a déjà a et b. Déduire c en évaluant en 0.

Jouer sur la parité, quand c'est possible On écrit la forme cherchée en remplaçant X par $-X$ et on joue sur l'unicité.

Exemple 78 On cherche a, b et c tels que

$$\frac{1}{X^2(X^2+1)}=\frac{a_1}{X}+\frac{a_2}{X^2}+\frac{bX+c}{X^2+1}.$$

En jouant sur la parité, montrer que $a_1=b=0$. Trouver les autres coefficients.

Cette méthode ne marche pas si il y a des facteurs qui n'ont aucune parité !

Mettre au même dénominateur et identifier c'est la méthode bourrin, quand on n'a plus rien en tête. On peut la faire dès le début, mais on obtient un système linéaire, qui induit souvent des erreurs de calculs.