$\mathbb{K}[X]$

Contexte : dans ce chapitre, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ (mais en pratique on prendra $\mathbb{K}=\mathbb{R}$ ou $\mathbb{K}=\mathbb{C}$).

Objectifs du chapitre :

— Définir rigoureusement les objets rencontrés en TACMAS.

— Démontrer les théorèmes admis en TACMAS.

— Décrire l'arithmétique de $\mathbb{K}[X]$.

I Construction. Structure.

I.1 Algèbre $\mathbb{K}[X]$

Rappel : un polynôme n'a pas vocation à s'appliquer à un scalaire. Il a vocation à s'appliquer à *tout élément de toute* $\mathbb{K}$*-algèbre* (scalaire, matrice, endomorphisme, ...) : cette motivation nous conduit à la définition suivante.

Définition 1 .

- On appelle indéterminée la lettre X.
- On appelle polynôme en X à coefficients dans $\mathbb{K}$ toute combinaison linéaire formelle de puissances de l'indéterminée X.
- On appelle monôme tout polynôme de la forme a_nX^n.

L'indéterminée X est un objet formel, rien de plus, de même pour les expressions X^0, X^1, X^2, ..., X^n, etc. Une combinaison linéaire formelle des puissances de l'indéterminée est simplement une expression de la forme $a_1X^{i_1}+a_2X^{i_2}+\cdots+a_rX^{i_r}$ où les a_k sont des scalaires et les i_k des entiers distincts. Cette expression est formelle au sens où l'égalité entre deux telles expressions est l'égalité syntaxique, aux trois identifications suivantes près (sans lesquelles parler de "combinaison linéaire" serait usurper une appellation contrôlée) :

1. on identifie X^0 avec le scalaire 1 et X^1 avec l'indéterminée X ;
2. on identifie les combinaisons linéaires qui ne se distinguent que par l'ordre des termes, par exemple $a_1X^{i_1}+a_2X^{i_2}+a_3X^{i_3}$ et $a_3X^{i_3}+a_1X^{i_1}+a_2X^{i_2}$;
3. on identifie une combinaison linéaire de la forme $a_1X^{i_1}+a_2X^{i_2}+\cdots+a_rX^{i_r}+0X^{i_{r+1}}$ avec la combinaison linéaire correspondante $a_1X^{i_1}+a_2X^{i_2}+\cdots+a_rX^{i_r}$.

Proposition-Définition 2 .

Un polynôme est toujours de la forme $P=a_0+a_1X+\cdots+a_nX^n=\sum_{k=0}^{n}a_kX^k$, où n désigne un entier naturel et a_0,...,a_n des éléments de $\mathbb{K}$.

Les éléments a_0, ..., a_n sont alors appelés les coefficients de P.

Lorsqu'ils sont tous nuls, on dit que P est le polynôme nul.

Démonstration. Il suffit d'utiliser de façon répétée les règles 2. et 3. d'identification présentées précédemment : on note n le plus grand des entiers i_k (ou même un entier quelconque plus grand que le plus grand des i_k), on ajoute des coefficients nuls pour toutes les puissances de X absentes de la somme, et on réordonne enfin les termes. □

Définition 3 .

On appelle degré de P l'élément de $\mathbb{N}\cup\{-\infty\}$ suivant : $\deg(P)=\sup_{\overline{\mathbb{R}}}\{i,\ a_i\neq 0\}$.

Ainsi un polynôme est nul si et seulement si son degré est $-\infty$ et, si $a_n\neq 0$, alors $\deg(a_0+a_1X+\cdots+a_nX^n)=n$.

Notation 1

- On note $\mathbb{K}[X]$ l'ensemble de tous les polynômes à coefficients dans $\mathbb{K}$.
- On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré $\leqslant n$.

Remarque 1

On peut donc agréablement noter un polynôme $\sum_{k=0}^{+\infty} a_k X^k$, où la suite $(a_k)_{k\in\mathbb{N}}$ est nulle à partir d'un certain rang (on dit aussi qu'elle est presque nulle). Le polynôme nul correspond alors à la suite $(a_k)_{k\in\mathbb{N}}$ telle que $a_k = 0$ pour tout $k \in \mathbb{N}$.

Toujours en appliquant nos deux règles, on a immédiatement :

Théorème 1 : Identification.

Deux polynômes sont égaux si et seulement si les suites presque nulles $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ sont identiques.
Dit autrement : $P = Q \Leftrightarrow \forall k \in \mathbb{N},\ a_k = b_k$.

Bref, deux polynômes sont égaux si et seulement si tous leurs coefficients de même degré sont égaux. C'était facile mais il reste à montrer qu'on peut encore l'utiliser sur des fonctions polynomiales et pas seulement sur les polynômes formels.

I.2 Structure d'algèbre

Définition 4 .

On définit une loi de composition interne $+$ sur $\mathbb{K}[X]$ de la manière suivante :
si $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ sont deux éléments de $\mathbb{K}[X]$, on note $P+Q$ le polynôme :
$P + Q = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_n + b_n)X^n$.

Proposition 1 .

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

Démonstration. Toujours le même argument (travailler coefficient par coefficient). Exercice à savoir faire ! □

Remarque 2

$$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{N}} \\ P = a_0 + a_1 X + \cdots + a_n X^n & \mapsto & (a_0, a_1, \cdots, a_n, 0, 0, \ldots, 0, \ldots) \end{array} \right. \text{ est un morphisme de groupe.}$$

$Im(\Psi) = \mathbb{K}^{(\mathbb{N})}$ (les suites presque nulles). La corestriction $\Psi : \mathbb{K}[X] \to \mathbb{K}^{(\mathbb{N})}$ est un isomorphisme de groupe.

Définition 5 .

On définit une loi de composition externe $\cdot : \left\{ \begin{array}{ccc} \mathbb{K}\times\mathbb{K}[X] & \to & \mathbb{K}[X] \\ (\lambda, P) & \mapsto & \lambda \cdot P \end{array} \right.$ par : si $P = \sum_{k=0}^{+\infty} a_k X^k$ alors
$\lambda \cdot P = (\lambda a_0) + (\lambda a_1)X + \cdots + (\lambda a_n)X^n$

Proposition 2 .

$(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.

Démonstration. Toujours le même argument (travailler coefficient par coefficient). Exercice à savoir faire ! □

Remarque 3

$$\Psi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{(\mathbb{N})} \\ P = a_0 + \cdots + a_n X^n & \mapsto & (a_0, \cdots, a_n, 0, \ldots, 0, \ldots) \end{array} \right. \text{ est un isomorphisme de } \mathbb{K}\text{-ev.}$$

Ainsi, on aurait pu (dû ?) **définir** un polynôme comme une suite presque nulle, et X comme la suite $(0, 1, 0, 0, \ldots)$... c'est ce qu'on peut faire en informatique en définissant un polynôme par la liste (ou le tableau) de ses coefficients.

Remarque 4

- Par définition, $\mathbb{K}[X]$ a une base canonique : $(1, X, X^2, \ldots, X^n, \ldots)$.
- $\mathbb{K}_n[X]$ est clairement un sev de $\mathbb{K}[X]$ qui a aussi une base canonique : $(1, X, X^2, \ldots, X^n)$.

Définition 6 .

Soit $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{j=0}^{m} b_j X^j$.

On définit le polynôme noté $P \times Q$ par : $P \times Q = \sum_{k=0}^{n+m} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i b_j = \sum_{r=0}^{k} a_r b_{k-r}$.

Notation 2 Pour un polynôme P quelconque, on note évidemment $P^2 = P \times P$, $P^3 = P^2 \times P$, etc.

Théorème 2 .

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif, d'élément unité le polynôme constant 1.

DÉMONSTRATION.

1. On a déjà vu que $(\mathbb{K}[X], +)$ forme un groupe commutatif.

2. Soient trois polynômes $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ et $R = \sum_{k=0}^{\ell} c_k X^k$. On a :

$$\begin{aligned}
(P \times Q) \times R &= \left(\sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k\right) \times \sum_{k=0}^{\ell} c_k X^k && \text{par définition de } \times \\
&= \sum_{k=0}^{n+m+\ell} \sum_{i=0}^{k} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) c_{k-i} X^k && \text{par définition de } \times \\
&= \sum_{k=0}^{n+m+\ell} \sum_{i=0}^{k} \left(\sum_{j=0}^{i} a_j b_{i-j} c_{k-i}\right) X^k && \text{par distributivité} \\
&= \sum_{k=0}^{n+m+\ell} \sum_{j=0}^{k} \left(\sum_{i=j}^{k} a_j b_{i-j} c_{k-i}\right) X^k && \text{par permutation de } \Sigma \\
&= \sum_{k=0}^{n+m+\ell} \sum_{j=0}^{k} a_j \left(\sum_{i=j}^{k} b_{i-j} c_{k-i}\right) X^k && \text{par distributivité} \\
&= \sum_{k=0}^{n+m+\ell} \sum_{j=0}^{k} a_j \left(\sum_{i=0}^{k-j} b_i c_{k-j-i}\right) X^k && \text{par réindiçage} \\
&= \left(\sum_{k=0}^{n} a_k X^k\right) \times \sum_{k=0}^{m+\ell} \left(\sum_{i=0}^{k} b_i c_{k-i}\right) X^k && \text{par définition de } \times \\
&= P \times (Q \times R) && \text{par définition de } \times.
\end{aligned}$$

Ainsi $\times$ est associative.

3. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. Si l'on note $Q = b_0 = 1$, alors le coefficient général $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ de $P \times Q$ vaut $a_k b_0 = a_k$ car pour $i \neq k$, on a $k - i \neq 0$ et donc $b_{k-i} = 0$. Ainsi a-t-on $P \times 1 = P$.

   On obtient de même (ou on déduit de la commutativité mentionnée plus bas) qu'on a $1 \times P = P$.

   Finalement $\times$ possède un élément neutre dans $\mathbb{K}[X]$, à savoir le polynôme 1.

Il reste à vérifier :

4. $\times$ est commutative.
5. $\times$ est distributive sur $+$, c'est-à-dire :
   $\forall (P, Q, R) \in \mathbb{K}[X]^3,\ P \times (Q + R) = P \times Q + P \times R$ (distributivité à gauche).

Ces deux points entraînant évidemment la distributivité à droite.

Exercice 1. Montrer ces deux points 4 et 5.

□

Corollaire 1 : Structure de $\mathbb{K}$-algèbre.

$(\mathbb{K}[X], +, \times, \cdot)$ forme une $\mathbb{K}$-algèbre.

Démonstration. Il reste à voir que $\cdot$ est compatible avec $\times$ et $1_{\mathbb{K}}$, et c'est facile. □

Remarque 5

$\mathbb{K}_n[X]$ **n'**est **pas** un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$!

Proposition 3 .

L'anneau $\mathbb{K}[X]$ est intègre, c'est-à-dire qu'un produit de deux polynômes est nul si et seulement si un des deux facteurs est nul.

Démonstration. Le sens réciproque est vrai dans tout anneau. Soient $P = a_0 + \cdots + a_n X^n$ et $Q = b_0 + \cdots + b_m X^m$ tels que $PQ = 0$. Supposons par l'absurde $P \neq 0$ et $Q \neq 0$. À renommage près on peut donc supposer $a_n \neq 0$ et $b_m \neq 0$. Par suite on a $PQ = a_0 b_0 + \cdots + a_n b_m X^{n+m} \neq 0$.

□

I.3 Applications polynomiales

Définition 7 .

Soit $(\mathcal{A}, +, \times, \cdot)$ une $\mathbb{K}$-algèbre. Pour tout polynôme $P = \sum_{k=0}^{d} a_k X^k$ de $\mathbb{K}[X]$ on peut considérer l'application polynomiale associée à P dans $\mathcal{A}$, simplement définie par : $\widetilde{P}^{\mathcal{A}} \left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ A & \mapsto & \sum_{k=0}^{d} a_k A^k \end{array} \right.$, la somme et les multiplications considérées dans cette expression étant celles de l'algèbre $\mathcal{A}$.

En général, on note encore P l'application $\tilde{P}^{\mathcal{A}}$ pour éviter trop de lourdeurs, le contexte permettant de déterminer dans quelle algèbre on se trouve.

Exemples 1 Pour $\mathbb{K} = \mathbb{R}$, considérons le polynôme $X^2 + 1 \in \mathbb{R}[X]$.

1. Ce polynôme induit une application $\left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^2 + 1 \end{array} \right.$ qui ne s'annule pas.
2. Ce polynôme induit une application $\left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & z^2 + 1 \end{array} \right.$ qui s'annule exactement deux fois.
3. Ce polynôme induit une application $\left\{ \begin{array}{ccc} \mathcal{M}_2(\mathbb{R}) & \to & \mathcal{M}_2(\mathbb{R}) \\ M & \mapsto & M^2 + I_2 \end{array} \right.$ qui s'annule une infinité de fois, par exemple sur toutes les matrices de la forme $\begin{pmatrix} 0 & \lambda \\ -\frac{1}{\lambda} & 0 \end{pmatrix}$ $(\lambda \in \mathbb{R}^*)$.
4. Ce polynôme induit une application $\left\{ \begin{array}{ccc} \mathbb{R}^I & \to & \mathbb{R}^I \\ f & \mapsto & \left(x \mapsto f(x)^2 + 1\right) \end{array} \right.$.

On a de manière évidente, du fait des définitions de la somme et du produit de fonctions :

Théorème 3 : Lien polynôme/application polynomiale.

Si $\mathcal{A} \neq \{0\}$ alors $P \mapsto \tilde{P}$ est un morphisme d'algèbres injectif, c'est-à-dire :

1. $\forall (P, Q) \in \mathbb{K}[X]^2,\ \forall (\lambda, \mu) \in \mathbb{K}^2\ \widetilde{\lambda P + \mu Q}^{\mathcal{A}} = \lambda \widetilde{P}^{\mathcal{A}} + \mu \widetilde{Q}^{\mathcal{A}}$ (linéarité) ;
2. $\forall (P, Q) \in \mathbb{K}[X]^2,\ \widetilde{PQ}^{\mathcal{A}} = \widetilde{P}^{\mathcal{A}}\, \widetilde{Q}^{\mathcal{A}}$ (préservation des produits) ;
3. $\forall (P, Q) \in \mathbb{K}[X]^2,\ \widetilde{P}^{\mathcal{A}} = \widetilde{Q}^{\mathcal{A}} \Rightarrow P = Q$ (injectivité).

Cela justifie qu'on note P plutôt que $\tilde{P}^{\mathcal{A}}$.

La théorème est intéressant car on connaît plein de théorèmes sur les fonctions polynômiales ; ce théorème permet d'en déduire des théorèmes analogues mais portant sur les polynômes formels.

Exercice 2. Les deux premiers points (c'est un morphisme d'algèbre) découlent immédiatement des définitions.
Le montrer est censé être un exercice facile, je vous le laisse pour la maison.

Reste l'injectivité.

Soient $P = \sum_{k=0}^{n} a_k, Q = \sum_{k=0}^{m} b_k \in \mathbb{K}[X]$ Soient $\lambda, \mu \in \mathbb{R}$
Quitte à ce que certains coefficients soient nuls, on peut supposer que $m = n$.

— $\widetilde{\lambda P + \mu Q}^{\mathcal{A}} = x \mapsto \widetilde{\lambda P + \mu Q}^{\mathcal{A}}(x)$ Or $\lambda P + \mu Q = \lambda \sum_{k=0}^{n} a_k X^k + \mu \sum_{k=0}^{n} b_k X^k$. Par définition de P et Q $\lambda P + \mu Q = \sum_{k=0}^{n} (\lambda a_k + \mu b_k) X^k$ par définition de $\cdot$ et $+$.
Donc

Démonstration. Montrons l'injectivité dans le cas $\mathcal{A} = \mathbb{K} = \mathbb{R}$ (on verra dans quelques pages une démonstration générale).

Soient $P,\ Q \in \mathbb{R}[X]$ et supposons $\tilde{P} = \tilde{Q}$ *i. e.* $\widetilde{P - Q} = x \mapsto 0$.

Notons $P = p_0 + p_1 X + \cdots + p_n X^n$ et $Q = q_0 + q_1 X + \cdots + q_n X^n$ (quitte à ce que certains coefficients soient nuls).
On a $x \mapsto 0 = \widetilde{P - Q} = x \mapsto (p_0 - q_0) + (p_1 - q_1)x + \cdots + (p_n - q_n)x^n$.

On évalue en 0 on trouve $p_0 = q_0$.
On dérive et on évalue en 0 on trouve $p_1 = q_1$.
On redérive et on évalue en 0 on trouve $2(p_2 - q_2) = 0$ donc $p_2 = q_2$.
Etc. On trouve finalement $n!(p_n - q_n) = 0$ donc $p_n = q_n$.
On a donc $P = Q$.
D'où l'injectivité. □

Remarque 6

On a vu dans le corollaire 1 que $(\mathbb{K}[X], +, \times, \cdot)$ est justement une $\mathbb{K}$-algèbre.

À tout polynôme P, on peut donc associer une application $\widetilde{P}^{\mathbb{K}[X]} : \mathbb{K}[X] \to \mathbb{K}[X]$!

Remarque 7

On a donc toujours : $P(X) = P$!

Définition 8 .

Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q \in \mathbb{K}[X]$.

On définit le polynôme composé $P \circ Q$, noté parfois simplement $P(Q)$, par : $P \circ Q = \widetilde{P}^{\mathbb{K}[X]}(Q) = \sum_{k=0}^{+\infty} a_k Q^k$.

I.4 Dérivation des polynômes

On définit la dérivée d'un polynôme de la seule façon possible pour avoir $\widetilde{P'} = \tilde{P}'$, c'est-à-dire pour que la dérivée de l'application associée soit l'application associée à la dérivée. Cela donne :

Définition 9 .

Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$.

On appelle polynôme dérivé de P le polynôme $P' = \sum_{k=1}^{d} a_k k X^{k-1}$ i. e. $P' = \sum_{k=0}^{d-1} (k+1) a_{k+1} X^k$.

De même que pour les fonctions, on définit la dérivation n-ième par $P^{(0)} = P$ et, pour tout $n \in \mathbb{N}$, $P^{(n+1)} = \left(P^{(n)}\right)'$.

Le fait que $P \mapsto \tilde{P}$ soit un morphisme d'anneau injectif permet gratuitement de récupérer les propriétés algébriques de la dérivation connues sur les fonctions polynômiales (car connues sur toutes les fonctions suffisament dérivables).

Théorème 4 : Propriétés de la dérivation.

- $P \mapsto P'$ est linéaire, donc $P \mapsto P^{(n)}$ est linéaire ;
- $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)' = P'Q + PQ'$, donc $\forall (P,Q) \in \mathbb{K}[X],\ (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$;
- $\forall (P,Q) \in \mathbb{K}[X],\ (P \circ Q)' = Q' \times P' \circ Q$, donc $\forall P \in \mathbb{K}[X],\ \forall (\alpha,\beta) \in \mathbb{K}^2,\ P^{(n)}(\alpha X + \beta) = \alpha^n P^{(n)}(\alpha X + \beta)$.

Les formules de Taylor se transposent de la même façon, mais on a pour les polynômes une version de luxe :

Théorème 5 : Taylor pour les polynômes.

- En 0 : $P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(0)}{k!} X^k$.
- En λ : $P(X+\lambda) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\lambda)}{k!} X^k$.
- En λ (v2) : $P(X) = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(\lambda)}{k!} (X-\lambda)^k$.

Démonstration. On peut le déduire de la formule de Taylor pour les fonctions (cf cours "familles en dimension finie"). On peut aussi procéder comme suit :

1. Notons $P = a_0 + a_1 X + a_2 X^2 + \cdots + a_p X^p$. On a $P(0) = a_0$, puis, par définition de la dérivation, $P'(0) = a_1$, $P''(0) = 2a_2$, …, $P^{(k)}(0) = k! a_k$, …, $P^{(n)}(0) = n! a_n$.
   Comme une factorielle n'est jamais nulle, on peut réécrire ces égalités $a_0 = P(0)$, $a_1 = P'(0)$, $a_2 = \frac{P''(0)}{2}$, …, $a_k = \frac{P^{(k)}(0)}{k!}$, …, $a_n = \frac{P^{(n)}(0)}{n!}$. On a donc bien $P = \sum_{k=0}^{p} a_k X^k = \sum_{k=0}^{p} \frac{P^{(k)}(0)}{k!} X^k$.
2. On applique la formule précédente au polynôme $Q(X) = P(X+\lambda)$. On a $P(X+\lambda) = \sum_{k=0}^{p} \frac{Q^{(k)}(0)}{k!} X^k$. D'après le point 3 du théorème 3 on a, pour tout entier k, $Q^{(k)}(0) = P^{(k)}(0+\lambda) = P^{(k)}(\lambda)$. D'où le résultat.
3. Il suffit de composer l'égalité précédente à droite par $X - \lambda$. □

I.5 Propriétés du degré

Proposition 4 : Degré d'une dérivée.

Soit P un polynôme. Alors on a :

- $\deg(P') = \begin{cases} \deg(P) - 1 \text{ si } \deg(P) \geqslant 1 \\ -\infty \text{ sinon.} \end{cases}$
- $\deg(P^{(n)}) = \begin{cases} \deg(P) - n \text{ si } \deg(P) \geqslant n \\ -\infty \text{ sinon.} \end{cases}$

Démonstration. Il suffit d'écrire la définition. □

On s'intéresse dans la suite au degré d'une expression de la forme $P \square Q$, avec $\square \in \{+, \times, \circ\}$.

On convient des règles suivantes pour la gestion du polynôme nul :

$-\infty + n = -\infty$
$-\infty \times 0 = 0$ et si $n \neq 0$ alors $-\infty \times n = -\infty$

Théorème 6 : Degré d'une CL.

Soient P et Q deux polynômes, λ un scalaire. Alors on a :

1. $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$;
2. si $\deg(P) \neq \deg(Q)$, alors $\deg(P+Q) = \max(\deg P, \deg Q)$;
3. si $\lambda \neq 0$, alors $\deg(\lambda P) = \deg(P)$.

Démonstration. Supposons P de degré n et Q de degré m.

Alors on peut écrire $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$, avec $a_n \neq 0$ et $b_m \neq 0$.

1. Si $m = n$, alors on a $P+Q = \sum_{k=0}^{n} (a_k + b_k) X^k$ qui est de degré au plus n (et éventuellement de degré strictement inférieur si $a_n + b_n = 0$).
2. Sinon on a $P+Q = \sum_{k=0}^{m} (a_k + b_k) X^k + \sum_{k=m+1}^{n} a_k X^k$ qui est de degré $n = \max(\deg P, \deg Q)$.
3. Idem. □

On peut utiliser ce théorème pour établir que $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$.

Théorème 7 : Degré d'un produit.

Soient P et Q deux polynômes. Alors on a : $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Démonstration. Soit $n = \deg P$ et $m = \deg Q$. On écrit $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{j=0}^{m} b_j X^j$ avec $a_n \neq 0$ et $b_m \neq 0$.

Dans le produit PQ, il n'y a aucun terme en X^k avec $k > n+m$. Le terme en $k = n+m$ est $c_{n+m} = a_n b_m \neq 0$.

On a donc bien $\deg(PQ) = n+m$. □

Remarque 8

La proposition précédente montre à nouveau que $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$ pour $n \geqslant 1$.

On peut aussi l'utiliser pour retrouver l'intégrité de $\mathbb{K}[X]$ en une demi-ligne !

Corollaire 2 : Degré d'une puissance.

Soit P un polynôme et $n \in \mathbb{N}$. Alors on a : $\deg(P^n) = n \deg(P)$.

Démonstration. Par récurrence immédiate. ☺ □

Théorème 8 : Degré d'une composée.

Soient P un polynôme **et** Q **un polynôme non constant**. Alors on a : $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Démonstration. Notons $n = \deg(P)$ et $m = \deg(Q)$. Comme Q est supposé non constant, on a $m \geqslant 1$.

- Si $P = 0$, on a $P \circ Q = 0$. Ainsi on a $\deg(P) = -\infty = \deg(P \circ Q)$ et, comme $m \geqslant 1$, $\deg(P) \times \deg(Q) = -\infty$. L'égalité annoncée est donc vérifiée dans ce cas.
- Si $\deg(P) = 0$, c'est-à-dire si P est un polynôme constant non nul, alors $P \circ Q = P$ et $0 = \deg(P \circ Q)$ est bien égal à $\deg(P) \times \deg(Q)$.
- Si $n \geqslant 1$ alors on écrit $P = a_n X^n + P_1$ et $Q = b_m X^m + Q_1$ avec $a_n \neq 0$, $b_m \neq 0$, $\deg(P_1) < n$ et $\deg(Q_1) < m$. On obtient $P \circ Q = a_n (b_m X^m + Q_1)^n + P_1(b_m X^m + Q_1)$. Le terme de plus haut degré de $a_n(b_m X^m + Q_1)^n$ est $a_n b_m X^{nm}$ qui a pour degré nm, tandis que le terme de plus haut degré de $P_1(b_m X^m + Q_1)$ a pour degré $(n-1)m$. Comme on a $m \geqslant 1$, on a $nm > (n-1)m$, ce qui signifie que $P \circ Q$ a pour terme de plus haut degré $a_n b_m X^{mn}$. Ainsi $\deg(P \circ Q) = nm = \deg(P) \times \deg(Q)$. □

Remarque 9

Si Q est constant il peut se produire qu'il soit une racine de P et dans ce cas on a $P \circ Q = 0$...

Enfin, fixons un peu de terminologie pour la suite :

- On appelle terme de plus haut degré d'un polynôme non nul $P = \sum a_k X^k$ de degré d le monôme $a_d X^d$.
- On appelle coefficient dominant d'un polynôme non nul $P = \sum a_k X^k$ de degré d le coefficient a_d.
- On dit d'un polynôme qu'il est unitaire lorsqu'il est de coefficient dominant 1.

On notera dans ce chapitre $\mathcal{U}$ l'ensemble des polynômes unitaires de $\mathbb{K}[X]$ (le contexte permettant de déterminer $\mathbb{K}$).

II Racines

II.1 Division euclidienne

Théorème 9 : Division euclidienne.

Soit $(A,B)\in\mathbb{K}[X]\times(\mathbb{K}[X]\setminus\{0\})$.
Alors il existe un unique couple $(Q,R)\in\mathbb{K}[X]^2$ tel que : $A=BQ+R$ et $\deg(R)<\deg(B)$.

Démonstration. **Unicité** : Soient $(Q,R)\in\mathbb{K}[X]^2$ et $(Q',R')\in\mathbb{K}[X]^2$ tels que $\begin{cases}A=BQ+R\\ \deg(R)<\deg(B)\end{cases}$ et $\begin{cases}A=BQ'+R'\\ \deg(R')<\deg(B).\end{cases}$ On a en particulier $BQ+R=BQ'+R'$ d'où $B(Q-Q')=R'-R$.

Or $\deg(R'-R)\leqslant\max(\deg R,\deg R')<\deg B$, et si on a $Q-Q'\neq 0$, alors $\deg\big(B(Q-Q')\big)=\deg B+\deg(Q-Q')\geqslant\deg B$.
La seule possibilité est qu'on ait $Q-Q'=0$, donc $Q=Q'$, et il s'ensuit $R=R'$.

Existence : Je laisse la démonstration version "comment poser une division euclidienne" et on fait au tableau la version "je recopie la preuve vue dans $\mathbb{N}$".

On fixe B et on montre par récurrence qu'on a $\forall n\in\mathbb{N}$, $\mathcal{P}_n$, en notant $\mathcal{P}_n$ la propriété : $\mathcal{P}_n$: $\forall A\in\mathbb{K}_n[X]$, $\exists(Q,R)\in\mathbb{K}[X]^2$, $A=BQ+R$ et $\deg(R)<\deg(B)$.

Initialisation : Soit $A=a_0\in\mathbb{K}_0[X]$. Si on a $\deg B>0$, alors on écrit $A=B\times 0+a_0$.
Si on a $\deg B=0$, alors $B=b_0\neq 0$ et on écrit $A=B\times\dfrac{a_0}{b_0}+0$. Ainsi $\mathcal{P}_0$ est vraie.

Hérédité : Soit $n\in\mathbb{N}$ et supposons $\mathcal{P}_n$ vraie. Soit $A\in\mathbb{K}_{n+1}[X]$.
Si on a $\deg B>n+1$, alors on écrit $A=B\times 0+A$.
Sinon : $A=a_{n+1}X^{n+1}+a_nX^n+\cdots+a_1X+a_0$ et $B=b_dX^d+\cdots+b_1X+b_0$, où $d\leqslant n+1$. Soit $A_1=A-\dfrac{a_{n+1}}{b_d}X^{n+1-d}B$.
Le polynôme A_1 est de degré au plus n donc on peut appliquer l'hypothèse de récurrence : il existe Q_1 et R_1, avec $\deg R_1<\deg B$, tels que $A_1=BQ_1+R_1$. On en déduit : $A=A_1+\dfrac{a_{n+1}}{b_d}X^{n+1-d}B=B\left(Q_1+\dfrac{a_{n+1}}{b_d}X^{n+1-d}\right)+R_1$,
donc $Q=\left(Q_1+\dfrac{a_{n+1}}{b_d}X^{n+1-d}\right)$ et $R=R_1$ conviennent : $\mathcal{P}_{n+1}$ est vraie.
La propriété est donc bien héréditaire.

Conclusion : La propriété est vraie au rang 0, et elle est héréditaire, donc d'après le théorème de récurrence elle est vraie pour tout entier $n\in\mathbb{N}$. Le théorème est donc démontré pour tout polynôme A non nul. Si $A=0$, il suffit de prendre $Q=R=0$. □

Reformulation : le théorème de division euclidienne se reformule $\forall B\in\mathbb{R}[X]\setminus\{0\}$, $\mathbb{K}[X]=B\mathbb{K}[X]\oplus\mathbb{K}_{\deg(B)-1}[X]$.

Exercice 3. Exemple déjà vu dans une vie antérieure : quelle est la division euclidienne de X^n-1 par X^d-1 ?

D'après le théorème de la division euclidienne dans $\mathbb{N}$: $\exists!(q,r),n=qd+r$ avec $r<q$.
donc :

Proposition 5 : Invariance par extension de corps.

Soit $(A,B)\in\mathbb{R}[X]\times(\mathbb{R}[X]\setminus\{0\})$ $\Big($ en particulier on a $(A,B)\in\mathbb{C}[X]\times(\mathbb{C}[X]\setminus\{0\})$ $\Big)$.

Le quotient et le reste de la division euclidienne de A par B sont les mêmes pour la division euclidienne dans $\mathbb{C}[X]$ que pour la division euclidienne dans $\mathbb{R}[X]$.

Démonstration. C'est immédiat par unicité de la division euclidienne ! □

II.2 Racines

Proposition-Définition 10 .

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

1. $P(\alpha) = 0$.
2. Le polynôme $(X - \alpha)$ divise P.

On dit alors que α est une racine de P dans $\mathbb{K}$.

Démonstration. Fixons $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ et examinons la division euclidienne de P par $X - \alpha$.

On a $P = (X - \alpha)Q + R$ avec $\deg R < 1$ autrement dit R est une constante $c \in \mathbb{K}$.
L'équivalence demandée s'en déduit immédiatement ! □

Théorème 10 : **très important.**

1. Un polynôme de degré $n \geqslant 0$ a au plus n racines.
2. Si $P \in \mathbb{K}[X]$ a une infinité de racines alors $P = 0$.
3. Si $P \in \mathbb{K}_n[X]$ a $n + 1$ racines alors $P = 0$.

Démonstration.

1. Soit P de degré n. Supposons par l'absurde qu'il a au moins $n + 1$ racines : $\lambda_1, \ldots, \lambda_{n+1}$.
   Ainsi il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - \lambda_1) \cdots (X - \lambda_{n+1})Q$.
   Donc $n = \deg(P) = (n + 1) + \deg(Q)$.
   Si $Q = 0$ on a $n = -\infty$; si $Q \neq 0$ on a $n \geqslant n + 1$; dans tous les cas on a une contradiction.
2. Par l'absurde. Supposons $P \neq 0$ *i. e.* $n = \deg(P) \geqslant 0$.
   Alors P a au plus n racines et donc n'a pas une infinité de racines, contradiction.
3. Comme dans le 1. et le seul cas possible de la disjonction de cas est $Q = 0$.

□

Application 1 On retrouve que $\left\{ \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ P & \mapsto & \tilde{P} \end{array} \right.$ est injective (y compris pour $\mathbb{K} = \mathbb{C}$). En effet, soient P, Q tels que $\tilde{P} = \tilde{Q}$. Comme $\mathbb{K}$ est infini, et que $\widetilde{P - Q}$ est la fonction nulle, $P - Q$ a une infinité de racines, et donc $P - Q$ est le polynôme nul !

Plus généralement, si $\mathcal{A} \neq 0$ est une $\mathbb{K}$-algèbre on a (à identification près de $\lambda \cdot 1_{\mathcal{A}}$ et λ) $\mathbb{K} \subset \mathcal{A}$ et donc $\left\{ \begin{array}{ccc} \mathcal{A} & \to & \mathcal{A} \\ P & \mapsto & \tilde{P} \end{array} \right.$ est injective.

Exercice 4.

1. **Rappel :** *(Formule de Vandermonde.)* Soient $p, q, n \in \mathbb{N}$. Montrer qu'on a $\displaystyle\sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}$.

   Soit $(1 + X)^{m+n} \in \mathbb{K}[X]$. On a

$$(1 + X)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} X^k \quad (1)$$

$$\begin{aligned} (1 + X)^m (1 + X)^m &= \sum_{k=0}^{m} \binom{m}{k} X^k \sum_{k=0}^{n} \binom{n}{k} X^k \\ &= \sum_{k=0}^{m+n} \left(\sum_{r=0}^{k} \binom{m}{n} \binom{n}{k-r} \right) X^k \quad (2) \end{aligned}$$

Donc par identification de (1) et (2) car (1) = (2) :

$$\sum_{r=0}^{k} \binom{m}{r}\binom{n}{k-r} = \binom{m+n}{k}$$

2. *(Identité de Chu-Vandermonde.)* Soit α un **réel**. Montrer qu'on a $\sum_{k=0}^{n} \binom{\alpha}{k}\binom{\alpha}{n-k} = \binom{2\alpha}{n}$.

Méth. 2 On a vu : $\forall p,q,n : \sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k}$

D'après (1) (avec $q = p$), ce polynôme $P(X)$ a pour racines tout les entiers $p \in \mathbb{N}$
Donc P a une infinité de racines, donc $P = 0$, donc $\forall \alpha \in \underline{\underline{\mathbb{R}}}, P(\alpha) = 0$ ie :

$$\forall \alpha \in \mathbb{R}, \sum_{k=0}^{n} \binom{\alpha}{n}\binom{\alpha}{n-k} = \binom{2\alpha}{n}$$

Définition 11 .

Un polynôme P de degré n est dit :

- scindé lorsqu'il peut s'écrire $P(X) = a_n(X-\lambda_1)\cdots(X-\lambda_n)$.
- scindé à racines simples lorsqu'il peut s'écrire $P(X) = a_n(X-\lambda_1)\cdots(X-\lambda_n)$ avec les λ_i distincts.

/!\ La notion de polynôme scindé n'est pas invariante par extension de corps.
Exemple : X^2+1.

Théorème 11 : de d'Alembert-Gauss (rappel).

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

Démonstration.
On a déjà admis dans le cours sur $\mathbb{C}$ "tout polynôme de $\mathbb{C}[X]$ a toujours une racine" (un petit DE ?). Une récurrence immédiate sur le degré de P montre alors que tout polynôme P de $\mathbb{C}[X]$ est scindé : notons $P \in \mathbb{C}[X]$; si P est constant il est scindé ; sinon il a une racine λ ; ainsi P est de la forme $P = (X-\lambda)Q$ et on a abaissé le degré de 1 ; on recommence sur Q jusqu'à tomber sur un polynôme constant.
Et voilà. □

II.3 Relations coefficients-racines

$P(X) = a_2X^2 + a_1X + a_0$
scindé de racine(s) λ_1 et λ_2

$$\begin{aligned} P(X) &= a_2(X-\lambda_1)(X-\lambda_2) \\ &= a_2(X^2 - (\lambda_1+\lambda_2X) + \lambda_1\lambda_2) \end{aligned}$$

En identifiant : $\lambda_1+\lambda_2 = -\frac{a_1}{a_2}$ et $\lambda_1\lambda_2 = \frac{+a_0}{a_2}$

Proposition 6 : Cas $n = 3$.

Supposons $a_3X^3 + a_2X^2 + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \lambda_3$. Alors :

$$\begin{cases} \frac{a_2}{a_3} = -(\lambda_1+\lambda_2+\lambda_3) \\ \frac{a_1}{a_3} = +(\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_2\lambda_3) \\ \frac{a_0}{a_3} = -\lambda_1\lambda_2\lambda_3 \end{cases}$$

Pour $n = 4$

$$\begin{aligned}
P(X) &= a_4X^4 + a_3X^3 + a_2 + X^2 + a_1X + a_0 \\
&= a_4\left((X-\lambda_1)(X-\lambda_2)(X-\lambda_3)(X-\lambda_4)\right) && \text{Car scindé de racines } \lambda_1,\lambda_2,\lambda_3,\lambda_4 \\
&= a_4(X^4 + (-\lambda_1-\lambda_2-\lambda_3-\lambda_4)X^3 \\
&+ (\lambda_1\lambda_2+\lambda_1\lambda_3+\lambda_1\lambda_4+\lambda_2\lambda_4+\lambda_3\lambda_4)X^2 \\
&+ (-\lambda_1\lambda_2\lambda_3-\lambda_1\lambda_2\lambda_4-\lambda_2\lambda_3\lambda_4-\lambda_1\lambda_3\lambda_4)X + \underbrace{\lambda_1\lambda_2\lambda_3\lambda_4}_{\text{produit}})
\end{aligned}$$

Théorème 12 : Cas général.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots, \lambda_n$.

On appelle k^e expression symétrique élémentaire le scalaire $\sigma_k = \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} \lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k}$.

Supposons $a_nX^n + \cdots + a_1X + a_0$ scindé de racines $\lambda_1, \lambda_2, \ldots \lambda_n$. Alors :

Pour tout $0 \leqslant i \leqslant n$ on a $\dfrac{a_i}{a_n} = (-1)^{n-i}\sigma_{n-i}$

En général on s'arrange pour avoir $a_n = 1$.

Exercice 5. Résoudre $\begin{cases} x+y+z = 5 \\ x^2+y^2+z^2 = \frac{33}{2} \\ xyz = 1. \end{cases}$

$$\begin{cases} x+y+z &= 0 \\ xy+yz+xz &= -1 \\ xyz &= 0 \end{cases}$$

a pour solution (x, y, z) tel que x, y, z sont les racines de

$$\begin{aligned}
P(X) &= (X-x)(X-y)(X-z) \\
&= X^3 - (x+y+z)X^2 + (xy+yz+xz)X - xyz \\
&= X^3 - X \\
&= X(X+1)(X+1)
\end{aligned}$$

$$S = \left(\begin{pmatrix}0\\1\\-1\end{pmatrix}, \begin{pmatrix}-1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\-1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\0\end{pmatrix}\right)$$

$$\begin{cases} x+y+z &= 5 \quad L_1 \\ x^2+y^2+z^2 &= \frac{33}{2} \quad L_2 \\ xyz &= 1 \quad L_3 \end{cases}$$

$$\begin{aligned}
L_1^2 &\Leftrightarrow (x+y+z)^2 = 25 \\
&\Leftrightarrow x^2+y^2+z^2+2(xy+xz+yz) = 25 \\
&\Leftrightarrow xy+xz+yz = \frac{25-(x^2+y^2+z^2)}{2} \\
&\Leftrightarrow xy+xz+yz = \frac{25-\frac{33}{2}}{2} = \frac{50-33}{4} \\
&\Leftrightarrow xy+xz+yz = \frac{17}{4}
\end{aligned}$$

Donc

$$(S) \Leftrightarrow \begin{cases} x+y+z & = 5 \\ xy+yz+xz & = \frac{17}{4} \\ xyz & = 1 \end{cases}$$
$$\Leftrightarrow x, y, z \text{ sont les racines de } X^3 - 5X^2 + \frac{17}{4}X - 1$$

... ou encore de $4X^3 - 20X^2 + 17 - 4 \in \mathbb{Z}[X]$.

Une racine évidente est de la forme $\frac{p}{q}$ avec $\begin{cases} p|a_0 = 4 \\ q|a_4 = 4 \end{cases}$

4 est une racine évidente car

$$\begin{aligned} 4 \cdot 4^3 - 20 \cdot 4^2 + 17 \cdot 4 - 4 &= 4(4^3 - 20 \cdot 4 + 17 - 1) \\ &= 4(64 - 80 + 16) \\ &= 0 \end{aligned}$$

$$\begin{array}{cccc|l} 4X^3 & -20X^2 & +17X & -4 & X-4 \\ 4X^3 & -16X^2 & & & 4X^2-4X+1 \\ \cline{5-5} & -4X^2 & +17X & -4 & \\ & -4X^2 & +16X & & \\ \cline{5-5} & & X & -4 & \\ & & & 0 & \end{array}$$

Donc

$$\begin{aligned} P(X) &= (X-4)(4X^2 - 4x + 1) \\ &= (X-4)(2X-1)^2 \end{aligned}$$

Conclusion

$$S = \left\{ \begin{pmatrix} 4 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ 4 \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 4 \end{pmatrix} \right\}$$

II.4 Multiplicité

Proposition-Définition 12 : Racines multiples.

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}$. Les trois propositions suivantes sont équivalentes :

i. $r = \max\{k \in \mathbb{N} \setminus \{0\},\ (X-\alpha)^k \text{ divise } P\}$.

ii. On peut écrire $P = (X-\alpha)^r Q$ avec $Q(\alpha) \neq 0$.

iii. $P(\alpha) = 0,\ P'(\alpha) = 0, \ldots,\ P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$.

Lorsqu'elles sont vérifiées, on dit que α est une racine de multiplicité r de P.

Pour $r = 1$ on parle de racine simple, pour $r = 2$ de racine double, pour $r = 3$ de racine triple, etc.

On parle de racine multiple dès qu'on a $r \geqslant 2$.

Exercice 6. Montrons-le.

$\boxed{i \implies ii}$

$r = \max\{k, (X-\alpha)^k | P\}$

En particulier $(X-\alpha)^r | P$ donc il existe $Q \in \mathbb{K}[X]$ tel que

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

Montrons $Q(\alpha) \neq 0$ par l'absurde. Supposons $Q(\alpha) = 0$. Alors α est racine de Q donc il existe $\tilde{Q} \in \mathbb{K}[X]$ tel que

$$Q = (X - \alpha)\tilde{Q}$$

d'où $P = (X - \alpha)^{r+1}\tilde{Q}$ ce qui contredit la maximalité de r.

$\boxed{ii \implies iii}$. On suppose qu'il existe $Q \in \mathbb{K}[X]$ tel que $\begin{cases} P & = (X-\alpha)^n Q \\ Q(\alpha) & \neq 0 \end{cases}$

Donc pour $n \in \mathbb{N}$ on a

$$\begin{aligned} P^{(n)} &= \sum_{k=0}^{n} \binom{n}{k} \left((X-\alpha)^r\right)^{(k)} Q^{(n-k)} \\ &= \sum_{k=0}^{n} \binom{n}{k} r(r-1)\cdots(r-k+1)(X-\alpha)^{r-k} Q^{(n-k)} \end{aligned}$$

Pour $n \in [\![0, \ldots, r-1]\!]$ et $k \leq n$ on a $r - k > 0$, donc pour $n \in [\![0, r-1]\!]$

$$\begin{aligned} P^{(n)}(\alpha) &= \sum_{k=0}^{n} \binom{n}{k} r(r-1)\cdots(r-k+1) \cdot 0 \cdot Q^{(n-k)} \\ &= 0 \end{aligned}$$

Pour $n = r$, on a

$$\begin{aligned} P^{(n)}(\alpha) &= P^{(r)}(\alpha) \\ &= \sum_{k=0}^{r-1} 0 + \binom{r}{r} r! \times 1 \times Q^{(0)}(\alpha) \\ &= r!Q(\alpha) \\ &\neq 0 \end{aligned}$$

$\boxed{iii \implies i}$ Supposons $P(\alpha) = \cdots = P^{(r-1)}(\alpha) = 0$ et $P^{(r)}(\alpha) \neq 0$
D'après la formule de Taylor sur les polynômes,

$$\begin{aligned} P &= \sum_{k=0}^{\deg P} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \underbrace{\sum_{k=0}^{r-1} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k}_{0} + \sum_{k=r}^{\deg P} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k \\ &= \sum_{i=0}^{\deg P - r} \frac{P^{(r+i)}(\alpha)}{(r+i)!}(X-\alpha)^{r+i} \\ &= (X-\alpha)^r \sum_{i=0}^{\deg P - r} \frac{P^{(r+i)}(\alpha)}{(r+i)!}(X-\alpha)^i \\ &=: (X-\alpha)^r Q(X) \end{aligned}$$

Ainsi, $(x-\alpha)^r | P$
Reste à montrer que $(X-\alpha)^{r+1} \not| P$
Montrons-le par l'absurde. Supposons $(X-\alpha)^{r+1} | P = (X-\alpha)^r Q(X)$
On a donc $X - \alpha | Q$ donc $Q(\alpha) = 0$
donc $\dfrac{P^{(r)}(\alpha)}{r!} = 0$ donc $P^{(r)}(\alpha) = 0$. $\boxed{\lightning}$ □

Remarque 10

L'exercice CCINP $n°85$ consiste essentiellement en cette question de cours !

Remarque 11

Avec la définition précédente, on peut donc dire que α est racine de multiplicité 0 de P si et seulement si ce n'est pas une racine de P (c'est dans le programme). On peut aussi dire que tout scalaire est racine de multiplicité infinie du polynôme nul.

Remarque 12

Si P est un polynôme admettant des racines distinctes α_i, pour $i \in \{1, \dots, s\}$, de multiplicités respectives r_i, alors P est divisible par $(X-\alpha_1)^{r_1}(X-\alpha_2)^{r_2}\dots(X-\alpha_s)^{r_s} = \prod_{i=1}^{s}(X-\alpha_i)^{r_i}$.

Exercice 7. Donner tous les polynômes de degré 6 admettant 1 comme racine de multiplicité 2 et -1 comme racine de multiplicité 3.
P est de degré 6.

$$(X-1)^2(X+1)^3 | P \qquad 1 \text{ racine double et } -1 \text{ racine triple.}$$

Donc P est de la forme $(X-1)^2(X+1)^3 Q$ avec $\begin{cases} Q(1) & \neq 0 \\ Q(-1) & \neq 0 \end{cases}$.
$\deg P = 6$ donc $\deg Q = 1$ ie $Q = \alpha(X+\lambda)$ avec $\begin{cases} \alpha & \neq 0 \\ \lambda & \neq \pm 1 \end{cases}$
Finalement,

$$S = \left\{\alpha(X-1)^2(X+1)^3(X-\lambda), (\alpha,\lambda) \in \mathbb{R}^\times \times \mathbb{R} \setminus \{\pm 1\}\right\}$$

Corollaire 3 .

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

1. P a au plus n racines **comptées avec leur multiplicité**.
2. P est scindé si et seulement si il a n racines **comptées avec leur multiplicité**.
3. Si P a au moins $n+1$ racines **comptées avec multiplicité**, c'est le polynôme nul.

II.5 Racines complexes d'un polynôme de $\mathbb{R}[X]$

Définition 13 .

Pour $P \in \mathbb{C}[X]$, on appelle **polynôme conjugué** de $P = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ le polynôme $\overline{P}$ défini par $\overline{P}(X) = \overline{a_0} + \overline{a_1}X + \overline{a_2}X^2 + \dots + \overline{a_n}X^n$.

Remarque 13

La conjugaison étant un automorphisme de corps involutif sur $\mathbb{C}$ elle induit un automorphisme d'anneau involutif sur $\mathbb{C}[X]$. Elle est de plus compatible avec la dérivation et avec $P \mapsto \tilde{P}$.

Remarque 14 $\overline{P} = P \Leftrightarrow P \in \mathbb{R}[X]$. **C'est à ça que sert à la conjugaison des polynômes.**

Corollaire 4 .

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

1. α racine de $P \Leftrightarrow \overline{\alpha}$ racine de P.
2. α racine de P de multiplicité $k \Leftrightarrow \overline{\alpha}$ racine de P de multiplicité k.

Démonstration. 1. Il suffit de montrer l'implication directe par involutivité de la conjugaison.

Supposons $P(\alpha) = 0$. On a $P \in \mathbb{R}[X]$ donc $\overline{P} = P$.

On conjugue : $\overline{P(\alpha)} = \overline{0}$ *i. e.* $\overline{P}(\overline{\alpha}) = 0$ *i. e.* $P(\overline{\alpha}) = 0$. Youpie.

2. Il suffit de montrer l'implication directe par involutivité de la conjugaison.

α est racine de P de multiplicité k signifie que α est racine de P, P', …, $P^{(k-1)}$ mais pas de $P^{(k)}$.

On utilise le point 1. sur P, P', …, $P^{(k-1)}$ et sa contraposée sur $P^{(k)}$.

□

Corollaire 5 .

Soit $P \in \mathbb{R}_{2n+1}[X]$. Alors P a une racine **réelle**.

Démonstration. D'après d'Alembert-Gauss, P a $2n+1$ racines complexes comptées avec multiplicité.

Or P est à coefficients réels donc ses racines vont par paires avec leur conjugué qui a la même multiplicité.

Montrons que l'une est réelle par l'absurde : si ce n'était pas le cas on aurait un nombre pair de racines comptées avec leur multiplicité. C'est une contradiction. □

On aurait aussi pu utiliser le TVI !

III Arithmétique dans $\mathbb{K}[X]$

Lorsqu'on a un anneau, on a une arithmétique (qui consiste, essentiellement, en l'étude de sa relation de divisibilité). L'arithmétique d'un anneau dans lequelle on a un théorème de division euclidienne est essentiellement la même que celle de $\mathbb{Z}$: nous allons l'illustrer ici, en prenant notre sur cours sur $\mathbb{Z}$ et en le recopiant. Recopier, c'est le bien. Avec l'ordinateur en plus ça va vite.

III.1 Divisibilité des polynômes

Définition 14 .

On dit d'un polynôme B de $\mathbb{K}[X]$ qu'il divise un polynôme A de $\mathbb{K}[X]$, et on écrit $B \mid A$, lorsqu'il existe un polynôme C de $\mathbb{K}[X]$ vérifiant $A = BC$. On dit alors de B qu'il est un diviseur de A, et de A qu'il est un multiple de B.

Notation 3

- L'ensemble des multiples de P dans $\mathbb{K}[X]$ se note $P\mathbb{K}[X]$.
- On pourra, comme dans $\mathbb{Z}$, noter $D(P)$ l'ensemble des diviseurs de P.

Proposition 7 : Inversibles de $\mathbb{K}[X]$. L'ensemble des inversibles de $\mathbb{K}[X]$ est $\mathbb{K}[X]^\times = \mathbb{K}^*$

Démonstration. $\boxed{\supset}$ Si $c \in \mathbb{K}^*$ alors c est inversible puisque son inverse est c^{-1}.

$\boxed{\subset}$ Soit P un polynôme inversible et notons Q son inverse. On a $PQ = 1$ donc $\deg(PQ) = 0$.
D'après la formule des degrés $\deg(P) + \deg(Q) = 0$. Donc $\deg(P) = \deg(Q) = 0$ et en particulier $P \in \mathbb{K}^*$. □

Proposition 8 .

La relation de divisibilité sur $\mathbb{K}[X]$ est réflexive et transitive mais n'est pas antisymétrique.

Si on la restreint à l'ensemble $\mathcal{U}$ des polynômes unitaires de $\mathbb{K}[X]$, elle devient alors antisymétrique et est par conséquent une relation d'ordre sur $\mathcal{U}$. Idem sur $\mathcal{U} \cup \{0\}$ si on ne veut pas se priver du polynôme nul.

Démonstration.
- Réflexivité : soit $P \in \mathbb{K}[X]$. On a $1 \in \mathbb{K}[X]$ et $P = 1 \times P$ donc $P \mid P$.
- Transitivité : soient $P, Q, R \in \mathbb{K}[X]$ et supposons $P \mid Q$ et $Q \mid R$. Il existe donc $S, T \in \mathbb{K}[X]$ tels que $Q = PS$ et $R = QT$, donc $R = P(ST)$ et donc $P \mid R$.
- La relation de divisibilité n'est pas antisymétrique sur $\mathbb{K}[X]$: $3X^2 \mid X^2$ et $X^2 \mid 3X^2$ mais $X^2 \neq 3X^2$.
- Plaçons-nous maintenant dans $\mathcal{U} \cup \{0\}$: soit $(P, Q) \in \left(\mathcal{U} \cup \{0\}\right)^2$ et supposons $P \mid Q$ et $Q \mid P$. Il existe $S \in \mathbb{K}[X]$ tel que $Q = SP$ et il existe $T \in \mathbb{K}[X]$ tel que $P = TQ$. On en déduit $P = STP$ et donc on a soit $P = 0$, soit $ST = 1$ par intégrité.
- Évidemment, restreindre une relation antisymétrique donne une relation antisymétrique, donc la divisibilité est aussi un ordre sur $\mathcal{U}$. □

On retiendra donc que $\mathcal{U}$ **joue dans** $\mathbb{K}[X]$ **le rôle joué dans** $\mathbb{Z}$ **par** $\mathbb{N} \setminus \{0\}$.

Proposition-Définition 15 .

On dit de deux polynômes P et Q qu'ils sont associés lorsqu'une des propositions suivantes est vérifiées :
- $P \mid Q$ et $Q \mid P$;
- il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.

L'association est donc la relation d'équivalence canoniquement associée à la divisibilité. La multiplication par un scalaire non nul joue dans $\mathbb{K}[X]$ le rôle joué par la multiplication par ± 1 dans $\mathbb{Z}$. On retrouve bien que $\mathcal{U}$ joue dans $\mathbb{K}[X]$ le rôle joué dans $\mathbb{Z}$ par $\mathbb{N} \setminus \{0\}$. On voit en particulier que tout polynôme non nul est associé à un unique polynôme unitaire.

Démonstration. $\boxed{\Rightarrow}$ Soit $(P, Q) \in \mathbb{K}[X]^2$ tels que $P|Q$ et $Q|P$.
Ainsi il existe $C \in \mathbb{K}[X]$ tel que $P = QS$ et $T \in \mathbb{K}[X]$ tel que $Q = PT$.
On a en particulier les relations $\deg(P) = \deg(Q) + \deg(S)$ et $\deg(Q) = \deg(P) + \deg(T)$, dont on déduit en réinjectant : $\deg(S) + \deg(T) = 0$. Et donc $\deg(S) = \deg(T) = 0$. Ainsi S est un polynôme constant non nul ; en posant $\lambda = S$, on a bien $P = \lambda Q$ avec $\lambda \in \mathbb{K}^*$.
$\boxed{\Leftarrow}$ λ et $\frac{1}{\lambda}$ sont dans $\mathbb{K}[X]$ donc lol. □

III.2 Propriétés algébriques de la divisibilité

Proposition 9 .

La divisibilité est stable par :
- CL : si $C \mid A$ et $C \mid B$ alors $C \mid AU + BV$.
- Produit : $\begin{cases} \text{si } A \mid B \text{ alors } AC \mid BC \,; \\ \text{si } A \mid B \text{ et } P \mid Q \text{ alors } AP \mid BQ. \end{cases}$
- Puissances : si $n \in \mathbb{N}$ et $A \mid B$ alors $A^n \mid B^n$.

Démonstration. Fastoche (recopier le cours sur $\mathbb{Z}$). □

Proposition 10 .

La divisibilité est invariante par extension de corps : si $P,\ Q \in \mathbb{R}[X]$ alors $P \mid Q$ dans $\mathbb{R}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{C}[X]$.

Démonstration. Immédiat car il suffit d'utiliser le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

III.3 PGCD

Définition 16 .

Soient P et Q dans $\mathbb{K}[X]$.
1. On dit que D est **un** pgcd de P et Q lorsque c'est un plus grand diviseur de P et de Q (pour la divisibilité).
2. Il existe un unique pgcd unitaire (ou nul), on l'appelle **le** pgcd et on le note $\mathrm{PGCD}(P, Q)$ ou $P \wedge Q$.

Exercice 8. Reformuler cette définition.

— — $D|P$ et $D|Q$
— $\forall R \in \mathbb{K}[X], (R|P \text{ et } R|Q) \implies R|D$

— $P \wedge Q = \inf_{(\mathcal{U}\cup\{0\},\ |)}\{P, Q\}$
— $\mathcal{D}(D) = \mathcal{D}(P) \cap \mathcal{D}(Q)$

Proposition 11 : Propriétés immédiates du PGCD.

- Homogénéité : si K est unitaire alors $KA \wedge KB = K(A \wedge B)$;
- Commutativité : $B \wedge A \ = \ A \wedge B$;
- Associativité : $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.

Pour montrer l'existence, ne faisons pas comme dans $\mathbb{Z}$ (on pourrait), mais utilisons l'algorithme d'Euclide.

Lemme 1 : Lemme préparatoire à l'algorithme d'Euclide.

1. Si R est le reste dans la division euclidienne de A par B alors $A \wedge B = B \wedge R$.
2. Si D est unitaire, $D \wedge 0 = D$.

Démonstration. 1. Il suffit de montrer que les diviseurs communs à A et B sont les mêmes que les diviseurs communs à B et R. Cela provient de la stabilité par CL avec les deux CL $A = BQ + R$ et $R = A - BQ$.
2. Les diviseurs communs à D et 0 sont juste les diviseurs de D d'où le résultat.

□

L'existence du PGCD est assurée par l'algorithme d'Euclide :

- On pose $R_0 = A$ et $R_1 = B$.
- Tant que $R_{n+1} \neq 0$ on définit R_{n+2} comme le reste dans la DE de R_n par R_{n+1}.
- Le PGCD est le dernier reste non nul R_n (au coefficient dominant près).

Reste à montrer la terminaison et la correction de cet algorithme.

Démonstration. On copie le cours sur $\mathbb{Z}$.

- Terminaison : par division euclidienne, pour tout $n \geqslant 1$ tel que $R_n \neq 0$, on a $\deg(R_{n+1}) < \deg(R_n)$. On a donc $\deg(B) = \deg(R_1) > \deg(R_2) > \deg(R_3) > \cdots$. Comme il n'y a qu'un nombre fini d'éléments dans $\{-\infty\} \cup \{0, \dots, \deg(B)\}$, il existe nécessairement un rang $N \geqslant 2$ tel que $\deg(R_N) = -\infty$, c'est-à-dire $R_N = 0$ et $\deg(R_{N-1}) \geqslant 0$. D'où la terminaison.
- Correction : on a alors, par le lemme préparatoire, $R_{n-1} \wedge R_n = R_n \wedge R_{n+1}$ pour tout $n \in \{1, \dots, N-1\}$. Donc : $A \wedge B = R_0 \wedge R_1 = R_1 \wedge R_2 = \cdots = R_{N-2} \wedge R_{N-1} = R_{N-1} \wedge R_N = R_{N-1} \wedge 0$. Le PGCD est donc associé à R_{N-1}.□

Exercice 9. Calculons par exemple $\left(X^6 + 1\right) \wedge \left(X^4 + 1\right)$.

Théorème 13 : Théorème d'Eudoxe (théorème "sur la relation de Bézout").

Si $D = A \wedge B$ alors $\exists (U, V) \in \mathbb{K}[X]^2,\ AU + BV = D$.

Formulation moderne : pour D unitaire : $D = A \wedge B \Leftrightarrow A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.

Démonstration. Il suffit de remonter l'algorithme d'Euclide. □

Exercice 10. Trouvons une relation de Bézout pour $A = X^6 + 1$ et $B = X^4 + 1$.

Proposition 12 .

Le PGCD est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le pgcd de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

Démonstration. Immédiat d'après le lien divisibilité/division euclidienne et l'invariance de la division euclidienne par extension de corps. □

Exercice 11. Calculons $\left(X^6 - 1\right) \wedge \left(X^4 - 1\right)$.

III.4 Polynômes premiers entre eux

Définition 17 .

On dit que deux polynômes P et Q sont premiers entre eux lorsque $P \wedge Q = 1$.

Proposition 13 .

Le caractère "premiers entre eux" est invariant par extension de corps : $P,\ Q \in \mathbb{R}[X]$ sont premiers entre eux dans $\mathbb{R}[X]$ si et seulement si ils le sont dans $\mathbb{C}[X]$.

Remarque 15

L'homogénéïté entraîne que si A et B sont non nuls et D est leur PGCD, alors $\dfrac{A}{D}$ et $\dfrac{B}{D}$ sont premiers entre eux.

Théorème 14 : Théorème de Bézout.

Soient A et B deux polynômes. On a $A \wedge B = 1 \Leftrightarrow \exists (U,V),\ AU + BV = 1$.

Démonstration. $\boxed{\Rightarrow}$ C'est Eudoxe.
$\boxed{\Leftarrow}$ Si $AU + BV = 1$ par stabilité par CL $A \wedge B | 1$ donc $A \wedge B = 1$. □

Théorème 15 : Lemme de Gauss.

Si $\begin{cases} A \wedge B = 1 \\ A | BC \end{cases}$ alors $A | C$.

Démonstration. Comme dans $\mathbb{Z}$... exercice. □

III.5 PPCM

Définition 18 .

Soient P et Q dans $\mathbb{K}[X]$.

1. On dit que M est **un** ppcm de P et Q lorsque c'est un plus petit multiple de P et de Q.
2. Il existe un unique ppcm unitaire (ou nul), on l'appelle **le** ppcm et on le note $\text{ppcm}(P,Q)$ ou $P \vee Q$.

Exercice 12. Reformuler cette définition.

Proposition 14 : Propriétés immédiates du PPCM.

- Homogénéité : si K est unitaire alors $KA \vee KB = K(A \vee B)$;
- Commutativité : $B \vee A \ = \ A \vee B$;
- Associativité : $(A \vee B) \vee C = A \vee (B \vee C)$.

Pour montrer l'existence, on peut s'appuyer sur la remarque suivante (démonstration en exercice) :

Remarque 16

Si A et B sont unitaires, alors $(A \wedge B) \times (A \vee B) = A \times B$.

Exercice 13. $(X^6-1) \vee (X^4-1) = (X-i)(X+i)(X-j)(X-\bar{j})(X+j)(X+\bar{j}) = (X^2+1)(X^2+X+1)(X^2-X+1)$.

Proposition 15 .

Le PPCM est invariant par extension de corps : si $P, Q \in \mathbb{R}[X]$ alors le ppcm de P et Q dans $\mathbb{R}[X]$ est le même que dans $\mathbb{C}[X]$.

III.6 Polynômes irréductibles

On cherche un analogue à la décomposition d'un nombre entier en produit de nombres premiers. Pour cela on commence par s'interroger sur l'analogue dans $\mathbb{K}[X]$ de la notion de nombre premier, ce qu'on appellera polynôme irréductible.

Définition 19 .

Un polynôme $P \in \mathbb{K}[X] \setminus \mathbb{K}$ est dit irréductible lorsqu'on a :

$$\forall (U,V) \in \mathbb{K}[X]^2,\ P = UV \ \Rightarrow \begin{cases} U \text{ inversible} \\ V \text{ associé à } P \end{cases} \text{ ou } \begin{cases} U \text{ associé à } P \\ V \text{ inversible} \end{cases}$$

Exemples 2

1. $X^2 + X + 1$ est irréductible dans $\mathbb{R}$.
2. $X^2 + X + 1$ n'est pas irréductible dans $\mathbb{C}$ puisque $X^2 + X + 1 = (X - j)(X - \overline{j})$.
3. $aX + b$ avec $a \neq 0$ est toujours irréductible dans $\mathbb{K}$.

/!\ La notion de polynôme irréductible dépend donc du corps considéré.

Théorème 16 : Théorème de décomposition.

Tout polynôme peut s'écrire comme produit de polynômes irréductibles, de façon unique à l'ordre des facteurs près et à association près.

Exercice 14. Le démontrer.

Notons que décomposer deux polynômes en produit d'irréductibles permet d'en calculer le pgcd et le ppcm.

Le théorème de d'Alembert-Gauss se reformule :

Théorème 17 : Irréductibles de $\mathbb{C}$.

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

Théorème 18 : Irréductibles de $\mathbb{R}$.

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

— les $X - \lambda,\ \lambda \in \mathbb{R}$;

— les $X^2 + bX + c,\ \Delta < 0$.

Démonstration. Exercice. □

Exemple 3 $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$.