

POLYNÔMES À UNE INDÉTERMINÉE

Dans tout le chapitre, n, p, q, m, r et s désignent des entiers naturels et r et s non nuls. K désigne \mathbb{R} ou \mathbb{C} . Les éléments de K sont appelés des scalaires.

Introduction : RAPPELS A LIRE EN AUTONOMIE ...

- Soit f une fonction polynomiale réelle telle que : $\forall t \in \mathbb{R}, f(t) = a_0 + a_1 t + \dots + a_p t^p$ où p entier naturel et a_0, \dots, a_p réels appelés coefficients de f (a_k étant le coefficient de rang k). Alors, ou bien tous les a_k sont nuls et f est la fonction nulle et a pour degré $-\infty$. ou bien l'un des a_k est non nul et le degré de f noté $\deg(f)$ est le plus grand entier k tel que $a_k \neq 0$. Deux fonctions polynomiales sont égales lorsqu'elles ont les mêmes coefficients. Une racine réelle (resp. complexe) de f est un réel (resp complexe) α tel que $f(\alpha) = 0$.

- Soit f et g deux fonctions polynomiales telles que : $\forall t \in \mathbb{R}, f(t) = a_0 + a_1 t + \dots + a_p t^p = \sum_{k=0}^p a_k t^k$ et $g(t) = b_0 + b_1 t + \dots + b_q t^q = \sum_{k=0}^q b_k t^k$ où p et q entiers naturels et $a_0, \dots, a_p, b_0, \dots, b_q$ réels avec a_p et b_q non nuls. Donc $\deg(f) = p$ et $\deg(g) = q$. Quitte à ajouter des termes nuls dans l'expression de f ou celle de g , on peut écrire : $f(t) = a_0 + a_1 t + \dots + a_m t^m = \sum_{k=0}^m a_k t^k$ et $g(t) = b_0 + b_1 t + \dots + b_m t^m = \sum_{k=0}^m b_k t^k$ où $m = \max(p, q)$. Alors,

$$(f + g)(t) = f(t) + g(t) = a_0 + b_0 + (a_1 + b_1)t + \dots + (a_m + b_m)t^m = \sum_{k=0}^m (a_k + b_k)t^k$$

$$(f \times g)(t) = f(t) \times g(t) = a_0 b_0 + (a_0 b_1 + a_1 b_0)t + (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + \dots + (a_p b_q)t^{p+q} = \sum_{k=0}^{p+q} c_k t^k$$

$c_k = \sum_{j=0}^k a_j b_{k-j}$. De plus, $\deg(f + g) \leq m = \max(p, q)$ car je ne sais pas si $a_m + b_m = 0$ et $\deg(fg) = p + q$ car $a_p b_q \neq 0$.

On va définir un ensemble plus abstrait et plus large que l'ensemble des fonctions polynomiales vérifiant quasiment les mêmes propriétés qui va nous permettre de travailler avec des polynômes de matrices, d'endomorphismes... Pour cela, on va définir un polynôme par la suite de ses coefficients.

I Généralités

1. Définitions et opérations

1 Def : Un polynôme à coefficients dans K est une suite d'éléments de K nulle à partir d'un certain rang (dite presque nulle), c'est donc un objet de la forme $P = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$ où $n \in \mathbb{N}$, a_0, a_1, \dots, a_n sont des éléments de K et sont appelés les coefficients de P .

2NB : D'après l'égalité de deux suites, deux polynômes sont égaux s'ils ont les mêmes coefficients.

On définit trois opérations sur les polynômes à coefficients dans K : une addition entre polynômes, une multiplication d'un polynôme par un scalaire et une multiplication entre polynômes.

3 Def : Soit P et Q deux polynômes à coefficients dans K . Soit $\alpha \in K$. On pose $P = (a_0, a_1, a_2, \dots, a_p, 0, 0, \dots) = (a_n)_{n \in \mathbb{N}}$ tel que $\forall n > p, a_n = 0$ et $Q = (b_0, b_1, b_2, \dots, b_q, 0, 0, \dots) = (b_n)_{n \in \mathbb{N}}$ tel que $\forall n > q, b_n = 0$. $P + Q = (a_n + b_n)_{n \in \mathbb{N}} = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_m + b_m, 0, 0, \dots)$ où $m = \max(p, q)$. $\lambda P = (\lambda a_0, \lambda a_1, \lambda a_2, \dots, \lambda a_p, 0, 0, \dots) = (\lambda a_n)_{n \in \mathbb{N}}$. $P \times Q = (c_n)_{n \in \mathbb{N}}$ tel que $\forall n \in \mathbb{N}, c_n = \sum_{k=0}^n a_k b_{n-k} = \sum_{k=0}^n a_{n-k} b_k$. **Prop :** $P + Q, \lambda P$ et $P \times Q$ ainsi définis sont des polynômes à coefficients dans K .

Démo3 : $P + Q, PQ$ et λP sont des suites d'éléments de K . Il est clair que $P + Q$ et λP sont des suites presque nulles. Vérifions que $P \times Q$ est une suite presque nulle : Soit $n > p + q$. Alors $c_n = \sum_{k=0}^n a_k b_{n-k} \stackrel{\text{car } \forall k > p, a_k = 0}{=} \sum_{k=0}^p a_k b_{n-k} \stackrel{\text{car } \forall k \leq p, n-k \geq n-p > q \text{ donc } b_{n-k} = 0}{=} 0$.

OK !

4 Def : Soit P un polynôme à coefficients dans K . Par convention, $P^0 = (1, 0, 0, \dots)$ et $\forall m \in \mathbb{N}^*, P^m = P^{m-1} \times P$.

NB : cela revient à dire que $\forall m \in \mathbb{N}^*, P^m = \underbrace{P \times P \times \dots \times P}_{m \text{ fois}}$

2. Nouvelle écriture d'un polynôme-Indéterminée.

5 Déf.: On note X la suite presque nulle $X = (0,1,0,0, \dots)$. X est appelée l'indéterminée.

X n'est pas un scalaire, c'est un polynôme i.e. une suite presque nulle. On ne doit pas écrire " $X = 2$ " (HORREUR!).

6 Théo.: $\forall k \in \mathbb{N}, X^k$ est la suite presque nulle : $X^k = \left(\underset{u_0}{0}, 0, \dots, 0, \underset{u_k}{1}, 0, 0, \dots \right) = (u_n)$ tq $u_n = \begin{cases} 0 & \text{si } n \neq k \\ 1 & \text{si } n = k \end{cases}$

Démo 6 par récurrence sur k . Notons \mathcal{H}_k la propriété : $X^k = \left(\underset{u_0}{0}, 0, \dots, 0, \underset{u_k}{1}, 0, 0, \dots \right)$.

Init : par définition de P^0 , $X^0 = (1,0,0, \dots)$. Donc, \mathcal{H}_0 est vraie.

Propag : Soit k un entier naturel. Je suppose que \mathcal{H}_k est vraie et sous cette hypothèse, je vais prouver que \mathcal{H}_{k+1} est vraie.

On sait que : $X^k = \left(\underset{u_0}{0}, 0, \dots, 0, \underset{u_k}{1}, 0, 0, \dots \right) = (u_n)$ tq $\forall n \neq k, u_n = 0$ et $u_k = 1$ et $X = \left(\underset{v_0}{0}, \underset{v_1}{1}, \dots, 0, 0, \dots \right) = (v_n)$ tq que:

$\forall n \neq 1, v_n = 0$ et $v_1 = 1$. Posons $X^{k+1} = X^k X = (c_n)_{n \in \mathbb{N}}$. Alors $c_n = \sum_{l=0}^n u_l v_{n-l}$.

Donc, Si $n < k$ alors $c_n = \sum_{l=0}^n u_l v_{n-l} \stackrel{\text{car } u_l=0 \text{ si } l < k}{=} 0$.

Si $n \geq k$ alors $c_n = \sum_{l=0}^n u_l v_{n-l} \stackrel{\text{car } u_l=0 \text{ si } l \neq k}{=} u_k v_{n-k} = v_{n-k} \stackrel{\text{car } v_l=0 \text{ si } l \neq 1}{=} \begin{cases} 0 & \text{si } n-k \neq 1 \\ 1 & \text{si } n-k = 1 \end{cases}$

Ainsi, $X^{k+1} = \left(\underset{c_0}{0}, 0, \dots, 0, \underset{c_{k+1}}{1}, 0, 0, \dots \right)$.. OK.

CCL : le théorème de récurrence assure que $\forall k, \mathcal{H}_k$ est vraie. OK !

Alors d'après les opérations sur les polynômes, on a : $\forall (a_1, a_2, \dots, a_n) \in K^{n+1}$,

$a_0 X^0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} + a_n X^n = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, a_2, 0, \dots) + \dots +$

$(0, 0, \dots, 0, a_n, 0, 0, \dots) = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) =$ la suite nulle à partir du rang $n+1$ dont les premiers termes sont a_0, \dots, a_n . On peut donc dire que :

7 Nouvelle écriture d'un polynôme :

Tout polynôme à coefficients dans K s'écrit de manière unique (**) sous la forme :

$$P = a_0 X^0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} + a_n X^n = \sum_{k=0}^n a_k X^k \text{ (forme développée de } P\text{)}.$$

où $n \in \mathbb{N}, a_0, a_1, \dots, a_n$ sont des éléments de K , appelés coefficients de P et X est l'indéterminée.

P est aussi noté $P(X)$.

On note $\mathbf{K}[X]$ l'ensemble des polynômes (à une indéterminée et) à coefficients dans K .

(**) d'après l'égalité de deux polynômes.

8 Polynômes particuliers :

- On note $0 = 0X^0 + 0X + 0X^2 + \dots + 0X^{n-1} + 0X^n$ le polynôme nul. Le polynôme nul est le seul polynôme dont tous les coefficients sont tous nuls.

Tout polynôme non nul peut s'écrire sous la forme $P = \sum_{k=0}^p a_k X^k$ tq $a_p \neq 0$.

- Tout polynôme βX^0 (où $\beta \in K$) est noté β et appelé polynôme constant. De même, $a_0 X^0 \stackrel{\text{noté}}{=} a_0$.
- Pour tout $\lambda \in K^*$ et tout $k \in \mathbb{N}$, $\lambda X^k = 0 + 0X + 0X^2 + \dots + 0X^{k-1} + \lambda X^k + 0X^{k+1}$ est un monôme (polynôme avec un seul coefficient non nul).

9 Déf: A tout polynôme $P = a_0 X^0 + a_1 X + a_2 X^2 + \dots + a_{n-1} X^{n-1} + a_n X^n = \sum_{k=0}^n a_k X^k$, on associe la fonction polynomiale

\tilde{P} définie par : $\forall t \in K, \tilde{P}(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_{n-1} t^{n-1} + a_n t^n = \sum_{k=0}^n a_k t^k$.

\tilde{P} est une fonction de K dans K .

10 Attention : P et \tilde{P} sont deux objets de natures mathématiques distinctes : $P \neq \tilde{P}$.

11 notation : On note souvent E l'ensemble des fonctions polynomiales de \mathbb{R} dans \mathbb{R} .

3. Propriétés de l'addition et la multiplication polynomiales et de la multiplication (externe) par un scalaire- Composition.

12 Nouvelles écritures de $P + Q, PQ$ et λP - Combinaison linéaire.

Soit $P = \sum_{k=0}^p a_k X^k$ et $Q = \sum_{k=0}^q b_k X^k$ deux éléments de $K[X]$ et λ un élément de K . Alors,

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

$$\lambda P = \sum_{k=0}^p \lambda a_k X^k$$

$$P \times Q = PQ = \sum_{k=0}^{p+q} c_k X^k \quad \text{tel que } c_k = \sum_{l=0}^k a_l b_{k-l} = \sum_{l=0}^k a_{k-l} b_l = \sum_{\substack{0 \leq i, j \leq k \\ i+j=k}} a_i b_j$$

somme double

Pour tous scalaires α et β , $\alpha P + \beta Q = \sum_{k=0}^{\max(p,q)} (\alpha a_k + \beta b_k) X^k$ est appelé une combinaison linéaire de P et Q et est un élément de $K[X]$.

13 Règles de calcul

Soit P, Q et R trois éléments de $K[X]$, μ et γ deux scalaires. Alors,

1. $(P + Q) + R = P + (Q + R) \stackrel{\text{noté}}{\equiv} P + Q + R$
2. $P + Q = Q + P$
3. $P + 0 = P = 0 + P$
4. $P + (-1)P = 0$
5. $\gamma(P + Q) = \gamma P + \gamma Q$
6. $(\gamma + \mu)P = \gamma P + \mu P$
7. $1P = P$
8. $(\mu\gamma)P = \mu(\gamma P) = \gamma(\mu P) \equiv \gamma\mu P$
9. $(PQ)R = P(QR) \equiv PQR$
10. $PQ = QP$
11. $(P + Q)R = PR + QR$ et $R(P + Q) = RP + RQ$
12. $\gamma(PQ) = P(\gamma Q) = (\gamma P)Q \equiv \gamma PQ$
13. $PQ = 0 \Leftrightarrow P = 0$ ou $Q = 0$ (produit polynôme intègre)
14. $\forall (k, l) \in \mathbb{N}^2, X^k X^l = X^{k+l}$.

Démo : Posons $P = (a_n), Q = (b_n),$ et $R = (c_n),$

9) Montrons que $(PQ)R = P(QR)$ i.e. que ces deux polynômes ont les mêmes coefficients.

Posons $PQ = (\theta_n), (PQ)R = (\mu_n),$ et $QR = (u_n)$ et $P(QR) = (v_n)$. Soit $n \in \mathbb{N}$.

D'une part, $\theta_n = \sum_{k=0}^n a_k b_{n-k}$ et $\mu_n = \sum_{k=0}^n \theta_k c_{n-k}$. Donc, $\mu_n = \sum_{k=0}^n (\sum_{i=0}^k a_i b_{k-i}) c_{n-k} = \sum_{k=0}^n \sum_{i=0}^k a_i b_{k-i} c_{n-k}$

$\mu_n = \sum_{i=0}^n \sum_{k=i}^n a_i b_{k-i} c_{n-k} = \sum_{i=0}^n \sum_{l=0}^{n-i} a_i b_l c_{n-l-i}$.

D'autre part, $\forall n \in \mathbb{N}, u_n = \sum_{k=0}^n b_k c_{n-k}$ et $v_n = \sum_{k=0}^n a_k u_{n-k}$. Donc, $v_n = \sum_{k=0}^n a_k \sum_{j=0}^{n-k} b_j c_{n-k-j} = \sum_{k=0}^n \sum_{j=0}^{n-k} a_k b_j c_{n-k-j}$.

Donc, $\mu_n = v_n$. Ainsi $(PQ)R = P(QR)$ puisqu'ils ont les mêmes coefficients.

13) Montrons que : $PQ = 0$ si et seulement si $P = 0$ ou $Q = 0$.

D'après la définition du produit de deux polynômes, si $P = 0$ ou $Q = 0$ alors $PQ = 0$.

Montrons la réciproque par contraposée. Montrons que si P et Q sont non nuls alors PQ est non nul.

Supposons donc que P et Q sont non nuls. Alors on peut écrire $P = \sum_{k=0}^p a_k X^k$ et $Q = \sum_{k=0}^q b_k X^k$ avec $a_p \neq 0$ et $b_q \neq 0$.

Donc, $PQ = \sum_{k=0}^{p+q} \theta_k X^k$ vérifie : $\theta_{p+q} = \sum_{l=0}^{p+q} \underbrace{a_l}_{\substack{\text{nul} \\ \text{si } l > p}} \underbrace{b_{p+q-l}}_{\substack{\text{nul} \\ \text{si } l < p}} = a_p b_q \neq 0$. Donc PQ non nul.

14) Soit $(k, l) \in \mathbb{N}^2$. Si $k = 0$ alors $X^0 X^l = 1 X^l = X^l$ (d'après 7).

Si $k > 0$ alors $X^k X^l = (X^{k-1} X) X^l = X^{k-1} (X X^l) = X^{k-1} X^{l+1} \stackrel{\text{si } k > 1, \text{ alors } X^{k-1} = X^{k-2} X}{=} \dots = X^{l+k}$.

14 NB: ce sont quasiment les mêmes règles de calcul que dans K sauf que l'inverse d'un polynôme n'existe pas dans $K[X]$ donc on n'écrit pas $\frac{P}{Q}$. Par contre, on pourra utiliser le théorème de division euclidienne.

15 Généralisation : Soit P_1, P_2, \dots, P_m des éléments de $K[X]$ et β_1, \dots, β_m des éléments de K .

$\prod_{k=1}^m P_k$ est le produit des polynômes P_1, P_2, \dots, P_m .

$\sum_{k=1}^m \beta_k P_k$ est une combinaison linéaire des polynômes P_1, P_2, \dots, P_m .

16 Prop : Formule du binôme de Newton et formule de factorisation

pour tous polynômes P et Q et tout entier naturel m ,

$$(P + Q)^m = \sum_{j=0}^m \binom{m}{j} P^j Q^{m-j} \quad \text{et si } m \text{ non nul, } P^m - Q^m = (P - Q) \left(\sum_{j=0}^{m-1} P^j Q^{m-1-j} \right).$$

17 Déf : Soit $P = \sum_{k=0}^p a_k X^k$ et Q deux éléments de $K[X]$. Alors, $P \circ Q = P(Q) = \sum_{k=0}^p a_k Q^k$ est un élément de $K[X]$ appelé composée de Q par P . En particulier, $X^p \circ X^k = (X^k)^p = X^{kp}$.

18 Attention : ne pas confondre $P(Q)$ et PQ .

19 Exemple : $P = X^9 + 4X^3 - 5 = T(X^3) = T \circ Q$ avec $T = X^3 + 4X - 5$ et $Q = X^3$.

20 Polynômes pairs ou impairs

Si $P(X) = P(-X)$ (on dit que P est pair) alors $P = \sum_{k=0}^p a_{2k} X^{2k} = T(X^2) = T \circ X^2$ tq $T = \sum_{k=0}^p a_{2k} X^k$.

Si $P(X) = -P(-X)$ (P est impair) alors $P = \sum_{k=0}^p a_{2k+1} X^{2k+1} = X \times T(X^2) = X \times (T \circ X^2)$ tq $T = \sum_{k=0}^p a_{2k+1} X^k$.

Démo : Considérons un polynôme P tel que $P(X) = P(-X)$. Alors P s'écrit sous la forme $P = \sum_{k=0}^n a_k X^k$.

Par conséquent, $P(-X) = \sum_{k=0}^n a_k (-X)^k = \sum_{k=0}^n a_k (-1)^k X^k$. Comme $P(X) = P(-X)$, on a $P(X) = \sum_{k=0}^n a_k X^k = \sum_{k=0}^n a_k (-1)^k X^k$.

Alors par unicité des coefficients de P , $\forall k \in \llbracket 0, n \rrbracket$, $a_k (-1)^k = a_k$. Par conséquent, $\forall k \in \llbracket 0, n \rrbracket$ tq k impair, $-a_k = a_k$ donc $a_k = 0$.

Ainsi, $P(X) = \sum_{\substack{0 \leq k \leq n \\ k \text{ pair}}} a_k X^k \stackrel{\text{}}{=} \sum_{j=0}^p a_{2j} X^{2j} = \sum_{j=0}^p a_{2j} (X^2)^j = T(X^2)$ avec $T = \sum_{j=0}^p a_{2j} X^j$. OK !

4. Degré

21 Déf : Soit $P = \sum_{k=0}^p a_k X^k$.

• Si $P = 0$ (i.e. tous les a_k sont nuls) alors par **convention**, le degré de P est $-\infty$. on note $\deg(0) = -\infty$.

• Si $P \neq 0$ (i.e. au moins l'un des a_k est non nul) alors par **définition**, le **degré de P** est le plus grand entier k tel que $a_k \neq 0$.

Autrement dit, $\deg(P)$ est l'entier qui vérifie : $a_{\deg(P)} \neq 0$ et $\forall k > \deg(P)$, $a_k = 0$.

Alors, $P = \sum_{k=0}^{\deg(P)} a_k X^k = \sum_{k=0}^n a_k X^k$ avec $n \geq \deg(P)$.

$a_{\deg(P)}$ est appelé le **coefficient dominant** de P .

$a_{\deg(P)} X^{\deg(P)}$ est appelé le **terme dominant** de P .

• Le polynôme nul n'a pas de coefficient dominant, ni de terme dominant.

22 Rques : 1) Dans la suite du cours, on notera $\text{codom}(P)$ le coefficient dominant de P . Cette notation n'est pas officielle mais pratique ! Si vous souhaitez l'utiliser en devoir, vous devez donc la définir.

2) Quitte à ajouter des termes nuls, tout polynôme P s'écrit sous la forme $P = \sum_{k=0}^n a_k X^k$ où $n \in \mathbb{N}$ et $n \geq \deg(P)$.

23 Exemple : Soit $P_n = \frac{1}{2i} [(X-i)^n - (X+i)^n]$ où $n \in \mathbb{N}^*$. Déterminons son degré et son coefficient dominant et vérifions que P_n est à coefficients réels.

$$P_n \stackrel{FBN}{=} \frac{1}{2i} \left[\sum_{k=0}^n \binom{n}{k} (-i)^k X^{n-k} - \sum_{k=0}^n \binom{n}{k} (i)^k X^{n-k} \right] = \frac{1}{2i} \left[\sum_{k=0}^n \binom{n}{k} ((-i)^k - i^k) X^{n-k} \right] = \frac{1}{2i} \left[\sum_{k=0}^n \binom{n}{k} ((-1)^k - 1) i^k X^{n-k} \right]$$

$$P_n = \frac{1}{2i} \left[\sum_{\substack{k=0 \\ k \text{ impair}}}^n \binom{n}{k} (-2) i^k X^{n-k} \right] = \frac{-1}{i} \left[\sum_{1 \leq 2p+1 \leq n} \binom{n}{2p+1} i^{2p+1} X^{n-2p-1} \right] = \frac{-1}{i} \left[\sum_{1 \leq 2p+1 \leq n} \binom{n}{2p+1} (-1)^p i X^{n-2p-1} \right]$$

$$P_n = \left[\sum_{1 \leq 2p+1 \leq n} \binom{n}{2p+1} (-1)^{p+1} X^{n-(2p+1)} \right] = \left[\sum_{p=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2p+1} (-1)^{p+1} X^{n-(2p+1)} \right].$$

J'en déduis que P_n est à coefficients réels (et même entiers) et $\deg P_n = n - 1$ et $\text{codom}(P_n) = -n$.

24 Théo : Soit P et Q deux éléments de $K[X]$ et β un scalaire.

1) $\deg(\beta P) = \begin{cases} \deg(P) & \text{si } \beta \neq 0 \\ -\infty & \text{si } \beta = 0 \end{cases}$ et si P et β non nuls alors $\text{codom}(\beta P) = \beta \text{codom}(P)$.

2) $\deg(PQ) = \deg(P) + \deg(Q)$ et si P et Q non nuls alors $\text{codom}(PQ) = \text{codom}(P)\text{codom}(Q)$.

3) $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.

De plus,

Si $\deg(P) < \deg(Q)$ alors $\deg(P+Q) = \deg(Q)$ et $\text{codom}(P+Q) = \text{codom}(Q)$.

Si $\deg(P) = \deg(Q)$ et $\text{codom}(P) + \text{codom}(Q) \neq 0$ alors $\deg(P+Q) = \deg(Q) = \deg(P)$

et $\text{codom}(P+Q) = \text{codom}(P) + \text{codom}(Q)$.

Si $\deg(P) = \deg(Q)$ et $\text{codom}(P) + \text{codom}(Q) = 0$ alors $\deg(P+Q) < \deg(P) = \deg(Q)$.

Démo : Les résultats sont évidents si P ou Q est nul.

Soit P et Q deux polynômes non nuls. Alors on peut écrire $P = \sum_{k=0}^p a_k X^k$ et $Q = \sum_{k=0}^q b_k X^k$ avec $p = \deg(P)$,

$q = \deg(Q)$ et $a_p \neq 0$ et $b_q \neq 0$. Par définition de $\beta P, PQ$ et $P+Q$, on sait déjà que $\deg(\beta P) \leq \deg(P)$, $\deg(PQ) \leq \deg(P) + \deg(Q)$ et $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.

1) Soit $\beta \in \mathbb{R}^*$. Alors $\beta P = \sum_{k=0}^p \beta a_k X^k$ et $\beta a_p \neq 0$. Donc, $\deg(\beta P) = p = \deg(P)$ et $\text{codom}(\beta P) = \beta a_p = \beta \text{codom}(P)$.

2) $PQ = \sum_{k=0}^{p+q} c_k X^k$ vérifie : $c_{p+q} = \sum_{l=0}^{p+q} \underbrace{a_l}_{\substack{\text{nul} \\ \text{si } l > p}} \underbrace{b_{p+q-l}}_{\substack{\text{nul} \\ \text{si } l < p}} = a_p b_q \neq 0$. Donc, $\deg(PQ) = p+q = \deg(P) + \deg(Q)$ et

$\text{codom}(PQ) = a_p b_q = \text{codom}(P)\text{codom}(Q)$.

3) $P+Q = \sum_{k=0}^{\max(p,q)} (a_k + b_k) X^k$. On voit immédiatement que : $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$. Précisons :

Si $a_{\max(p,q)} + b_{\max(p,q)} \neq 0$ alors $\deg(P+Q) = \max(p, q)$. Si $a_{\max(p,q)} + b_{\max(p,q)} = 0$ alors $\deg(P+Q) < \max(p, q)$.

- Si $\deg(P) = p < q = \deg(Q)$ alors $\max(p, q) = q$ et $a_{\max(p, q)} + b_{\max(p, q)} = a_q + b_q = b_q \neq 0$. Donc $\deg(P + Q) = \deg(Q)$ et $\text{codom}(P + Q) = \text{codom}(Q)$.
- Mais si $\deg(P) = p = q = \deg(Q)$ alors $\max(p, q) = p = q$ et $a_{\max(p, q)} + b_{\max(p, q)} = a_p + b_p$.
 - Si $a_p + b_p = 0$ alors $\deg(P + Q) < \deg(P) = \deg(Q)$.
 - Mais, si $a_p + b_p \neq 0$ alors $\deg(P + Q) = \deg(P) = \deg(Q)$ et $\text{codom}(P + Q) = \text{codom}(P) + \text{codom}(Q)$.

25 Généralisation : Soit P_1, P_2, \dots, P_m des éléments de $K[X]$ et β_1, \dots, β_m des éléments de K .

- $\deg(\prod_{k=1}^m P_k) = \sum_{k=1}^m \deg(P_k)$ et si P_1, P_2, \dots, P_m sont tous non nuls, alors $\text{codom}(\prod_{k=1}^m P_k) = \prod_{k=1}^m \text{codom}(P_k)$.
- En particulier, $\forall P \in K[X], \forall m \in \mathbb{N}, \deg(P^m) = m \deg(P)$ et si $P \neq 0$ alors $\text{codom}(P^m) = (\text{codom}(P))^m$.
- $\deg(\sum_{k=1}^m \beta_k P_k) \leq \max(\deg(P_1), \dots, \deg(P_m))$ et si pour tout $k \in \{1, \dots, m-1\}, \deg P_m > \deg P_k$ et $\beta_m \neq 0$ alors $\deg(\sum_{k=1}^m \beta_k P_k) = \deg P_m$ et $\text{codom}(\sum_{k=1}^m \beta_k P_k) = \beta_m \text{codom}(P_m)$.

26 Exemples importants:

- 1) Les polynômes constants sont les polynômes de degré 0 ou $-\infty$. Un polynôme constant non nul est de degré 0.
- 2) Si $\mu \in K$ et $n \in \mathbb{N}$ alors $\deg((X - \mu)^n) = n$ et si $\beta \in K^*$ alors $\deg(\beta(X - \mu_1)^{n_1}(X - \mu_2)^{n_2} \dots (X - \mu_r)^{n_r}) = \sum_{k=1}^r n_k$.
De plus, $\text{codom}((X - \mu)^n) = 1$ et si $\beta \in K^*$ alors $\deg(\beta(X - \mu_1)^{n_1}(X - \mu_2)^{n_2} \dots (X - \mu_r)^{n_r}) = \beta$.

26 Théo Soit P et Q deux polynômes. Alors,

$$\deg(P \circ Q) = \begin{cases} -\infty & \text{si } P = 0 \text{ ou } (Q = 0 \text{ et le terme constant de } P \text{ est nul}) \\ 0 & \text{si } Q = 0 \text{ et le terme constant de } P \text{ n'est pas nul} \\ \deg(P) \times \deg(Q) & \text{si } P \text{ et } Q \text{ sont non nuls} \end{cases}$$

Et si P et Q sont non nuls alors $\text{codom}(P \circ Q) = \text{codom}(P)(\text{codom}(Q))^{\deg(P)}$

Démo : • Si $P = 0$ alors $P \circ Q = 0$ donc $\deg(P \circ Q) = -\infty$

• Si $Q = 0$ alors $P \circ Q = \text{terme constant de } P$; donc $\deg(P \circ Q) = -\infty$ si le terme constant de P est nul et $\deg(P \circ Q) = 0$ si le terme constant de P n'est pas nul.

• Désormais P et Q non nul. Alors $P = \sum_{k=0}^p a_k X^k$ avec $p = \deg(P)$ et Q deux éléments de $K[X]$. Alors, $P \circ Q = P(Q) = \sum_{k=0}^p a_k Q^k$. Or, $\forall k \in [0, p-1], \deg(a_k Q^k) \stackrel{\text{car } a_k \neq 0}{=} \deg(Q^k) = p \deg(Q) > k \deg(Q) = \deg(Q^k) \geq \deg(a_k Q^k)$. Donc dans la

somme $\sum_{k=0}^p a_k Q^k$, le terme $a_p Q^p$ a un degré strictement supérieur aux degrés des autres termes. Par conséquent, $\deg(P \circ Q) = \deg(a_p Q^p) = p \deg(Q) = \deg(P) \deg(Q)$.

$\text{codom}(P \circ Q) = \text{codom}(a_p Q^p) = a_p [\text{codom}(Q)]^p = \text{codom}(P) \text{codom}(Q)^{\deg(P)}$.

27 Exemple : Soit $P \in K[X]$ et $Q(X) = P(X + 1) - P(X)$. Déterminons $\deg(Q)$ en fonction de $\deg(P)$ et le cas échéant $\text{codom}(Q)$.

• Si $P = 0$ alors $Q = 0$ et $\deg Q = \deg P = -\infty$.

• Si $P \neq 0$ alors $\deg P(X + 1) \stackrel{\text{théo 26}}{=} \deg P \times \deg(X + 1) = \deg P$. Donc, $\deg Q \leq \max(\deg P, \deg(P(X + 1))) = \deg(P)$. De plus,

$\text{codom} P(X + 1) = \text{codom} P \times [\text{codom}(X + 1)]^{\deg(P)} = \text{codom} P$. Donc, $\deg Q \leq \deg P - 1$.

Par conséquent, si $\deg P \leq 0$ ie. P est un polynôme constant alors $Q = 0$.

Etudions le cas où $n = \deg P \geq 1$. On a : $P = \sum_{k=0}^n a_k X^k$ avec $n = \deg P \geq 1$. Alors

$$P(X + 1) = \sum_{k=0}^n a_k (X + 1)^k = a_n (X + 1)^n + a_{n-1} (X + 1)^{n-1} + \underbrace{R(X)}_{\substack{\text{de degré} \\ \leq n-2}} \stackrel{FBN}{=} a_n X^n + n a_n X^{n-1} + a_{n-1} X^{n-1} + \underbrace{T(X)}_{\substack{\text{de degré} \\ \leq n-2}}$$

Donc, $P(X + 1) - P(X) = n a_n X^{n-1} + \underbrace{L(X)}_{\text{de degré } \leq n-2}$. Donc $\deg Q = n - 1$ et $\text{codom} Q = n a_n = n \text{codom}(P)$ dès que $n = \deg P \geq 1$.

28 Déf Un polynôme P de $K[X]$ est dit scindé (sur K) lorsqu'il peut s'écrire comme un produit de polynômes de $K[X]$ de degré 1.

29 Trois écritures sous forme scindée d'un même polynôme : $P = (a_1 X + b_1)(a_2 X + b_2) \dots (a_s X + b_s)$

$$\xleftrightarrow[\substack{\text{en mettant} \\ a_k (\neq 0) \text{ en facteur} \\ \text{dans chaque} \\ \text{parenthèse}}]{\text{en regroupant}} P = \beta (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_s) \xleftrightarrow[\substack{\text{les facteurs} \\ \text{contenant} \\ \text{le même } \alpha}]{\text{en regroupant}} P = \beta (X - \mu_1)^{n_1} (X - \mu_2)^{n_2} \dots (X - \mu_r)^{n_r}$$

5. l'ensemble $K_n[X]$.

30 Def Soit n un entier naturel. On note $K_n[X]$ l'ensemble des polynômes (à une indéterminée) à coefficient dans K et de degré inférieur ou égal à n .

31 Exemples : $K_0[X]$ est l'ensemble des polynômes constants et $K_1[X] = \{aX + b / (a, b) \in K^2\}$ est l'ensemble des polynômes de degré inférieur ou égal à 1.

32 NB : $\forall n, K_n[X] \subset K_{n+1}[X]$.

33 Theo Tout polynôme de $K_n[X]$ s'écrit de manière unique comme combinaison linéaire de $1, X, X^2, \dots, X^n$.

On dira que la famille $(1, X, X^2, \dots, X^n)$ est une base de $K_n[X]$.

34 notation : On note souvent E_n l'ensemble des fonctions polynomiales de \mathbb{R} dans \mathbb{R} de degré inférieur ou égal à n . On a les mêmes définitions et les mêmes résultats sur les fonctions polynomiales associées.

II Polynômes dérivés

1. Définition, écriture et degré

35 Déf: Soit $P = \sum_{k=0}^p a_k X^k$. Le polynôme dérivé de P est : $P^{(1)} = P' = \sum_{k=1}^p k a_k X^{k-1} = \sum_{k=0}^{p-1} (k+1) a_{k+1} X^k$.

On définit alors les polynômes dérivés successifs :

par convention, $P^{(0)} = P$ est le polynôme dérivé 0^{ème} de P

Et $\forall j \in \mathbb{N}^*$, $P^{(j)} = (P^{(j-1)})'$ est le polynôme dérivé $j^{\text{ème}}$ de P .

36 Conséquence: on retrouve les formules de dérivation des fonctions polynomiales. Autrement dit, pour tout entier naturel j , $\tilde{P}^{(j)} = \widetilde{P^{(j)}}$. On a aussi les mêmes règles de calcul :

37 Règles de calcul Soit j un entier naturel, α, β, γ des scalaires et P et Q des polynômes.

$$(\beta P + \gamma Q)^{(j)} = \beta P^{(j)} + \gamma Q^{(j)}$$

$$(PQ)^{(j)} = \sum_{l=0}^j \binom{j}{l} P^{(l)} Q^{(j-l)} \quad (\text{Leibniz})$$

$$(P \circ Q)' = Q' \times (P' \circ Q)$$

$$(P \circ (X + \alpha))^{(j)} = P^{(j)}(X + \alpha)$$

$$\left(\prod_{j=1}^m P_j \right)' = \sum_{i=1}^m P_i' \left(\prod_{\substack{j=1 \\ j \neq i}}^m P_j \right)$$

38 Prop : Pour tous entiers naturels k et j , $(X^k)^{(j)} = \begin{cases} 0 & \text{si } j > k \\ \frac{k!}{(k-j)!} X^{k-j} & \text{si } j \leq k \end{cases}$

39 Prop : Pour tout entier naturel j et tout polynôme $P = \sum_{k=0}^p a_k X^k$,

$$P^{(j)} = \begin{cases} 0 & \text{si } j > p \\ \sum_{k=j}^p a_k \frac{k!}{(k-j)!} X^{k-j} & \text{si } j \leq p \end{cases}$$

40 Prop : Pour tout entier naturel j et tout polynôme P , $\deg(P^{(j)}) = \begin{cases} -\infty & \text{si } j > \deg(P) \\ \deg(P) - j & \text{si } j \leq \deg(P) \end{cases}$

et si P est non nul alors et $j \leq \deg(P)$ alors $\text{codom}(P^{(j)}) = \frac{\deg(P)!}{(\deg(P)-j)!} \text{codom}(P)$.

(Si P est nul alors tous ses polynômes dérivés sont nuls)

Démo : Soit $P = \sum_{k=0}^{\deg(P)} a_k X^k$ un polynôme non nul et $j \in \mathbb{N}$.

D'après ce qui précède, $P^{(j)} = \begin{cases} 0 & \text{si } j > \deg(P) \\ \sum_{k=j}^{\deg(P)} a_k \frac{k!}{(k-j)!} X^{k-j} & \text{si } j \leq \deg(P) \end{cases}$. Donc, si $j > \deg(P)$ alors $\deg(P^{(j)}) = -\infty$. Par contre, si $j \leq$

$\deg(P)$, alors comme $a_{\deg(P)} \frac{\deg(P)!}{(\deg(P)-j)!} \neq 0$, on peut affirmer que $\deg(P^{(j)}) = \deg(P) - j$ et $\text{codom}(P^{(j)}) = \frac{\deg(P)!}{(\deg(P)-j)!} \text{codom}(P)$.

41 Théo : Soit $P = \sum_{k=0}^p a_k X^k$ un polynôme.

Alors, $\forall j \in \mathbb{N}$, $a_j = \frac{\tilde{P}^{(j)}(0)}{j!}$ et $P = \sum_{k=0}^p \frac{\tilde{P}^{(k)}(0)}{k!} X^k$

Démo : Le résultat est évident avec un polynôme P nul puisque tous les scalaires a_j sont nuls et les fonctions polynomiales $\tilde{P}^{(j)}$ aussi. Soit $P = \sum_{k=0}^{\deg(P)} a_k X^k$ un polynôme non nul et $j \in \mathbb{N}$.

D'après la prop 39, $P^{(j)} = \begin{cases} 0 & \text{si } j > \deg(P) \\ \sum_{k=j}^{\deg(P)} a_k \frac{k!}{(k-j)!} X^{k-j} & \text{si } j \leq \deg(P) \end{cases}$. Donc, $\forall t \in K$, $\tilde{P}^{(j)}(t) = \begin{cases} 0 & \text{si } j > \deg(P) \\ \sum_{k=j}^{\deg(P)} a_k \frac{k!}{(k-j)!} t^{k-j} & \text{si } j \leq \deg(P) \end{cases}$.

En particulier, $\tilde{P}^{(j)}(0) = \begin{cases} 0 = 0 \times j! = a_j \times j! & \text{si } j > \deg(P) \\ \sum_{k=j}^{\deg(P)} a_k \frac{k!}{(k-j)!} 0^{k-j} = a_j \frac{j!}{(0)!} 0^0 = a_j j! & \text{si } j \leq k \end{cases} = a_j j!$. Ainsi, $a_j = \frac{\tilde{P}^{(j)}(0)}{j!}$ valable pour tout $j \in \mathbb{N}$.

Il s'en suit que $P = \sum_{j=0}^{\deg(P)} \frac{\tilde{P}^{(j)}(0)}{j!} X^j$.

42 Exemple : Soit $P \in \mathbb{R}[X]$ non nul de degré n et $Q = (X^2 + 1)P'' - 6P$. Déterminons le degré de Q et le cas échéant son coefficient dominant.

On sait que : $\deg((X^2 + 1)P'') = 2 + \deg P'' = \deg P = \deg(-6P)$. Donc $\deg Q \leq \max(\deg((X^2 + 1)P''), \deg(-6P)) = \deg P$.

De plus, $\text{codom}((X^2 + 1)P'') = \text{codom}(P'') = n(n-1)\text{codom}(P)$ et $\text{codom}(-6P) = -6\text{codom}(P)$. On a deux cas :

Si $n(n-1) - 6 = (n-3)(n+2) \neq 0$ ie $n \neq 3$ alors $\deg Q = \deg P = n$ et $\text{codom}(Q) = (n(n-1) - 6)\text{codom}(P)$

Si $n(n-1) - 6 = 0$ ie $n = 3$ alors $\deg Q < \deg P$. Posons $P = a + bX + cX^2 + dX^3$ avec $d \neq 0$.

Alors $P'' = 2c + 6dX$ et $Q = (X^2 + 1)(2c + 6dX) - 6(a + bX + cX^2 + dX^3) = (2c - 6a) + (6d - 6b)X - 4cX^2$. Donc, $\deg Q =$

$$\begin{cases} 2 \text{ si } c \neq 0 \\ 1 \text{ si } c = 0 \text{ et } d \neq b \\ 0 \text{ si } c = 0, d = b \text{ et } a \neq 0 \\ -\infty \text{ si } c = 0 = a, d = b \end{cases} \text{ et } \text{codom}(Q) = \begin{cases} -4c \text{ si } c \neq 0 \\ 6d - 6b \text{ si } c = 0 \text{ et } d \neq b \\ 2c - 6a \text{ si } c = 0, d = b \text{ et } a \neq 0 \\ n' \text{ existe pas si } c = 0 = a \text{ et } d = b \end{cases}$$

2. Formule de Taylor pour les polynômes

43 Théorème : Soit P un élément de $K_n[X]$ et α un élément de K . Alors, $P = \sum_{k=0}^n \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$ et cette écriture est l'unique manière d'écrire P comme combinaison linéaire des polynômes $1, X - \alpha, (X - \alpha)^2, \dots, (X - \alpha)^n$.

On dira que la famille $(1, X - \alpha, (X - \alpha)^2, \dots, (X - \alpha)^n)$ est une base de $K_n[X]$.

Démonstration : Soit P un élément de $K_n[X]$ non nul et α un élément de K .

Existence : Posons $Q = P \circ (X + \alpha) = P(X + \alpha)$. Alors d'après le théorème 41, $Q = \sum_{k=0}^{\deg(Q)} \frac{\tilde{Q}^{(k)}(0)}{k!} X^k$.

De plus, $\deg Q = \deg P \times \deg(X + \alpha) = \deg(P) \leq n$. Donc $Q = \sum_{j=0}^n \frac{\tilde{Q}^{(j)}(0)}{j!} X^j$ car $\forall j > \deg(Q), \tilde{Q}^{(j)} = 0$.

Enfin, on montre par récurrence sur j que : $\forall j \in \mathbb{N}, Q^{(j)} = P^{(j)} \circ (X + \alpha)$. Donc, $\forall j \in \mathbb{N}, \forall t \in K, \tilde{Q}^{(j)}(t) = \tilde{P}^{(j)}(t + \alpha)$. Il s'en suit

que : $\tilde{Q}^{(j)}(0) = \tilde{P}^{(j)}(\alpha)$. Et ainsi, $Q = \sum_{j=0}^n \frac{\tilde{P}^{(j)}(\alpha)}{j!} X^j$. Alors $P = Q \circ (X - \alpha) = Q(X - \alpha) = \sum_{j=0}^n \frac{\tilde{P}^{(j)}(\alpha)}{j!} (X - \alpha)^j$. Le polynôme P

est donc bien une combinaison linéaire des polynômes $1, (X - \alpha), (X - \alpha)^2, \dots, (X - \alpha)^n$.

Unicité : Si $P = \sum_{j=0}^n b_j (X - \alpha)^j = \sum_{j=0}^n c_j (X - \alpha)^j$ alors $Q = P(X + \alpha) = \sum_{j=0}^n b_j X^j = \sum_{j=0}^n c_j X^j$ et par unicité des coefficients d'un polynôme, $\forall j, b_j = c_j$. D'où l'unicité de l'écriture.

44 Corollaire

- Si deux polynômes ont toutes leurs dérivées successives qui prennent les mêmes valeurs en un scalaire α alors ces polynômes sont égaux.
- Le polynôme nul est le seul polynôme dont toutes les dérivées successives s'annulent en α . Si $\deg(P) \leq n$ et il existe un réel α tq : $P(\alpha) = P^{(1)}(\alpha) = \dots = P^{(n)}(\alpha) = 0$ alors P est le polynôme nul.

45 Exemple : Soit $n \in \mathbb{N}$. Les polynômes P de $K_n[X]$ vérifiant : $P'(2) = 2P^{(4)}(2)$ sont tous les polynômes de la forme $a_0 + a_1(X - 2) + a_2(X - 2)^2 + a_3(X - 2)^3 + \frac{a_4}{2 \times 4!}(X - 2)^4 + a_5(X - 2)^5 + \dots + a_n(X - 2)^n$ où $a_0, a_1, a_2, a_3, a_4, \dots, a_n$ des scalaires.

III Divisibilité

1. Définition

46 Définition : Soit A et B deux polynômes de $K[X]$.

On dit que B divise A (dans $K[X]$) lorsqu'il existe un polynôme Q (de $K[X]$) tel que : $A = BQ$.

47 Remarques : • Tout polynôme divise 0, 0 ne divise que 0.

- Les polynômes constants non nuls divisent tout polynôme. Tout polynôme P est divisible par tout polynôme βP tels que $\beta \in K^*$. Ces polynômes βP tels que $\beta \neq 0$ sont appelés les polynômes associés de P .
- Si B divise A non nul alors $\deg(B) \leq \deg(A)$.

48 Exemples

- 1) La formule de factorisation assure que $\forall m \in \mathbb{N}^*, \forall (A, B) \in K[X]^2, A - B$ divise $A^m - B^m$.
- 2) $X^2 + X + 1$ et $X - 1$ divisent $X^3 - 1$ dans $\mathbb{R}[X]$ (d'après la formule de factorisation 16) et $X - j, X - j^2, X - 1$ divisent $X^3 - 1$ dans $\mathbb{C}[X]$. $X - i$ et $X + i$ divisent $X^2 + 1$ dans $\mathbb{C}[X]$.

49 Définition : Un polynôme P , non constant, est irréductible lorsque ses seuls diviseurs dans $K[X]$ sont les polynômes constants et ses associés.

50 Théorème : Tout polynôme de $K[X]$ de degré 1 est irréductible dans $K[X]$.

Démonstration : Soit A un polynôme de $K[X]$ de degré 1 et B l'un de ses diviseurs dans $K[X]$. Alors il existe $Q \in K[X]$ tq : $A = BQ$.

Donc, $1 = \deg(A) = \deg(B) + \deg(Q)$. Par conséquent,

ou bien $\deg(B) = 1$ et $\deg(Q) = 0$ et dans ce cas, $Q = \beta \in K^*$ et $B = \frac{1}{\beta}A$ est associé à A .

ou bien $\deg(B) = 0$ et $\deg(Q) = 1$ et dans ce cas, $B = \beta \in K^*$ polynôme constant.
 J'en conclus que les diviseurs de A sont constants ou associés à A ce qui signifie que A est irréductible.

51 Déf-prop : Un polynôme P est unitaire lorsque P non nul et $\text{codom}(P) = 1$.

Tout polynôme non nul a un polynôme associé unitaire.

Démo : Soit Q un polynôme non nul. Alors $Q = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0$ avec $n = \deg(Q)$ et donc $a_n \neq 0$.

Par conséquent, $Q = a_n \left(X^n + \frac{a_{n-1}}{a_n} X^{n-1} + \dots + \frac{a_0}{a_n} \right) = a_n P$ avec P unitaire. Alors P est un associé unitaire de Q .

2. Théorème de la division euclidienne

52 Théorème de la division euclidienne : Soit A et B deux éléments $K[X]$ tels que $B \neq 0$.

Alors il existe un unique polynôme Q et un unique polynôme R tels que : $A = BQ + R$ et $\deg R < \deg B$.

Démo de l'unicité : Supposons qu'il existe R_1, R_2, Q_1, Q_2 polynômes tels que :

$$A = BQ_1 + R_1 = BQ_2 + R_2 \text{ et } \deg(R_1) < \deg(B) \text{ et } \deg(R_2) < \deg(B).$$

Alors $B(Q_1 - Q_2) = R_2 - R_1$ (*). Donc, $\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) \leq \max(\deg(R_1), \deg(R_2)) < \deg(B)$.

Par conséquent, $\deg(Q_1 - Q_2) < 0$. Cela implique que $\deg(Q_1 - Q_2) = -\infty$ i.e. $Q_1 - Q_2 = 0$. Ainsi $Q_1 = Q_2$.

Alors (*) donne $R_1 - R_2 = 0$. Ainsi $R_1 = R_2$. D'où l'unicité de Q et R s'ils existent...

Démo de l'existence : Notons $p = \deg(B)$ et $B = \sum_{k=0}^p b_k X^k$ avec $b_p \neq 0$. Faisons une preuve par récurrence...

Posons H_n la propriété : « si A est un polynôme tel que $\deg(A) \leq n$ alors il existe deux polynômes Q et R tels que $\deg(R) < \deg(B)$ et $A = BQ + R$ »

Initialisation. soit $n < p$. Alors, $A = B \times \underset{=Q}{0} + \underset{=R}{A}$ et Q et R ainsi définis vérifient les propriétés souhaitées. J'en déduis que

H_0, H_1, \dots, H_{p-1} sont vraies.

Propagation : soit $n \in \mathbb{N}$. Je suppose que H_n est vraie et je vais montrer sous cette hypothèse que H_{n+1} est vraie. Je suppose donc que $\deg(A) \leq n + 1$.

Ou bien $\deg(A) \leq n$ alors H_n s'applique à A et je peux affirmer qu'il existe deux polynômes Q et R tels que $\deg(R) < \deg(B)$ et $A = BQ + R$

Ou bien $\deg(A) = n + 1$. Posons $A = \sum_{k=0}^{n+1} a_k X^k$ avec $a_{n+1} \neq 0$. On a : $a_{n+1} X^{n+1} = b_p X^p \times \frac{a_{n+1}}{b_p} X^{n+1-p}$.

On pose alors $Q_n = \frac{a_{n+1}}{b_p} X^{n+1-p}$ et $A_1 = A - Q_n B$.

Or, $\deg(Q_n B) = \deg(Q_n) + \deg(B) = n + 1 - p + p = \deg(A)$ et $\text{codom}(Q_n B) = \text{codom}(Q_n) \text{codom}(B) = \frac{a_{n+1}}{b_p} b_p = a_{n+1} =$

$\text{codom}(A)$. Donc, $\deg(A_1) < \deg(A) = \deg(Q_n B)$. Par conséquent $\deg(A_1) \leq n$. Alors je peux appliquer H_n au polynôme A_1 . Il existe donc deux polynômes Q_1 et R_1 tels que $\deg(R_1) < \deg(B)$ et $A_1 = BQ_1 + R_1$. Par conséquent, $BQ_1 + R_1 = A - Q_n B$.

Il s'en suit que $A = B(Q_1 + Q_n) + R_1$ avec $\deg(R_1) < \deg(B)$. Donc $Q = Q_1 + Q_n$ et $R = R_1$ conviennent.

J'en conclus que $H_n \Rightarrow H_{n+1}$.

CCL : le théorème de récurrence simple permet de conclure que : $\forall n \in \mathbb{N}, H_n$ vraie. Et par conséquent pour tout polynôme A , il existe deux polynômes Q et R tels que $\deg(R) < \deg(B)$ et $A = BQ + R$. Et ces deux polynômes ont uniques d'après ce qui précède.

53 En pratique. Cf vidéo... pour vous exercer :

$$\begin{array}{r|l} 2X^5 - 3X^4 + X^2 - 4X + 1 & 3X^2 - 2X - 2 \\ - (X^5 - \frac{4}{3}X^4 - \frac{4}{3}X^3) & \frac{2}{3}X^3 - \frac{5}{9}X^2 + \frac{2}{27}X + \frac{1}{81} \\ \hline -\frac{5}{3}X^4 + \frac{4}{3}X^3 + X^2 - 4X + 1 & \\ - (-\frac{5}{3}X^4 + \frac{10}{9}X^3 + \frac{10}{9}X^2) & \\ \hline \frac{2}{9}X^3 - \frac{1}{9}X^2 - 4X + 1 & \\ - (\frac{2}{9}X^3 - \frac{4}{27}X^2 - \frac{4}{27}X) & \\ \hline \frac{1}{27}X^2 - \frac{104}{27}X + 1 & \\ - (\frac{1}{27}X^2 - \frac{2}{81}X - \frac{2}{81}) & \\ \hline -\frac{310}{81}X + \frac{83}{81} & \end{array}$$

Alors, on a : $2X^5 - 3X^4 + X^2 - 4X + 1 = (3X^2 - 2X - 2) \left(\frac{2}{3}X^3 - \frac{5}{9}X^2 + \frac{2}{27}X + \frac{1}{81} \right) + \left(-\frac{310}{81}X + \frac{83}{81} \right)$

54 Premier critère de divisibilité : B divise A si et ssi le reste de la division euclidienne de A par B est nul.

