
1	Polynômes à travers leurs coefficients.	2
1.1	Combinaisons linéaires et produits de polynômes formels.	2
1.2	Évaluation d'un polynôme.	4
1.3	Structure d'anneau de $\mathbb{K}[X]$	5
1.4	Composition.	7
1.5	Degré.	7
1.6	Dérivation dans $\mathbb{K}[X]$	10
2	Racines et factorisation d'un polynôme.	13
2.1	Divisibilité et division euclidienne dans $\mathbb{K}[X]$	13
2.2	Racines et divisibilité.	15
2.3	Racines et rigidité des polynômes.	16
2.4	Multiplicité d'une racine.	17
2.5	Existence de racines : théorème de d'Alembert-Gauss.	18
2.6	Décomposition en facteurs irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$	19
3	Compléments.	20
3.1	Relations coefficients-racines pour un polynôme scindé.	20
3.2	Interpolation de Lagrange.	22
	Exercices	23

Introduction.

On appelle **fonction polynomiale** une fonction définie sur \mathbb{R} , de la forme

$$P : x \mapsto \sum_{k=0}^n a_k x^k,$$

où $n \in \mathbb{N}$ et a_0, a_1, \dots, a_n sont des réels.

On fait quelques remarques liminaires sur

- La suite de coefficients associés à une fonction polynomiale.
- La somme et le produit de deux fonctions polynomiales.
- Racines et factorisation d'un trinôme.

Le lien entre racines et factorisation sera étendu aux polynômes de degré quelconque : après avoir manipulé les polynômes comme des sommes en partie 1, nous les factoriserons en partie 2 en nous appuyant sur la notion de racines.

1 Polynômes à travers leurs coefficients.

1.1 Combinaisons linéaires et produits de polynômes formels.

Définition 1.

On appelle **polynôme** à coefficients dans \mathbb{K} une suite d'éléments de \mathbb{K} nulle à.p.d.c.r.

L'ensemble des **polynômes** à coefficients dans \mathbb{K} sera noté $\mathbb{K}[X]$.

- La suite nulle est un polynôme. Il est appelé **polynôme nul** et noté 0, ou $0_{\mathbb{K}[X]}$.
- La suite $(1, 0, 0, 0, \dots)$ est un polynôme. Il est appelé polynôme constant égal à 1 et noté 1.
- La suite $(0, 1, 0, 0, \dots)$ est un polynôme. Il est noté X et appelé **indéterminée**.
- Soit $n \in \mathbb{N}$. La suite dont tous les termes sont nuls sauf celui au rang n qui vaut 1 est un polynôme que l'on notera X^n . On l'appelle **monôme** d'ordre n :

$$X^n = (0, 0, \dots, 0, \underbrace{1}_{\text{rang } n}, 0, 0, \dots).$$

Proposition-Définition 2 (Somme de polynômes et multiplication par un scalaire).

Soient $P = (a_k)_{k \in \mathbb{N}}$ et $Q = (b_k)_{k \in \mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$.

La suite $(a_k + b_k)_{k \in \mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$, qui sera noté $P + Q$.

La suite $(\lambda a_k)_{k \in \mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$, qui sera $\lambda \cdot P$ ou plus simplement λP .

On verra au second semestre que $(\mathbb{K}[X], +, \cdot)$ est un \mathbb{K} -espace vectoriel. Ainsi, pour ce qui concerne les combinaisons linéaires, on utilise les mêmes règles de calcul que dans $(M_{n,p}(\mathbb{K}), +, \cdot)$. On ne les démontre pas ici (on ne les énonce même pas!) dans le but d'alléger l'exposé.

Corollaire 3.

Soit $P = (a_k)_{k \in \mathbb{N}}$ un polynôme de $\mathbb{K}[X]$ et m un entier tel que $\forall k > m \ a_k = 0$. Alors,

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

Preuve. On a

$$\begin{aligned} P &= (a_0, a_1, a_2, \dots, a_m, 0, 0, 0, \dots) \\ &= a_0(1, 0, 0, 0, \dots) + a_1(0, 1, 0, 0, \dots) + a_2(0, 0, 1, 0, 0, \dots) + \dots + a_m(0, 0, \dots, 0, \underbrace{1}_{\text{rang } m}, 0, 0, \dots) \\ &= a_0 1 + a_1 X + a_2 X^2 + \dots + a_m X^m \\ &= \sum_{k=0}^m a_k X^k. \end{aligned}$$

□

Notation.

Un polynôme $P = (a_k)_{k \in \mathbb{N}}$ de $\mathbb{K}[X]$ sera désormais noté

$$P = \sum a_k X^k.$$

Il s'agit juste d'une notation, qui permet d'oublier que les polynômes, formellement, sont des suites (on n'a pas besoin de savoir cela dans la pratique).

On peut aussi noter $P = \sum_{k \in \mathbb{N}} a_k X^k$ et lire cela comme une vraie somme (finie) puisque a est nulle à partir d'un certain rang.

Remarque. Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$. Par définition, les polynômes P et Q sont égaux si et seulement si les suites P et Q sont égales. Cela permettra « d'identifier le coefficient devant X^k ». Ainsi,

$$\sum a_k X^k = \sum b_k X^k \iff \forall k \in \mathbb{N} \quad a_k = b_k.$$

Corollaire 4.

Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes de $\mathbb{K}[X]$ et (λ, μ) deux scalaires de \mathbb{K} . On a

$$\lambda P + \mu Q = \sum (\lambda a_k + \mu b_k) X^k.$$

Preuve. C'est juste la définition : $\lambda P + \mu Q$ est la suite $(\lambda a_k + \mu b_k)_{k \in \mathbb{N}}$ et nous venons de décider de noter un tel polynôme $\sum (\lambda a_k + \mu b_k) X^k$. □

Proposition-Définition 5 (Produit de deux polynômes).

Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes de $\mathbb{K}[X]$.

Soit $(c_k)_{k \geq 0}$ la suite définie pour tout $k \in \mathbb{N}$ par

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

La suite c est un polynôme : on l'appelle **produit** de P et Q , noté $P \times Q$, ou encore PQ :

$$\left(\sum_{k \in \mathbb{N}} a_k X^k \right) \left(\sum_{k \in \mathbb{N}} b_k X^k \right) = \sum_{k \in \mathbb{N}} \left(\sum_{i=0}^k a_i b_{k-i} \right) X^k.$$

Preuve. Soient deux polynômes $P = (a_k)_{k \in \mathbb{N}}$ et $Q = (b_k)_{k \in \mathbb{N}}$. Ces suites sont nulles à.p.d.c.r. : il existe deux entiers p et q tels que

$$\begin{cases} \forall k > p \quad a_k = 0 \\ \forall k > q \quad b_k = 0 \end{cases}$$

On affirme ici que

$$\forall k > p + q \quad c_k = 0.$$

Ceci sera démontré dans la preuve de la proposition 20. □

1.2 Évaluation d'un polynôme.

Définition 6 (où l'on retrouve les fonctions polynomiales).

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$.

Pour $\alpha \in \mathbb{K}$, on appelle **évaluation** de P en α , et on note $P(\alpha)$ le nombre

$$P(\alpha) = \sum_{k=0}^{+\infty} a_k \alpha^k \quad (P \in \mathbb{K}[X] \text{ et } P(\alpha) \in \mathbb{K});$$

La somme précédente est *finie* puisque la suite (a_n) est par définition nulle à.p.d.c.r.

On parlera de $\tilde{P} : x \mapsto P(x)$ comme de la **fonction polynomiale associée** au polynôme P .

Exemples 7.

1. Soit $P = X^3 - 3X + 4$. Évaluer P en 2 et -1 .
2. Quelle est la fonction polynomiale associée à $X^2 - 1$? à X ?

Proposition 8 (opérations et évaluation).

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

$$(\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x), \quad \text{et} \quad (PQ)(x) = P(x) \cdot Q(x).$$

Exemple 9 (Méthode de Horner).

Soit $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$, et $P = \sum_{k=0}^n a_k X^k$. Soit $\alpha \in \mathbb{K}$. On peut calculer $P(\alpha)$ ainsi :

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

Le nombre d'opérations à effectuer est un $O(n)$.

Définition 10.

Soit $P \in \mathbb{K}[X]$. Une **racine** (ou un zéro) de P dans \mathbb{K} est un nombre $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

Exemple 11.

Donner une racine réelle de $P = X^5 - X^4 + X^3 - X^2 + X - 1$.

Donner les racines de $X^5 - 1$ dans \mathbb{C} .

Dans la seconde moitié du cours, la notion de racine jouera un rôle clé dans la factorisation des polynômes.

1.3 Structure d'anneau de $\mathbb{K}[X]$.

Théorème 12.

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Preuve (HP).

Pour ne pas avoir à introduire des coefficients pour chaque polynôme ci-dessous, on convient de noter $[A]_k$, pour $k \in \mathbb{N}$ le coefficient d'ordre k d'un polynôme A . Dans toute la suite, k est un entier naturel fixé.

On se donne pour les calculs ci-dessous P, Q, R trois polynômes de $\mathbb{K}[X]$.

1) $(\mathbb{K}[X], +)$ est un groupe abélien, de neutre le polynôme nul.

Il est assez facile de vérifier, en effet, qu'il s'agit d'un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$, groupe abélien connu.

2) La loi \times est une loi de composition interne sur $\mathbb{K}[X]$, cela a été établi par la proposition 5.

3) La loi \times est commutative.

$$[PQ]_k = \sum_{i=0}^k [P]_i [Q]_{k-i} = \sum_{j=k-i}^k [P]_{k-j} [Q]_j = \sum_{i=0}^k [Q]_i [P]_{k-i} = [QP]_k.$$

4) Le polynôme $1 (= 1_{\mathbb{K}[X]})$ est neutre pour le produit.

Rappelons la définition du *symbole de Kronecker*, défini pour i et j entiers par

$$\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

Le polynôme constant égal à 1 a tous ses coefficients nuls sauf celui d'ordre 0 qui vaut 1. Pour tout $i \in \mathbb{N}$, on a donc

$$[1_{\mathbb{K}[X]}]_i = \delta_{i,0}.$$

On calcule alors

$$[1_{\mathbb{K}[X]} \cdot P]_k \underset{3)}{=} [P \cdot 1_{\mathbb{K}[X]}]_k = \sum_{i=0}^k [P]_i \cdot [1_{\mathbb{K}[X]}]_{k-i} = \sum_{i=0}^k [P]_i \cdot \delta_{0,k-i} = 0 + [P]_k \cdot 1 = [P]_k.$$

5) Associativité. En écrivant de deux façons une somme triangulaire

$$\begin{aligned} [(PQ)R]_k &= \sum_{i=0}^k [PQ]_i [R]_{k-i} = \sum_{i=0}^k \left(\sum_{j=0}^i [P]_j [Q]_{i-j} \right) [R]_{k-i} \\ &= \sum_{j=0}^k [P]_j \left(\sum_{i=j}^k [Q]_{i-j} [R]_{k-i} \right) \\ &\underset{l=i-j}{=} \sum_{j=0}^k [P]_j \left(\sum_{l=0}^{k-j} [Q]_l [R]_{k-j-l} \right) \\ &= \sum_{j=0}^k [P]_j [QR]_{k-j} = [P(QR)]_k. \end{aligned}$$

6) Distributivité.

$$[P(Q+R)]_k = \sum_{i=0}^k [P]_i [Q+R]_{k-i} = \sum_{i=0}^k [P]_i ([Q]_{k-i} + [R]_{k-i}) = \sum_{i=0}^k [P]_i [Q]_{k-i} + \sum_{i=0}^k [P]_i [R]_{k-i} = [PQ]_k + [PR]_k.$$

□

Proposition 13 (Cohérence de la notation X^n).

Pour tout $n \in \mathbb{N}$, le polynôme X^n est bien le n ème itéré de X .

Preuve. (HP)

- Le polynôme X^0 est la suite $(1, 0, \dots)$: c'est bien le polynôme 1, par définition.
- Soit $n \in \mathbb{N}$. Vérifions que $X^{n+1} = X \times X^n$. Par définition, X^n est la suite dont tous les termes sont nuls saufs celui au rang n qui vaut 1. Ceci s'écrit

$$\forall k \in \mathbb{N} \quad [X^n]_k = \delta_{k,n}.$$

Fixons k et calculons le coefficient d'ordre k pour $X \times X^n$:

$$[X \times X^n]_k = \sum_{i=0}^k [X]_i [X^n]_{k-i} = \sum_{i=0}^k \delta_{i,1} \delta_{k-i,n}.$$

Le terme $\delta_{i,1} \delta_{k-i,n}$ est nul sauf si $i = 1$ et $k-i = n$, c'est-à-dire si $k = n+1$ et $i = 1$. Ainsi,

$$[X \times X^n]_k = \begin{cases} 0 & \text{si } k \neq n+1 \\ \delta_{1,1} \delta_{n,n} = 1 & \text{si } k = n+1 \end{cases}$$

On a bien $[X \times X^n]_k = \delta_{k,n+1} = [X^{n+1}]_k$, et ce pour tout k . On a bien vérifié que les polynômes $X \times X^n$ et X^{n+1} ont mêmes coefficients : ils sont égaux. \square

Comme dans tout anneau commutatif, il est possible d'écrire des identités remarquables dans $\mathbb{K}[X]$, notamment le binôme.

Exemple 14.

Dans la pratique, on calcule en se ramenant à faire des produits de monômes X^k comme on le faisait avec les fonctions polynomiales.

- Développer $(X^3 + 3)(X^4 - 5X^2 + X)$.
- À l'aide d'identités remarquables, factoriser $1 + X^4 + X^8$.

Exemple 15 (Formule de Vandermonde).

Soient $(p, q, n) \in \mathbb{N}^3$. En considérant $(X+1)^p(X+1)^q$, montrer que

$$\sum_{k=0}^n \binom{p}{k} \binom{q}{n-k} = \binom{p+q}{n}.$$

En particulier,

$$\binom{2n}{n} = \sum_{k=0}^n \binom{n}{k}^2.$$

Remarque.

Pour ce qui concerne les règles de calcul lorsqu'il y a un produit de polynômes et une multiplication par un scalaire en jeu, ce sont les mêmes que dans $M_n(\mathbb{K})$ et on a fait le choix de ne pas les énoncer ici pour alléger l'exposé. Par exemple, si λ est un scalaire, P un polynôme et n un entier naturel, on a $(\lambda P)^n = \lambda^n P^n$.

1.4 Composition.

Définition 16.

Soient deux polynômes $P = \sum a_k X^k$ et Q . Leur **composée** $P \circ Q$ est définie par

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

La somme ci-dessus a un nombre fini de termes non nuls, la suite $(a_k)_{k \in \mathbb{N}}$ étant nulle à.p.d.c.r.

Exemple : Calcul de $P \circ Q$ et $Q \circ P$ avec $P = 1 + X^2$ et $Q = 2 - X$.

Remarques.

1. On vérifiera que $X \circ P = P$ et que $P \circ X = P$. Cette dernière égalité explique que l'on écrit parfois $P(X)$ à la place de P . De la même façon, on écrira $P(X^2)$ ou $P(Q(X))$ pour désigner respectivement les polynômes $P \circ X^2$ et $P \circ Q$.
2. L'écriture $P(X + 1)$ peut alors prêter à confusion : s'agit-il de $P \circ (X + 1)$ ou de $P \times (X + 1)$? La bonne réponse, c'est la composition : pour le produit, on préférera l'écriture $(X + 1)P$.

1.5 Degré.

Définition 17.

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$, **non nul**.

On appelle **degré** de P , et on note $\deg(P)$ l'indice du dernier coefficient non nul de P :

$$\deg(P) = \max \{k \in \mathbb{N} : a_k \neq 0\}.$$

Par ailleurs, on pose $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Proposition-Définition 18.

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$ et $d \in \mathbb{N}$.

$$\deg(P) = d \iff \left(P = a_d X^d + \sum_{k=0}^{d-1} a_k X^k \text{ et } a_d \neq 0 \right).$$

Si P est un polynôme non nul de degré $d \in \mathbb{N}$, alors a_d est appelé **coefficient dominant** de P . Si ce coefficient vaut 1, le polynôme P est dit **unitaire**.

Que dire, en particulier, des polynômes de degré 0 ? Un polynôme $P = \sum a_k X^k$ est de degré 0 si et seulement si il s'écrit $P = a_0 \cdot 1_{\mathbb{K}[X]}$, avec $a_0 \neq 0$. Ainsi, les polynômes de degré 0 sont exactement les polynômes constants non nuls (les multiples scalaires du polynôme 1).

Exemple 19.

Soit $n \in \mathbb{N}^*$ et $P = (X + 2)^n - (X + 1)^n$. Calculer le degré de P et son coefficient dominant.

Proposition 20.

Soient $P, Q \in \mathbb{K}[X]$ deux polynômes. On a les résultats suivants :

1. $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$, avec égalité si $\deg(P) \neq \deg(Q)$;
2. $\forall \lambda \in \mathbb{K} \quad \deg(\lambda P) \leq \deg(P)$, avec égalité si $\lambda \neq 0$;
3. $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Complément.

On peut montrer en exercice que pour P et Q deux polynômes (avec $Q \neq 0$),

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

Remarque. Pour que la somme dans 3. ait un sens même lorsque l'un des polynômes est nul, on a convenu que pour $d \in \mathbb{N} \cup \{-\infty\}$, la somme $d + (-\infty)$ vaut $-\infty$. Cela semble assez naturel et explique le choix de $-\infty$ pour le degré du polynôme nul.

Preuve. Fixons dans cette preuve deux polynômes $P = \sum a_k X^k$ et $Q = \sum b_k X^k$.

1) • On traite à part le cas où l'un des deux polynômes est nul (supposons que Q l'est pour fixer les idées). Alors $P + Q = P$ et il est clair que $\deg(P + Q) = \deg(P) = \max(\deg(P), -\infty) = \max(\deg(P), \deg(Q))$.

• Supposons maintenant que P et Q sont non nuls. Leurs degrés sont alors des entiers naturels que l'on note respectivement p et q . On a donc

$$P = \sum_{k=0}^p a_k X^k \quad (\text{avec } a_p \neq 0) \quad \text{et} \quad Q = \sum_{k=0}^q b_k X^k \quad (\text{avec } b_q \neq 0).$$

Notons que les coefficients a_{p+1}, a_{p+2}, \dots ainsi que b_{q+1}, b_{q+2}, \dots existent bien mais sont nuls. En notant $m = \max(p, q)$, et en ajoutant éventuellement des termes nuls, on peut écrire

$$P + Q = \sum_{k=0}^p a_k X^k + \sum_{k=0}^q b_k X^k = \sum_{k=0}^m (a_k + b_k) X^k.$$

Il est clair alors que $\deg(P + Q) \leq m$, ce qu'il fallait démontrer.

Supposons $p \neq q$. Si $p > q$, alors $m = p$ et

$$P + Q = \underset{\neq 0}{(a_p + b_p)} X^p + \sum_{k=0}^{p-1} a_k X^k = \underset{\neq 0}{a_p} X^p + \sum_{k=0}^{p-1} a_k X^k.$$

Si $q > p$, alors $m = q$ et

$$P + Q = \underset{=0}{(a_q + b_q)} X^q + \sum_{k=0}^{q-1} a_k X^k = \underset{\neq 0}{a_q} X^q + \sum_{k=0}^{q-1} a_k X^k.$$

Dans les deux cas, on a bien que le degré de $P + Q$ vaut $m = \max(\deg(P), \deg(Q))$. On a bien vérifié qu'il est *suffisant* que deux polynômes soient de degrés différents pour avoir égalité dans l'inégalité.

2) Soit $\lambda \in \mathbb{K}^*$. Si P est nul, λP l'est aussi : ils ont bien même degré. Supposons que P est non nul et notons p son degré. On a donc $P = \sum_{k=0}^p a_k X^k$, avec $a_p \neq 0$. Ainsi,

$$\lambda P = \underbrace{\lambda a_p}_{\neq 0} X^p + \sum_{k=0}^{p-1} \lambda a_k X^k.$$

On a donc bien $\deg(\lambda P) = p = \deg(P)$.

3) • On traite à part le cas où l'un des deux polynômes est nul. Supposons que Q l'est pour fixer les idées. Alors $PQ = 0$ et $\deg(PQ) = -\infty$. D'autre part,

$$\deg(P) + \deg(Q) = \deg(P) + (-\infty) = -\infty.$$

Pour écrire la dernière égalité, il faut faire la convention naturelle $n + (-\infty) = -\infty = -\infty$ pour tout n entier et $(-\infty) + (-\infty) = -\infty = -\infty$.

• Supposons maintenant que P et Q sont non nuls. Leurs degrés sont alors des entiers naturels que l'on note respectivement p et q . Notons $(c_k)_{k \in \mathbb{N}}$ les coefficients de PQ tels que définis en à la définition 5. Soit $k > p + q$.

$$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^p a_i b_{k-i} + \sum_{i=p+1}^{p+q} a_i b_{k-i}$$

Dans la deuxième somme, tous les a_i sont nuls puisque $i > p$. Dans la première somme, on a

$$k - i > (p + q) - i \geq (p + q) - p = q.$$

Puisque $k - i > q$, $b_{k-i} = 0$. Ceci montre que

$$\forall k > (p + q) \quad c_k = 0.$$

La suite PQ est donc nulle au moins à partir de du rang $p + q + 1$ (c'est bien un polynôme!) et on peut écrire

$$PQ = \sum_{k=0}^{p+q} c_k X^k.$$

Reste à vérifier que c_{p+q} est non nul, ce que l'on fait en calculant

$$c_{p+q} = \sum_{i=0}^{p+q} a_i b_{p+q-i} = \sum_{i=0}^{p-1} a_i b_{p+q-i} + a_p b_q + \sum_{i=p+1}^{p+q} a_i b_{p+q-i}.$$

Dans la deuxième somme, tous les a_i sont nuls car $i > p$. Dans la première, les b_{p+q-i} sont nuls car $p + q - i > q$. Il reste $c_{p+q} = a_p b_q$, qui est bien non nul puisque a_p et b_q le sont. On a bien

$$\deg(PQ) = p + q = \deg(P) + \deg(Q).$$

□

⚠ Dans 1) ci-dessus, l'inégalité peut être stricte :

$$\underbrace{X^3 + X + 1}_{\text{degré 3}} + \underbrace{(-X^3)}_{\text{degré 3}} = \underbrace{X + 1}_{\text{degré 1}}$$

On voit qu'une somme de polynômes de degré 3 n'est pas nécessairement de degré 3. Plus généralement, l'ensemble des polynômes de degré n , pour n donné n'est pas une « bonne » partie de $\mathbb{K}[X]$ car elle n'est pas stable par combinaisons linéaires. En revanche, ce sera le cas de l'ensemble $\mathbb{K}_n[X]$, défini un peu plus loin.

Exemple 21 (Polynômes de Tchebychev.).

Soit $(T_n)_{n \in \mathbb{N}}$ une suite de polynômes définie par

$$T_0 = 1, \quad T_1 = X \quad \forall n \in \mathbb{N} \quad T_{n+2} = 2XT_{n+1} - T_n.$$

1. Calculer T_2, T_3, T_4 et T_5 .
2. Donner pour tout entier n le degré et le coefficient dominant de T_n .
3. Démontrer que pour tout $n \in \mathbb{N}$, et tout $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$.

Corollaire 22.

Pour $n \in \mathbb{N}$, on notera $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} , de degré inférieur ou égal à n . Cet ensemble contient le polynôme nul et est stable par combinaisons linéaires.

On a en particulier

- $\mathbb{K}_0[X] = \{a \cdot 1_{\mathbb{K}[X]}, a \in \mathbb{K}\}.$
- $\mathbb{K}_1[X] = \{aX + b, (a, b) \in \mathbb{K}^2\}.$
- $\mathbb{K}_2[X] = \{aX^2 + bX + c, (a, b, c) \in \mathbb{K}^3\}.$

Corollaire 23.

L'anneau $\mathbb{K}[X]$ est intègre : il est commutatif, et sans diviseurs de zéro :

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

Ainsi pouvons nous « simplifier » par un polynôme non nul :

$$\forall A, B, C \in \mathbb{K}[X] \quad (AB = AC \text{ et } A \neq 0) \implies B = C.$$

Corollaire 24 (Les inversibles de l'anneau des polynômes sont ceux constants non nuls).

$$U(\mathbb{K}[X]) = \mathbb{K}_0[X] \setminus \{0\}.$$

1.6 Dérivation dans $\mathbb{K}[X]$.**Définition 25.**

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$. Le polynôme

$$P' = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k$$

est appelé **polynôme dérivé** de P .

Remarque. Pas besoin de parler de dérivabilité ci-dessus : la définition ci-dessus est une opération purement formelle qui à la suite (a_k) associe la suite $((k+1)a_{k+1})$.

Proposition 26.

Soit $P \in \mathbb{R}[X]$. La fonction polynomiale associée au polynôme dérivé P' est la dérivée de la fonction polynomiale associée à P .

Proposition 27.

$$\forall P \in \mathbb{K}[X] \quad P \text{ est constant} \iff P' = 0_{\mathbb{K}[X]}.$$

Proposition 28 (Degré du polynôme dérivé).

$$\forall P \in \mathbb{K}[X] \quad \deg(P') = \begin{cases} \deg(P)-1 & \text{si } P \text{ n'est pas constant,} \\ -\infty & \text{si } P \text{ est constant.} \end{cases}$$

Proposition 29 (Dérivation et opérations).

Pour tous $P, Q \in \mathbb{K}[X]$, pour tous scalaires $\lambda, \mu \in \mathbb{K}$,

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

$$\forall n \in \mathbb{N} \quad (P^n)' = nP'P^{n-1} \quad \text{et} \quad (P \circ Q)' = Q' \cdot P' \circ Q.$$

Preuve Soient $P = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q = \sum_{k \in \mathbb{N}} b_k X^k$ deux polynômes de $\mathbb{K}[X]$, et $\lambda, \mu \in \mathbb{K}$.

- La preuve de la première égalité est de routine. Fixons un entier naturel k et comparons les coefficients d'ordre k .

$$[(\lambda P + \mu Q)']_k = (k+1)[\lambda P + \mu Q]_{k+1} = (k+1)(\lambda a_{k+1} + \mu b_{k+1}) = \lambda [P']_{k+1} + \mu [Q']_{k+1} = [\lambda P' + \mu Q']_k.$$

- Pour la seconde égalité, on calcule le coefficient d'ordre k du membre de droite :

$$\begin{aligned} [P'Q + PQ']_k &= [P'Q]_k + [PQ']_k \\ &= \sum_{i=0}^k [P']_i [Q]_{k-i} + \sum_{i=0}^k [P]_i [Q']_{k-i} \\ &= \sum_{i=0}^k (i+1)a_{i+1}b_{k-i} + \sum_{i=0}^k a_i(k-i+1)b_{k-i+1} \\ &= \sum_{j=1}^{k+1} j a_j b_{k-j+1} + \sum_{j=0}^k a_j (k-j+1) b_{k-j+1} \quad \begin{cases} \text{première somme : } j = i+1 \\ \text{seconde somme : } i = j \end{cases} \\ &= (k+1)a_{k+1}b_0 + \sum_{j=1}^k (j+k-j+1)a_j b_{k-j+1} + (k+1)a_0 b_{k+1} \\ &= (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j} = (k+1)[(PQ)]_{k+1} = [(PQ)']_k. \end{aligned}$$

- L'identité $(P^n)' = nP'P^{n-1}$ est vraie pour $n = 0$. Supposons qu'elle le soit pour un entier naturel n donné. Alors, en utilisant la formule pour la dérivée d'un produit,

$$(P^{n+1})' = (P \cdot P^n)' = P'P^n + P(P^n)' = P'P^n + P(nP'P^{n-1}) = (n+1)P'P^n,$$

ce qui montre l'identité au rang $n+1$. On conclut grâce au principe de récurrence.

- Notons $P = \sum_{k=0}^n a_k X^k$, où $n \geq \deg(P)$. On a

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

□

Définition 30.

Soit $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}$. On définit la **dérivée k -ème** de P , que l'on note $P^{(k)}$, en posant

$$P^{(0)} = P \quad \text{et} \quad \forall k \geq 1 \quad P^{(k)} = (P^{(k-1)})'.$$

Exemple 31.

$$\forall n, k \in \mathbb{N} \quad \forall a \in \mathbb{K} \quad ((X-a)^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} (X-a)^{n-k} & \text{si } 0 \leq k \leq n \\ 0 & \text{si } k > n \end{cases}$$

Proposition 32 (Linéarité de la dérivée n -ème et formule de Leibniz).

$$\forall (P, Q) \in \mathbb{K}[X] \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall n \in \mathbb{N} \quad (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$$

$$\forall (P, Q) \in \mathbb{K}[X] \quad \forall n \in \mathbb{N} \quad (PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Proposition 33 (Formule de Taylor pour les polynômes).

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

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

Remarque. Soit $P = \sum a_k X^k$. Notons $n = \deg(P)$ (ou 0 si P est nul). D'après la formule de Taylor, $P = \sum_{k=0}^n \frac{P^{(k)}(0)}{k!} X^k$. Par unicité des coefficients, on a que $a_k = \frac{P^{(k)}(0)}{k!}$, et ce pour tout entier k .

2 Racines et factorisation d'un polynôme.

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

Définition 34.

Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que B **divise** A s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B \mid A$.

Exemple 35.

Tous les polynômes divisent le polynôme nul.

Pour $n \in \mathbb{N}^*$, $X - 1$ divise $X^n - 1$:

$$X^n - 1 = (X - 1) \sum_{k=0}^{n-1} X^k, \quad \text{notamment} \quad X^3 - 1 = (X - 1)(X^2 + X + 1).$$

Proposition 36.

Soient deux polynômes A et B de $\mathbb{K}[X]$, A étant non nul. Si B divise A , alors $\deg(B) \leq \deg(A)$.

Proposition-Définition 37.

La relation divise sur $\mathbb{K}[X]$ est réflexive et transitive, mais elle n'est *pas* antisymétrique.

En effet, pour A et B deux polynômes,

$$(A \mid B \text{ et } B \mid A) \iff \exists \lambda \in \mathbb{K}^* \ A = \lambda B.$$

On dit alors que A et B sont **associés**.

Théorème 38.

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

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Exemple 39.

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

L'évaluation (en 1 ou -1 par exemple) permet parfois de détecter une éventuelle erreur de calcul.

Preuve.

- Unicité. Preuve en classe.

- Existence. On va raisonner par récurrence sur le degré du polynôme à diviser. Pour cela, fixons pour toute la preuve un polynôme B non nul, et notons p son degré qui est donc un entier naturel.

Pour $n \in \mathbb{N}$, on note

$\mathcal{P}(n)$ « Pour tout polynôme A de $\mathbb{K}_n[X]$ il existe un couple de polynômes (Q, R) tel que $A = BQ + R$ et $\deg(R) < \deg(B)$. »

- ★ Initialisation. Soit A un polynôme de $\mathbb{K}_0[X]$, c'est-à-dire un polynôme constant. On peut écrire $A = a_0 \cdot 1$. Deux cas se présentent. Si B est constant, alors on peut écrire $B = b_0 \cdot 1$, avec $b_0 \neq 0$ puisque B n'est pas nul. On écrit alors

$$a_0 \cdot 1 = \frac{a_0}{b_0} 1 \cdot b_0 1 + 0_{\mathbb{K}[X]}.$$

Cette division convient puisque le degré du reste $(-\infty)$ est strictement inférieur au degré de B (nul). Si B n'est pas constant, alors écrivons

$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$

De plus le degré du reste vaut $\deg(A) = 0 < \deg(B)$ (puisque B est non constant dans ce cas).

- ★ Hérédité. Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$. Pour démontrer $\mathcal{P}(n+1)$ prenons A dans $\mathbb{K}_{n+1}[X]$. Si A est de degré inférieur à n , $\mathcal{P}(n)$ s'applique et nous donne l'existence d'un couple quotient reste comme il faut. Supposons dorénavant que A est de degré $n+1$.

◇ Si le degré de B , noté p , satisfait $p > n+1$, alors il suffit de poser

$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$

Le reste vaut A et on a bien $\deg(A) = n+1 < p = \deg(B)$.

◇ Si $p \leq n+1$.

On peut écrire A et B sous la forme

$$\begin{aligned} A &= a_{n+1}X^{n+1} + \tilde{A} && \text{avec } a_{n+1} \neq 0 \quad \text{et } \deg(\tilde{A}) \leq n. \\ B &= b_pX^p + \tilde{B} && \text{avec } b_p \neq 0 \quad \text{et } \deg(\tilde{B}) \leq p-1. \end{aligned}$$

On "commence" alors une division par B en s'occupant d'abord du terme de plus haut degré de A :

$$\begin{aligned} A &= (b_pX^p + \tilde{B}) \cdot \frac{a_{n+1}}{b_p}X^{n+1-p} - \frac{a_{n+1}}{b_p}X^{n+1-p}\tilde{B} + \tilde{A} \\ &= B \cdot \frac{a_{n+1}}{b_p}X^{n+1-p} + C, \end{aligned}$$

où $C = \tilde{A} - \frac{a_{n+1}}{b_p}X^{n+1-p}\tilde{B}$. Le polynôme C est un polynôme de $\mathbb{K}_n[X]$, comme démontré par le calcul suivant :

$$\begin{aligned} \deg(C) &\leq \max \left[\underbrace{\deg(\tilde{A})}_{\leq n}, \deg \left(\frac{a_{n+1}}{b_p}X^{n+1-p}\tilde{B} \right) \right] \leq \max \left(n, (n+1-p) + \underbrace{\deg(\tilde{B})}_{\leq p-1} \right) \\ &\leq \max(n, n) = n. \end{aligned}$$

D'après $\mathcal{P}(n)$, il existe deux polynômes $(\tilde{Q}$ et $\tilde{R})$ tels que $C = B\tilde{Q} + \tilde{R}$ avec $\deg(\tilde{R}) < \deg(B)$. Réinjectons dans la division de A par B commencée plus haut :

$$A = B \cdot \frac{a_{n+1}}{b_p}X^{n+1-p} + B\tilde{Q} + \tilde{R} = B \left(\frac{a_{n+1}}{b_p}X^{n+1-p} + \tilde{Q} \right) + \tilde{R}.$$

On a bien ici une écriture du type $A = BQ + R$ avec $\deg(R) < \deg(B)$: $\mathcal{P}(n+1)$ est démontrée.

- ★ Conclusion. D'après le principe de récurrence, l'existence du couple quotient-reste est établie lorsque $A \in \mathbb{K}_n[X]$ et ce pour tout $n \in \mathbb{N}$. Puisque $\mathbb{K}[X] = \bigcup_{n=0}^{+\infty} \mathbb{K}_n[X]$, l'existence est établie pour tout polynôme A . \square

Corollaire 40.

Soit $(A, B) \in \mathbb{K}[X]^2$, avec $B \neq 0$.

On a que B divise A ssi le reste dans la division euclidienne de A par B est le polynôme nul.

Exemple 41 (juste le reste).

Soit $\theta \in \mathbb{R}$ et $n \geq 2$.

Déterminer le reste dans la division euclidienne de $(\sin \theta X + \cos \theta)^n$ par $X^2 + 1$.

Prouver qu'il n'existe aucune valeur de θ ni de n pour lesquelles $X^2 + 1$ divise $(\sin \theta X + \cos \theta)^n$.

2.2 Racines et divisibilité.**Définition 42** (bis).

Soit $P \in \mathbb{K}[X]$. Une **racine** (ou un zéro) de P dans \mathbb{K} est un nombre $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

La caractérisation suivante est le pivot de ce cours : elle fait le lien entre la notion de racine d'un polynôme et celle de divisibilité par un polynôme de degré 1.

Théorème 43 (Racine et divisibilité par un polynôme de degré 1).

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Il y a équivalence entre les deux assertions suivantes.

1. α est une racine de P .
2. $X - \alpha$ divise P .

Proposition 44.

Soit $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $\alpha_1, \alpha_2, \dots, \alpha_p \in \mathbb{K}$ des scalaires de \mathbb{K} deux à deux distincts. On a

$$\alpha_1, \alpha_2, \dots, \alpha_p \text{ sont racines de } P \iff \exists Q \in \mathbb{K}[X] \quad P = Q \cdot \prod_{k=1}^p (X - \alpha_k)$$

Exemple 45.

Soit $(p, q, r) \in \mathbb{N}^3$. Justifier qu'il existe $Q \in \mathbb{C}[X]$ tel que $X^{3p+2} + X^{3q+1} + X^{3r} = (X^2 + X + 1)Q$.

Définition 46.

Un polynôme est dit **scindé** dans $\mathbb{K}[X]$ (ou « sur \mathbb{K} ») s'il s'écrit comme produit polynômes de degré 1 à coefficients dans \mathbb{K} .

Corollaire 47 (Cas d'un degré égal au nombre de racines).

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$. Si P possède n racines deux à deux distinctes $\alpha_1, \dots, \alpha_n$ dans \mathbb{K} , alors il est scindé sur \mathbb{K} . Plus précisément, il existe $\lambda \in \mathbb{K}^*$ tel que

$$P = \lambda \prod_{k=1}^n (X - \alpha_k), \quad (\lambda \text{ étant le coefficient dominant de } P).$$

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

2.3 Racines et rigidité des polynômes.**Théorème 48.**

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si $P \neq 0$ et $P \in \mathbb{K}_n[X]$, alors P admet au plus n racines distinctes.
2. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n + 1$ racines deux à deux distinctes, alors $P = 0$.
3. Si P admet une infinité de racines alors $P = 0$.

Corollaire 49 (Montrer que $P = Q$ en prouvant que $P - Q$ a "trop" de racines).

Si P et Q sont de degré inférieur à n et que $P - Q$ possède $n + 1$ racines, alors $P = Q$.

Notamment, si P et Q coïncident sur une infinité de valeurs de \mathbb{K} , P et Q sont le même polynôme. En particulier, lorsque les fonctions polynomiales associées à P et Q sont égales, alors $P = Q$.

Exemple 50.

Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $\forall n \in \mathbb{N} \ P(n) = n^{666}$.

Exemple 51 (Factorisation des polynômes de Tchebychev).

Reprenons la suite $(T_n)_{n \in \mathbb{N}}$ définie par $T_0 = 1$, $T_1 = X$ $\forall n \in \mathbb{N} \ T_{n+2} = 2XT_{n+1} - T_n$.

Nous avons démontré que pour tout $n \in \mathbb{N}^*$, T_n est de degré n , de coefficient dominant 2^{n-1} et que pour tout θ réel, $T_n(\cos \theta) = \cos(n\theta)$.

1. Démontrer que T_n est l'unique polynôme de $\mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R} \ T_n(\cos \theta) = \cos(n\theta)$.
2. Démontrer que pour tout $n \in \mathbb{N}^*$,

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

2.4 Multiplicité d'une racine.

Définition 52.

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P . On dit que la racine α est de **multiplicité** $m \in \mathbb{N}$ si

$$(X - \alpha)^m \text{ divise } P \quad \text{et} \quad (X - \alpha)^{m+1} \text{ ne divise pas } P.$$

On dira que α est de multiplicité **au moins** égale à $k \in \mathbb{N}$ si $(X - \alpha)^k$ divise P .

Une racine de multiplicité 1 est dite **simple**. Une racine qui n'est pas simple est dite **multiple**.

Proposition 53.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$. Il y a équivalence entre les deux assertions suivantes.

1. α est racine de P de multiplicité m .
2. $\exists Q \in \mathbb{K}[X] \quad P = (X - \alpha)^m Q \quad \text{et} \quad Q(\alpha) \neq 0$.

Exemple. Considérons

$$P = (X + 1)X^2(X - 5)^3.$$

Il a pour racines -1 (racine simple), 0 (racine double) et 5 (racine de multiplicité 3).

Lemme 54.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Si $(X - \alpha)^k$ divise P , alors $(X - \alpha)^{k-1}$ divise P' .

Théorème 55 (Caractérisation de la multiplicité).

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a $(1) \iff (2)$, ainsi que $(3) \iff (4)$.

1. α est une racine de P de multiplicité au moins m .
2. $P(\alpha) = P'(\alpha) = P''(\alpha) = \dots = P^{(m-1)}(\alpha) = 0$.
3. α est une racine de P de multiplicité m .
4. $P(\alpha) = P'(\alpha) = P''(\alpha) = \dots = P^{(m-1)}(\alpha) = 0 \quad \text{et} \quad P^{(m)}(\alpha) \neq 0$.

Exemple 56.

En nous appuyant sur une racine multiple "facile", factorisons $P = X^4 + X^3 - 7X^2 - 13X - 6$.

Corollaire 57.

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

α est une racine simple de P si et seulement si $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

Proposition 58.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_p$, p racines de P distinctes deux à deux, de multiplicités respectives au moins égales à k_1, \dots, k_p . Alors, $\prod_{i=1}^p (X - \alpha_i)^{k_i}$ divise P .

On peut compter les racines d'un polynôme

- en considérant les racines deux à deux distinctes,
- ou bien *avec leur multiplicité*, en répétant m fois une racine dans la liste lorsque sa multiplicité vaut m .

Exemple. Le polynôme $P = (X + 1)X^2(X - 5)^3$ possède

- trois racines distinctes : $-1, 0$ et 5 ,
- six racines comptées avec leur multiplicité : $-1, 0, 0, 5, 5, 5$.

Corollaire 59.

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si $P \neq 0$ et $P \in \mathbb{K}_n[X]$, alors P admet au plus n racines comptées avec leur multiplicité.
2. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n + 1$ racines comptées avec leur multiplicité, alors P est le polynôme nul.

Corollaire 60 (Cas d'un degré égal au nombre de racines, comptées avec leur multiplicité).

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.

Si P possède p racines $\alpha_1, \dots, \alpha_p$ dans \mathbb{K} , de multiplicités m_1, \dots, m_p , et si $m_1 + \dots + m_p = n$, alors P est scindé sur \mathbb{K} . Plus précisément, il existe $\lambda \in \mathbb{K}^*$ tel que

$$P = \lambda \prod_{k=1}^p (X - \alpha_k)^{m_k}, \quad (\lambda \text{ étant le coefficient dominant de } P).$$

2.5 Existence de racines : théorème de d'Alembert-Gauss.**Théorème 61** (de d'Alembert-Gauss, ou théorème fondamental de l'algèbre).

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

Exemple 62.

Soit $P \in \mathbb{K}[X] \setminus \mathbb{K}_0[X]$. Montrer que $\tilde{P} : z \mapsto P(z)$, application de \mathbb{C} vers \mathbb{C} est surjective.

Proposition 63 (une racine réelle).

Un polynôme de $\mathbb{R}[X]$ de degré impair possède au moins une racine réelle.

2.6 Décomposition en facteurs irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Définition 64.

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il est dit **irréductible** dans $\mathbb{K}[X]$ si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes constants (non nuls) et les polynômes associés à P , c'est-à-dire ceux de la forme λP , $\lambda \in \mathbb{K}^*$.

Proposition 65.

Un polynôme P est irréductible ssi tous ses diviseurs ont un degré nul ou égal à $\deg(P)$.

Les polynômes irréductibles sont à $\mathbb{K}[X]$ ce que les entiers premiers sont à \mathbb{N} (ou \mathbb{Z}).

Proposition 66.

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

Proposition 67 (Factorisation en produit d'irréductibles à coeff. dans \mathbb{C}).

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

Plus précisément, pour tout $P \in \mathbb{C}[X]$, il existe $\lambda \in \mathbb{C}$, $p \in \mathbb{N}^*$, $\alpha_1, \dots, \alpha_p \in \mathbb{C}$, deux à deux distincts et $v_1, \dots, v_p \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^p (X - \alpha_k)^{v_k}.$$

Lemme 68.

Soit $P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ et $m \in \mathbb{N}^*$. Si α est racine de P alors $\bar{\alpha}$ l'est aussi et

$$B_\alpha = (X - \alpha)(X - \bar{\alpha}) = (X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2)$$

divise P dans $\mathbb{R}[X]$.

Si α a pour multiplicité m , alors $\bar{\alpha}$ aussi et B_α^m divise P dans $\mathbb{R}[X]$.

Proposition 69.

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

- les polynômes de degré 1,
- les polynômes de degré 2, n'ayant pas de racines réelles.

Proposition 70 (Factorisation en produit d'irréductibles à coeff. dans \mathbb{R}).

Tout polynôme de $\mathbb{R}[X]$ s'écrit comme produit de polynômes irréductibles de $\mathbb{R}[X]$.

Plus précisément, si $P \in \mathbb{R}[X]$, il existe $\lambda \in \mathbb{R}$, $p \in \mathbb{N}$, $\alpha_1, \dots, \alpha_p \in \mathbb{R}$ deux à deux distincts, et $m_1, \dots, m_p \in \mathbb{N}^*$, et il existe $p' \in \mathbb{N}$, $(\beta_1, \gamma_1), \dots, (\beta_{p'}, \gamma_{p'}) \in \mathbb{R}^2$, $v_1, \dots, v_{p'} \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^p (X - \alpha_k)^{m_k} \prod_{k=1}^{p'} (X^2 + \beta_k X + \gamma_k)^{v_k} \quad \text{avec} \quad \forall k \in \llbracket 1, p' \rrbracket \quad \beta_k^2 - 4\gamma_k < 0.$$

Méthode (Factorisation d'un polynôme en produit d'irréductibles).

- Renseignements utiles : le degré de P et son coefficient dominant.
- On cherche les racines complexes de P en posant l'équation $P(z) = 0$ avec $z \in \mathbb{C}$, ainsi que la multiplicité de ces racines. On obtient une factorisation dans $\mathbb{C}[X]$ (cf P67).
- Les racines réelles donnent des facteurs de degré 1. Les racines non réelles sont "couplées" avec leur conjuguées pour obtenir des polynômes de degré 2 sans racines réelles, comme dans le lemme 68. On obtient une factorisation dans $\mathbb{R}[X]$ (du type de celle de la proposition 70)

Exemple 71.

Factorisation de $X^6 - 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

3 Compléments.

3.1 Relations coefficients-racines pour un polynôme scindé.

Définition 72.

Soient $x_1, \dots, x_n \in \mathbb{K}$. On appelle **fonctions symétriques élémentaires** de x_1, \dots, x_n les nombres définis par

$$\forall k \in \llbracket 1, n \rrbracket \quad \sigma_k = \sum_{i_1 < i_2 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}.$$

On a notamment

$$\sigma_1 = \sum_{i=1}^n x_i, \quad \sigma_n = \prod_{i=1}^n x_i, \quad \sigma_2 = \sum_{i < j} x_i x_j.$$

Remarque. Dans le cas $n = 2$, il y a deux fonctions symétriques élémentaires de x_1, x_2 :

$$\sigma_1 = x_1 + x_2 \quad \sigma_2 = x_1 x_2.$$

Dans le cas $n = 3$, il y a trois fonctions symétriques élémentaires de x_1, x_2, x_3 :

$$\sigma_1 = x_1 + x_2 + x_3, \quad \sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3, \quad \sigma_3 = x_1 x_2 x_3.$$

Exemple 73.

Soient x, y, z trois scalaires de \mathbb{K} et $\sigma_1, \sigma_2, \sigma_3$ les fonctions symétriques élémentaires associées. Démontrer que

$$\begin{aligned} x^2 + y^2 + z^2 &= \sigma_1^2 - 2\sigma_2 \\ x^3 + y^3 + z^3 &= \sigma_1^3 + 3\sigma_3 - 3\sigma_1\sigma_2 \end{aligned} .$$

Proposition 74 (Relations coefficients-racines : formules de Viète).

Soit P un polynôme de degré $n \in \mathbb{N}^*$, scindé sur \mathbb{K} : il s'écrit donc

$$P = \sum_{k=0}^n a_k X^k \quad \text{et} \quad P = a_n \prod_{k=1}^n (X - \alpha_k),$$

où a_0, \dots, a_n sont ses coefficients et $\alpha_1, \dots, \alpha_n$ ses racines, répétées avec leur multiplicité. On a

$$P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^k \sigma_k X^{n-k} + \dots + (-1)^n \sigma_n \right),$$

avec $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires des racines $\alpha_1, \dots, \alpha_n$.

Ces nombres s'expriment donc en fonction des coefficients de P :

$$\forall k \in \llbracket 1, n \rrbracket \quad \sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

En particulier, pour la somme des racines σ_1 et le produit des racines σ_n ,

$$\sigma_1 = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Remarque. Soit $aX^2 + bX + c$ un polynôme de degré 2 et α_1 et α_2 ses deux racines complexes. On retrouve

$$\alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \alpha_1 \alpha_2 = \frac{c}{a}.$$

Preuve. Avant de développer $a_n(X - \alpha_1) \cdots (X - \alpha_n)$, on pourra commencer par examiner le cas $n = 3$ pour un polynôme unitaire :

$$P = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) = X^3 - \underbrace{(\alpha_1 + \alpha_2 + \alpha_3)}_{=\sigma_1} X^2 + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)}_{=\sigma_2} X - \underbrace{\alpha_1\alpha_2\alpha_3}_{=\sigma_3}.$$

□

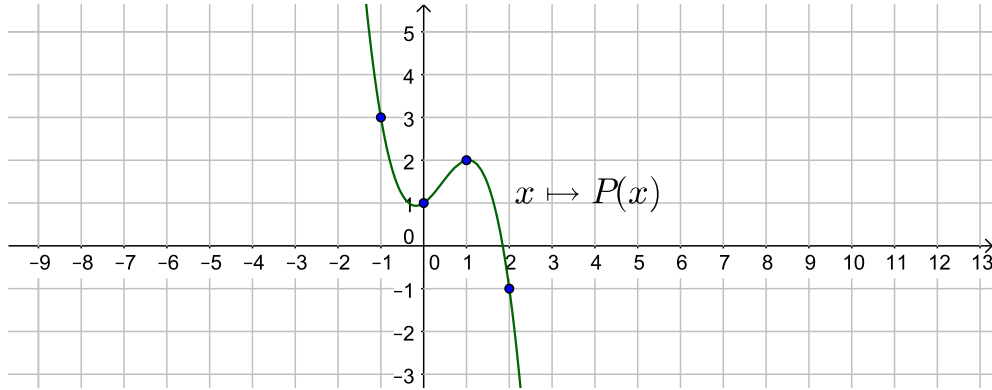
Exemple 75.

Trouver tous les triplets $(x, y, z) \in \mathbb{R}^3$ tels que

$$\begin{aligned} x + y + z &= 2 \\ x^2 + y^2 + z^2 &= 14 \\ x^3 + y^3 + z^3 &= 20 \end{aligned} .$$

3.2 Interpolation de Lagrange.

Interpolier, c'est proposer une fonction qui passe par un ensemble de points donnés. Ici, on a donné l'unique polynôme P de degré inférieur à 3 passant par les quatre points $(-1, 3)$, $(0, 1)$, $(1, 2)$ et $(2, -1)$.



Polynôme interpolateur.

Définition 76.

Soit $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in \mathbb{K}^n$, où les x_i sont deux à deux distincts. On pose

$$\forall i \in \llbracket 1, n \rrbracket \quad L_i = \frac{\prod_{\substack{k=1 \\ k \neq i}}^n (X - x_k)}{\prod_{\substack{k=1 \\ k \neq i}}^n (x_i - x_k)}.$$

Les polynômes (L_1, \dots, L_n) sont appelés **polynômes de Lagrange** associés à (x_1, \dots, x_n) .

Exemple 77 (Comprendre la définition avec un exemple).

Écrire la famille des quatre polynômes de Lagrange associés à $(x_1, x_2, x_3, x_4) = (-1, 0, 1, 2)$.

Proposition 78.

Soit $n \in \mathbb{N}^*$ et (L_1, \dots, L_n) la famille de polynômes de Lagrange associés à un n -uplet (x_1, \dots, x_n) de scalaire deux à deux distincts.

Tous les polynômes L_i sont de degré $n - 1$. De plus,

$$\forall (i, j) \in \llbracket 1, n \rrbracket^2 \quad L_i(x_j) = \delta_{i,j}.$$

Théorème 79.

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.

$$\exists ! P \in \mathbb{K}_{n-1}[X] \quad \forall i \in \llbracket 1, n \rrbracket \quad P(x_i) = y_i.$$

En notant (L_1, \dots, L_n) la famille de polynômes de Lagrange associés à (x_1, \dots, x_n) , on a

$$P = \sum_{i=1}^n y_i L_i.$$

Corollaire 80 (L'ensemble des polynômes interpolateurs).

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.

Soit P l'unique polynôme de $\mathbb{K}_{n-1}[X]$ tel que $\forall i \in \llbracket 1, n \rrbracket \quad P(x_i) = y_i$.

Les polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in \llbracket 1, n \rrbracket \quad Q(x_i) = y_i$ sont ceux de la forme

$$Q = P + A \cdot \prod_{i=1}^n (X - x_i), \quad \text{où } A \in \mathbb{K}[X].$$

Exercices**Polynômes à travers leurs coefficients/ L'anneau $\mathbb{K}[X]$.**

21.1 [◆◆◆] (1er TD : admettre la question 2)

On note $I =]-\frac{\pi}{2}, \frac{\pi}{2}[$.

1. Montrer que pour tout $n \in \mathbb{N}$, il existe un polynôme $P_n \in \mathbb{R}[X]$ tel que

$$\forall x \in I \quad \tan^{(n)}(x) = P_n(\tan(x)).$$

2. Montrer qu'un tel polynôme P_n est unique.
3. Donner pour tout entier n le degré et le coefficient dominant de P_n .
4. Démontrer que pour tout entier naturel n , les coefficients de P_n sont des entiers.

21.2 [◆◆◆] En calculant de deux façons différentes le coefficient devant X^n dans l'écriture développée de $(1 - X^2)^n$, obtenir une identité sur les coefficients binomiaux.

21.3 [◆◆◆] Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $4P = (P')^2$.

21.4 [◆◆◆] Trouver tous les polynômes P dans $\mathbb{R}[X]$ qui satisfont

$$P(X + 1) = XP'.$$

21.5 [◆◆◆] Soit Q un polynôme de $\mathbb{K}[X]$.

Démontrer que l'équation $P - P' = Q$ possède une unique solution dans $\mathbb{K}[X]$.

Racines et factorisation d'un polynôme.

21.6 [◆◆◆] Approximation de π par $\frac{22}{7}$.

1. Poser la division euclidienne de $X^4(1-X)^4$ par $1+X^2$.
2. Démontrer l'égalité $\int_0^1 \frac{x^4(1-x)^4}{1+x^2} dx = \frac{22}{7} - \pi$.
3. Prouver l'inégalité $\frac{1}{1260} \leq \frac{22}{7} - \pi \leq \frac{1}{630}$.

21.7 [◆◆◆] Donner le reste dans la division euclidienne de $X^{2023} + X^3 + 1$ par
a) $X^2 - 1$, b) $(X - 1)^2$.

21.8 [◆◆◆] Soient $(A, B, P) \in (\mathbb{K}[X])^3$ tels que P est non constant et $A \circ P | B \circ P$. Montrer que $A | B$.

21.9 [◆◆◆] Trouver tous les polynômes de $\mathbb{R}[X]$ tels que $(X+4)P(X) = XP(X+1)$.

21.10 [◆◆◆] Démontrer qu'il n'existe pas de polynôme P dans $\mathbb{R}[X]$ tel que

$$\forall n \in \mathbb{N} \quad P(n) = n^{666} + (-1)^n.$$

21.11 [◆◆◆] Montrer que, pour tout $n \in \mathbb{N}^*$, le polynôme $P = \sum_{k=0}^n \frac{X^k}{k!}$ n'a que des racines simples dans \mathbb{C} .

21.12 [◆◆◆] Soit $n \in \mathbb{N}^*$. Montrer que $(X-1)^3$ divise $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.

Factorisation de polynômes

21.13 [◆◆◆] Factoriser $X^6 + X^3 + 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

21.14 [◆◆◆] Soit $n \geq 2$. Factoriser $(X+i)^n - (X-i)^n$ en produit d'irréductibles de $\mathbb{C}[X]$.

21.15 [◆◆◆] Soit $n \in \mathbb{N}^*$. Factoriser $\sum_{k=0}^{n-1} X^k$ dans $\mathbb{C}[X]$. En déduire $\prod_{k=1}^n \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$.

Divers

21.16 [◆◆◆] Soit P un polynôme de $\mathbb{R}[X]$ de degré $n \geq 2$ scindé dans $\mathbb{R}[X]$ à racines simples.

1. Montrer que P' est scindé à racines simples.
2. Prouver que la moyenne arithmétique des racines de P et celle des racines de P' sont égales.

21.17 [◆◆◆] Démontrer qu'il existe un nombre fini de polynômes unitaires de $\mathbb{Z}[X]$ ayant un degré égal à n et des racines complexes de module inférieur à 1.

21.18 [◆◆◆] Soit $n \in \mathbb{N}^*$ et $P = nX^n - \sum_{k=0}^{n-1} X^k$.

1. Prouver que 1 est racine simple de P .
2. (*) En vous intéressant à $(X-1)P$, démontrer que toutes les racines complexes de P sont simples.
3. Donner la somme et le produit des racines.

21.19 [◆◆◆] Soit $n \in \mathbb{N}$.

1. Exprimer de deux façons différentes l'unique polynôme P de degré n tel que $\forall i \in \llbracket 0, n \rrbracket \quad P(i) = i^n$.
2. En considérant son coefficient dominant, démontrer l'identité

$$\sum_{i=0}^n (-1)^{n-i} \binom{n}{i} i^n = n!$$