Licence – Mathématiques
Algèbre 2

COURS À DISTANCE – SEMAINE 3 – POLYNÔMES : GÉNÉRALITÉS ET DIVISION EUCLIDIENNE

La notion de polynôme est une notion fondamentale en mathématiques, apparaissant dans de nombreux contextes, mais sous des formes parfois trompeuses. Les polynômes sont en effet souvent confondus avec les fonctions polynomiales. Il s’ensuit, en général, une grande confusion sur la nature du X apparaissant couramment dans ce contexte. Cette confusion peut s’expliquer d’une part par les natures très diverses que peut en effet recouvrir ce X , mais aussi par le fait qu’il ne joue, en réalité, aucun rôle puisque qu’un polynôme est entièrement déterminé par ses coefficients. Nous allons donner ici une définition formelle des polynômes se basant uniquement sur ces derniers.

On fixe maintenant $\mathbb{K}$ un corps commutatif, par exemple $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Remarque. On peut définir une notion de polynôme sur n’importe quel anneau. Dans tout ce qui suit, certaines propriétés restent vraies lorsqu’on enlève la propriété de commutativité ou d’intégrité et d’autres deviennent fausses. C’est un très bon exercice de chercher où chaque hypothèse est effectivement utilisée.

1 Définition

Notation 1.1. Si x dénote une suite indexée par $\mathbb{N}$, pour tout $k \in \mathbb{N}$, on notera par x_k son $k^{\text{ième}}$ terme.

Définition 1.2. On dit qu’une suite a est à support fini si elle est nulle à partir d’un certain rang, c’est-à-dire s’il existe $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k > n$. On note $\ell(\mathbb{K})$ l’ensemble des suites à valeurs dans $\mathbb{K}$, et $\ell_c(\mathbb{K}) \subset \ell(\mathbb{K})$ le sous-ensemble des suites à support fini. On définit également les deux opérations :

$$\begin{array}{ccc}
 \ell(\mathbb{K}) \times \ell(\mathbb{K}) & \longrightarrow & \ell(\mathbb{K}) \\
 +: (a, b) & \longmapsto & (a_k + b_k)_{k \in \mathbb{N}}
 \end{array}
 \quad \cdot \quad
 \begin{array}{ccc}
 \ell(\mathbb{K}) \times \ell(\mathbb{K}) & \longrightarrow & \ell(\mathbb{K}) \\
 (a, b) & \longmapsto & \left(\sum_{i=0}^k a_i \cdot b_{k-i} \right)_{k \in \mathbb{N}}
 \end{array}$$

Remarque 1.3. La définition du produit $a.b$ peut sembler disymétrique, mais en faisant le changement de variable $j = k - i$, le $k^{\text{ième}}$ terme de la suite $a.b$ peut également s’écrire $\sum_{j=0}^k a_{k-j} \cdot b_j$. Et en remarquant que $i + (k - i) = k$, on peut même symétriser directement la formule en :

$$(a.b)_k = \sum_{\substack{i_1, i_2 \in \mathbb{N} \\ i_1 + i_2 = k}} a_{i_1} \cdot b_{i_2}.$$

Proposition 1.4. Soit $a, b \in \ell_c(\mathbb{K})$, alors $a + b$ et $a.b$ sont dans $\ell_c(\mathbb{K})$.

Démonstration. Puisque a et b sont à supports finis, notons $n_a, n_b \in \mathbb{N}$ tels que $a_k = 0$ pour $k > n_a$ et $b_k = 0$ pour $k > n_b$. Alors, pour tout $k > \max(n_a, n_b)$, $a_k + b_k = 0 + 0 = 0$, et pour tout $k > n_a + n_b$,

$$\sum_{i=0}^k a_i \cdot b_{k-i} = \sum_{i=0}^{n_a} a_i \cdot b_{k-i} + \sum_{i=n_a+1}^k a_i \cdot b_{k-i} = \sum_{i=0}^{n_a} a_i \cdot 0 + \sum_{i=n_a+1}^k 0 \cdot b_{k-i} = 0.$$

En effet, pour $i > n_a$, $a_i = 0$ et pour $i \leq n_a$, on a $k - i > n_a + n_b - i \geq n_a + n_b - n_a = n_b$, et donc $b_{k-i} = 0$. □

Proposition 1.5. Les opérations $+$ et $\cdot$ munissent $\ell_c(\mathbb{K})$ d’une structure d’anneau unitaire commutatif dont le zéro est la suite 0, constante égale à zéro, et l’élément unité est la suite $1 := (1, 0, 0, \dots)$ dont tous les termes valent zéro sauf celui d’indice 0 qui vaut un.

Démonstration. Il est clair que $(\ell_c, +)$ est un groupe abélien dont la suite 0 est l'élément neutre.

Pour montrer l'associativité du produit, on considère $a, b, c \in \ell_c(\mathbb{K})$. Alors, pour tout $k \in \mathbb{N}$, on a

$$\begin{aligned} (a.(b.c))_k &= \sum_{\substack{i_1, i_2 \in \mathbb{N} \\ i_1 + i_2 = k}} a_{i_1} \cdot (b.c)_{i_2} = \sum_{\substack{i_1, i_2, i_2' \in \mathbb{N} \\ i_1 + i_2 + i_2' = k}} a_{i_1} \cdot b_{i_2'} \cdot c_{i_2} \\ &= \sum_{\substack{i_1', i_1'', i_2 \in \mathbb{N} \\ i_1' + i_1'' + i_2 = k}} a_{i_1'} \cdot b_{i_1''} \cdot c_{i_2} = \sum_{\substack{i_1, i_2 \in \mathbb{N} \\ i_1 + i_2 = k}} (a.b)_{i_1} \cdot c_{i_2} \\ &= ((a.b).c)_k. \end{aligned}$$

Avant d'attaquer la distributivité, montrons la commutativité. Pour tous $a, b \in \ell_c(\mathbb{K})$ et tout $k \in \mathbb{N}$, on a

$$(a.b)_k = \sum_{\substack{i_1, i_2 \in \mathbb{N} \\ i_1 + i_2 = k}} a_{i_1} \cdot b_{i_2} = \sum_{\substack{i_1, i_2 \in \mathbb{N} \\ i_1 + i_2 = k}} b_{i_1} \cdot a_{i_2} = (b.a)_k.$$

Concernant la distributivité, pour tous $a, b, c \in \ell_c(\mathbb{K})$ et tout $k \in \mathbb{N}$, on a

$$\begin{aligned} (a.(b+c))_k &= \sum_{i=0}^k a_i \cdot (b+c)_{k-i} = \sum_{i=0}^k a_i \cdot (b_{k-i} + c_{k-i}) = \sum_{i=0}^k a_i \cdot b_{k-i} + a_i \cdot c_{k-i} \\ &= \sum_{i=0}^k a_i \cdot b_{k-i} + \sum_{i=0}^k a_i \cdot c_{k-i} = (a.b)_k + (a.c)_k, \end{aligned}$$

et donc, en utilisant la commutativité, $(a+b).c = c.(a+b) = c.a + c.b = a.c + b.c$.

Enfin, pour tout $a \in \ell_c(\mathbb{K})$ et tout $k \in \mathbb{N}$, on a

$$(a.1)_k = (1.a)_k = \sum_{i=0}^k 1_i \cdot a_{k-i} = 1_0 \cdot a_k = a_k$$

et donc $a.1 = 1.a = a$. L'élément 1 est donc un élément unité. $\square$

Remarque 1.6. De la même manière, on montre que $(\ell(\mathbb{K}), +, \cdot)$ est un anneau unitaire commutatif, dont $\ell_c(\mathbb{K})$ est un sous-anneau. Par ailleurs, on peut remarquer que $\ell_0(\mathbb{K}) := \{a \in \ell(\mathbb{K}) \mid \forall k \in \mathbb{N}^*, a_k = 0\} \subset \ell(\mathbb{K})$ est un sous-anneau de $\ell_c(\mathbb{K})$ qui s'identifie naturellement avec $\mathbb{K}$. Plus précisément, l'application $\psi : \mathbb{K} \rightarrow \ell_0(\mathbb{K})$ qui envoie $\lambda \in \mathbb{K}$ sur la suite $(\lambda, 0, \dots)$ est un isomorphisme d'anneaux; le résultat est clair au niveau de la somme et, concernant le produit, on vérifie directement que $(\lambda_1, 0, \dots) \cdot (\lambda_2, 0, \dots) = (\lambda_1 \cdot \lambda_2, 0, \dots)$. Cela permet d'utiliser la multiplication dans $\ell(\mathbb{K})$ pour définir sur $\ell(\mathbb{K})$ une notion de multiplication par un scalaire de $\mathbb{K}$, à savoir $\lambda.a := \psi(\lambda).a$, qui plus prosaïquement parlant, multiplie chaque terme de a par λ . Puisque cela ne crée pas d'ambiguïté, nous identifierons par la suite $\mathbb{K}$ et $\ell_0(\mathbb{K})$ et noterons $\lambda.a$ pour $\psi(\lambda).a$.

Notation 1.7. On note X la suite $(0, 1, 0, \dots)$ dont tous les termes sont nuls sauf celui d'indice 1 qui vaut 1.

Proposition 1.8. Pour tout $k \in \mathbb{N}$, X^k est égal à la suite dont tous les termes valent 0 sauf celui d'indice k qui vaut 1. De fait, pour tout $a \in \ell_c(\mathbb{K})$, on a $a = \sum_{i=0}^n a_i \cdot X^i$ avec $n \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k > n$.

Démonstration. Montrons le résultat par récurrence sur $k \in \mathbb{N}$. Pour $k = 0$, on a bien (par convention) $X^0 = 1$. Supposons maintenant le résultat vrai au rang k , alors pour tout $l \in \mathbb{N}$, on a

$$(X^{k+1})_l = (X.X^k)_l = \sum_{i=0}^l X_i \cdot (X^k)_{l-i} = X_1 \cdot (X^k)_{l-1} = \begin{cases} 1 & \text{si } l-1 = k \text{ c\`ad si } l = k+1 \\ 0 & \text{sinon} \end{cases}.$$

La seconde partie de la proposition en découle directement par linéarité. $\square$

Notation 1.9. Il est traditionnel de noter la suite non nulle $a \in \ell_c(\mathbb{K})^*$ par $a_0 + a_1X + \cdots + a_nX^n$, avec $n \in \mathbb{N}$ tel que $a_n \neq 0$ et $a_k = 0$ pour tout $k > n$. Ici, la lettre X ne correspond donc ni à une variable, ni à une inconnue, mais juste à une notation pour un élément particulier, que l'on appelle souvent *indéterminée*. La suite nulle, quant à elle, est notée 0 . En accord avec ces conventions, l'anneau $(\ell_c(\mathbb{K}), +, \cdot)$ est noté $\mathbb{K}[X]$, et ses éléments sont appelés *polynômes (à coefficients dans $\mathbb{K}$)*. Il arrive que, pour certaines raisons, X soit remplacé par une autre notation, par exemple Y, Z ou α , il convient alors de modifier la notation $\mathbb{K}[Y], \mathbb{K}[Z]$ ou $\mathbb{K}[\alpha]$ en conséquence. Toujours inspiré par cette notation, le terme a_k est souvent appelé *coefficient (de degré k)* tandis que a_kX^k est appelé *terme (de degré k)*; a_0 est aussi appelé *terme constant*.

Remarque 1.10. En tant qu'anneau unitaire commutatif intègre, $\mathbb{K}[X]$ vérifie toutes les propriétés de ces derniers. Toutes les règles de calculs restent en particulier valables, notamment le binôme de Newton et les identités remarquables.

2 Division euclidienne

2.1 Degré d'un polynôme

Définition 2.1.1. Pour tout $P \in \mathbb{K}[X] \setminus \{0\}$, on définit $\deg(P)$ comme le plus grand degré des termes non nuls de P . Par convention, on pose $\deg(0) = -\infty$.

Définition 2.1.2.

- Pour tout polynôme non nul $P \in \mathbb{K}[X]$, on appelle respectivement *coefficient* et *terme dominant* le coefficient et le terme de degré $\deg(P)$, et on dit que le polynôme est *unitaire* si son coefficient dominant vaut 1.
- On appelle *polynôme constant* tout polynôme de degré 0 ou $-\infty$.

Proposition 2.1.3. Pour tous $P_1, P_2 \in \mathbb{K}[X]$, on a $\deg(P_1 + P_2) \leq \max(\deg(P_1), \deg(P_2))$ avec inégalité stricte si et seulement si P_1 et P_2 sont de même degré avec des coefficients dominants opposés.

Démonstration. Quitte à les permuter, par commutativité de la somme, on peut supposer $\deg(P_1) \geq \deg(P_2)$. Au sein de la preuve de la proposition 1.4, nous avons déjà montré que $\deg(P_1 + P_2) \leq \max(\deg(P_1), \deg(P_2))$. Si P_2 est nul, alors $\deg(P_1 + P_2) = \deg(P_1) = \max(\deg(P_1), \deg(P_2))$. Sinon, on note $(a_k)_{k \in \mathbb{N}}$ et $(b_k)_{k \in \mathbb{N}}$ les coefficients de, respectivement, P_1 et P_2 . Par définition du degré, on a donc $a_{\deg(P_1)}, b_{\deg(P_2)} \neq 0$, $a_k = 0$ pour $k > \deg(P_1)$ et $b_k = 0$ pour $k > \deg(P_2)$. Le terme de degré $\deg(P_1)$ de $P_1 + P_2$ vaut donc $a_{\deg(P_1)} + b_{\deg(P_1)}$. Si celui-ci s'annule, alors $\deg(P_1 + P_2) < \deg(P_1) = \max(\deg(P_1), \deg(P_2))$; s'il est non nul, alors $\deg(P_1 + P_2) \geq \deg(P_1) = \max(\deg(P_1), \deg(P_2))$ et donc $\deg(P_1 + P_2) = \max(\deg(P_1), \deg(P_2))$. $\square$

Proposition 2.1.4. La somme et la multiplication par un scalaire munissent $\mathbb{K}[X]$ d'une structure de $\mathbb{K}$ -espace vectoriel de dimension infinie.

Démonstration. Il a déjà été vérifié que $(\mathbb{K}[X], +)$ est un groupe abélien. Les propriétés concernant le produit par un scalaire découlent, quant à elles, de la structure d'anneaux de $\mathbb{K}[X]$. Rappelons en effet que cette opération, introduite dans la remarque 1.6, est définie par $\lambda.P := \psi(\lambda).P$ où ψ identifie, en tant qu'anneau, $\mathbb{K}$ aux polynômes constants. On a alors bien, pour tous $\lambda, \lambda_1, \lambda_2 \in \mathbb{K}$ et $P, P_1, P_2 \in \mathbb{K}[X]$,

- $\lambda.(P_1 + P_2) := \psi(\lambda).(P_1 + P_2) = \psi(\lambda).P_1 + \psi(\lambda).P_2 =: \lambda.P_1 + \lambda.P_2$;
- $(\lambda_1 + \lambda_2).P := \psi(\lambda_1 + \lambda_2).P = (\psi(\lambda_1) + \psi(\lambda_2)).P = \psi(\lambda_1).P + \psi(\lambda_2).P =: \lambda_1.P + \lambda_2.P$;

- $\lambda_1.(\lambda_2.P) := \psi(\lambda_1).(\psi(\lambda_2).P) = (\psi(\lambda_1).\psi(\lambda_2)).P = \psi(\lambda_1.\lambda_2).P =: (\lambda_1.\lambda_2).P$;
- $\bar{1}.P := \psi(\bar{1}).P = 1.P = P$, en notant $\bar{1}$ l'élément unité de $\mathbb{K}$.

L'ensemble $\mathbb{K}[X]$ est donc bien un espace vectoriel.

Concernant sa dimension, considérons une famille finie $\{P_1, \dots, P_k\}$ de polynômes. Il vient de la proposition 2.1.3 que toute combinaison linéaire de ces polynômes sera de degré au plus $n := \max \{\deg(P_i) \mid 1 \leq i \leq k\}$. Cette famille ne peut donc pas être génératrice car, par exemple, X^{n+1} n'est pas combinaison linéaire de polynômes de degré au plus n . On en déduit que $\mathbb{K}[X]$ ne peut donc pas être engendré en tant qu'espace vectoriel par une famille finie, il n'est donc pas de dimension finie. $\square$

Néanmoins, il est souvent agréable de pouvoir raisonner en dimension finie.

Définition 2.1.5. Pour tout $n \in \mathbb{N}^*$, on définit $\mathbb{K}[X]_n := \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$.

Proposition 2.1.6. Pour tout $n \in \mathbb{N}$, $\mathbb{K}[X]_n$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n + 1$.

Démonstration. D'après la proposition 2.1.3, $\mathbb{K}[X]_n$ est stable par somme, opposé et produit par un scalaire. C'est donc bien un sous-espace vectoriel. Il est clair que la famille $(1, X, \dots, X^n)$ est génératrice, montrons maintenant par récurrence sur n qu'elle est libre. Le résultat est évidemment vrai pour $n = 0$. Supposons-le donc vrai au rang n et considérons une relation $\sum_{i=0}^{n+1} a_i X^i = 0$ avec $a_0, \dots, a_{n+1} \in \mathbb{K}$. Si a_{n+1} était non nul, on aurait $X^{n+1} = a_{n+1}^{-1}.a_0 + a_{n+1}^{-1}.a_1 X + \dots + a_{n+1}^{-1}.a_n X^n$, ce qui n'est pas possible car $\deg(X^{n+1}) = n + 1$ et $\deg(a_{n+1}^{-1}.a_0 + a_{n+1}^{-1}.a_1 X + \dots + a_{n+1}^{-1}.a_n X^n) \leq n$. On en déduit que $a_{n+1} = 0$ et donc que $\sum_{i=0}^n a_i X^i = 0$, ce qui par hypothèse de récurrence implique que tous les a_i sont nuls. La famille $(1, X, \dots, X^n)$ est donc une base de cardinal $n + 1$, montrant que $\dim(\mathbb{K}[X]_n) = n + 1$. $\square$

Remarque 2.1.7. Dans la preuve ci-dessus, la famille infinie $\mathcal{B} := (1, X, X^2, \dots)$ se comporte comme une base infinie, dans le sens que toutes les sous-familles finies sont libres, et que tout élément de $\mathbb{K}[X]$ s'écrit comme combinaison linéaire (finie) d'éléments de $\mathcal{B}$. Il est alors tentant d'étendre tout cela à des combinaison linéaires infinies, mais il faut pour cela donner un sens à ces sommes infinies. Nous ne traiterons pas de cela ici, mais cela peut se faire de manière abstraite, on parle alors de séries formelles, ou bien avec des considérations de convergence, on met alors le pied dans l'analyse.

2.2 Intégrité et division

Nous venons de voir que la notion de degré pouvait permettre d'étudier, en tant qu'espace vectoriel, l'ensemble des polynômes. C'est également un outil efficace pour l'étudier en tant qu'anneau.

Proposition 2.2.1. Pour tous $P_1, P_2 \in \mathbb{K}[X]$, on a $\deg(P_1.P_2) = \deg(P_1) + \deg(P_2)$.

Démonstration. Quitte à les permuter, par commutativité du produit, on peut supposer $\deg(P_1) \geq \deg(P_2)$. Au sein de la preuve de la proposition 1.4, nous avons déjà montré que $\deg(P_1.P_2) \leq \deg(P_1) + \deg(P_2)$. Si P_2 est nul, alors $\deg(P_1.P_2) = \deg(0) = -\infty = \deg(P_1) + \deg(P_2)$. Sinon, on note $(a_k)_{k \in \mathbb{N}}$ et $(b_k)_{k \in \mathbb{N}}$ les coefficients de, respectivement, P_1 et P_2 . Par définition du degré, on a donc $a_{\deg(P_1)}, b_{\deg(P_2)} \neq$

0, $a_k = 0$ pour $k > \deg(P_1)$ et $b_k = 0$ pour $k > \deg(P_2)$. On en déduit

$$\begin{aligned}
(P_1 \cdot P_2)_{\deg(P_1) + \deg(P_2)} &= \sum_{i=0}^{\deg(P_1) + \deg(P_2)} a_i \cdot b_{\deg(P_1) + \deg(P_2) - i} \\
&= \left(\sum_{i=0}^{\deg(P_1) - 1} a_i \cdot b_{\deg(P_1) + \deg(P_2) - i} \right) + a_{\deg(P_1)} \cdot b_{\deg(P_2)} \\
&\quad + \left(\sum_{i=\deg(P_1) + 1}^{\deg(P_1) + \deg(P_2)} a_i \cdot b_{\deg(P_1) + \deg(P_2) - i} \right) \\
&= \left(\sum_{i=0}^{\deg(P_1) - 1} a_i \cdot 0 \right) + a_{\deg(P_1)} \cdot b_{\deg(P_2)} + \left(\sum_{i=\deg(P_1) + 1}^{\deg(P_1) + \deg(P_2)} 0 \cdot b_{\deg(P_1) + \deg(P_2) - i} \right) \\
&= a_{\deg(P_1)} \cdot b_{\deg(P_2)} \neq 0.
\end{aligned}$$

De fait $\deg(P_1 \cdot P_2) \geq \deg(P_1) + \deg(P_2)$, et donc $\deg(P_1 \cdot P_2) = \deg(P_1) + \deg(P_2)$. $\square$

Corollaire 2.2.2. L'anneau $\mathbb{K}[X]$ est intègre et les inversibles sont les polynômes constants non nuls, c'est-à-dire les polynômes de degré 0.

Démonstration. Si $P_1, P_2 \in \mathbb{K}[X]^*$, alors $\deg(P_1), \deg(P_2) \geq 0$ et donc $\deg(P_1 \cdot P_2) \geq 0$, c'est-à-dire $P_1 \cdot P_2 \neq 0$, ce qui montre par contraposé que $\mathbb{K}[X]$ est intègre.

Soit $P \in \mathbb{K}[X]^\times$. Il existe donc $P^{-1} \in \mathbb{K}[X]^*$ tel que $P \cdot P^{-1} = 1$. Puisque $P^{-1} \neq 0$, on a $\deg(P^{-1}) \geq 0$ et de fait $\deg(P) \leq \deg(P) + \deg(P^{-1}) = \deg(P \cdot P^{-1}) = \deg(1) = 0$. On en déduit que $\deg(P) = 0$. Réciproquement, il est clair que tout polynôme constant non nul est inversible. $\square$

Remarque 2.2.3. Les éléments de $\mathbb{K}[X]^* \setminus \mathbb{K}[X]^\times$ sont exactement les polynômes de degré 1 ou plus, c'est-à-dire de degré strictement positif.

Il est donc impossible de diviser par des polynômes de degré strictement positif. Mais à l'instar des nombres entiers, il est toutefois possible de définir une notion de division euclidienne.

Proposition 2.2.4. Soit $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]^*$. Il existe $R, S \in \mathbb{K}[X]$ avec $\deg(R) < \deg(Q)$ tels que $P = Q \cdot S + R$.

Démonstration. Soit $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]^*$. Montrons par récurrence généralisée sur $\deg(P)$ qu'il existe $R, S \in \mathbb{K}[X]$ tels que $P = S \cdot Q + R$ avec $\deg(R) < \deg(Q)$.

Si $\deg(P) < \deg(Q)$, alors le résultat est vrai en posant $S = 0$ et $R = P$. Supposons maintenant le résultat vrai en degré $n \geq \deg(Q) - 1$ et considérons P de degré $n + 1 \geq \deg(Q)$. Alors, P et Q étant non nuls, on peut noter $a_P, a_Q \in \mathbb{K}^*$ leurs coefficients dominants et considérer P et $a_P \cdot a_Q^{-1} \cdot X^{\deg(P) - \deg(Q)} \cdot Q$ qui sont deux polynômes de même degré $n + 1$ et de même coefficient dominant. D'après la proposition 2.1.3, $\deg(P - a_P \cdot a_Q^{-1} \cdot X^{\deg(P) - \deg(Q)} \cdot Q) \leq n$ et, par hypothèse de récurrence, il existe donc $R, \tilde{S}$ tels que $P - a_P \cdot a_Q^{-1} \cdot X^{\deg(P) - \deg(Q)} \cdot Q = \tilde{S} \cdot Q + R$ et $\deg(R) < \deg(Q)$. Il ne reste plus qu'à poser $S := a_P \cdot a_Q^{-1} \cdot X^{\deg(P) - \deg(Q)} + \tilde{S}$ pour conclure. $\square$

Remarque 2.2.5. De cette preuve, on peut extraire un algorithme de division euclidienne pour les polynômes très similaire à celui de la division telle que pratiquée dans les écoles primaires. En effet, la démonstration consiste à identifier ce par quoi il faut multiplier Q pour que son coefficient dominant soit égal à celui de P , de sorte à ce que, en retranchant ce produit à P on fasse diminuer le degré, et on répète cela jusqu'à obtenir un reste de degré strictement inférieur à celui de Q . Sur l'exemple $P := 2X^3 - X + 1$ et $Q := X^2 + 2X - 1$, cela donne :

étape 1 : par quoi faut-il multiplier $X^2 + 2X - 1$ pour avoir un coefficient dominant égal à celui de $2X^3 - X + 1$? Réponse : $2X$.

On pose alors $P_2 := P - 2X.Q = 2X^3 - X + 1 - 2X.(X^2 + 2X - 1) = -4X^2 + X + 1$.

étape 2 : par quoi faut-il multiplier $X^2 + 2X - 1$ pour avoir un coefficient dominant égal à celui de $-4X^2 + X + 1$? Réponse : -4 .

On pose alors $P_3 := P_2 + 4.Q = -4X^2 + X + 1 + 4.(X^2 + 2X - 1) = 9X - 3$.

On a enfin $\deg(9X - 3) = 1 < 2 = \deg(X^2 + 2X - 1)$, et on en déduit que

$$P = P_2 + 2X.Q = P_3 - 4.Q + 2X.Q = (2X - 4).Q + (9X - 3).$$

Ecrit façon *école primaire*, cela donne :

$$\begin{array}{ccc}
 \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 \end{array} \\
 \hline
 \end{array} & \rightsquigarrow & \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 2X \\
 \hline
 \end{array} \\
 \hline
 \end{array} \\
 \\
 \begin{array}{ccc}
 \rightsquigarrow & \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 - \quad (2X^3 \quad 4X^2 \quad -2X) \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 2X \\
 \hline
 \end{array} \\
 \hline
 \end{array} & \rightsquigarrow & \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 - \quad (2X^3 \quad 4X^2 \quad -2X) \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 2X \\
 \hline
 -4X^2 \quad X \quad +1 \\
 \hline
 2X \\
 \hline
 \end{array} \\
 \hline
 \end{array} \\
 \\
 \begin{array}{ccc}
 \rightsquigarrow & \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 - \quad (2X^3 \quad 4X^2 \quad -2X) \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 2X - 4 \\
 \hline
 -4X^2 \quad X \quad +1 \\
 - \quad (-4X^2 \quad -8X \quad +4) \\
 \hline
 \end{array} \\
 \hline
 \end{array} & \rightsquigarrow & \begin{array}{c|c}
 \begin{array}{r}
 2X^3 \quad -X \quad +1 \\
 - \quad (2X^3 \quad 4X^2 \quad -2X) \\
 \hline
 \end{array} & \begin{array}{r}
 X^2 + 2X - 1 \\
 \hline
 2X - 4 \\
 \hline
 -4X^2 \quad X \quad +1 \\
 - \quad (-4X^2 \quad -8X \quad +4) \\
 \hline
 9X \quad -3 \\
 \hline
 \end{array} \\
 \hline
 \end{array}
 \end{array}
 \end{array}$$

Proposition 2.2.6. Pour tout $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]^*$, les $R, S \in \mathbb{K}[X]$ tels que $P = S.Q + R$ et $\deg(R) < \deg(Q)$ sont uniques.

Démonstration. Supposons que $S_1.Q + R_1 = P = S_2.Q + R_2$ avec $R_1, R_2, S_1, S_2 \in \mathbb{K}[X]$, $Q \in \mathbb{K}[X]^*$ et $\deg(R_1), \deg(R_2) < \deg(Q)$. Alors $Q.(S_2 - S_1) = R_1 - R_2$ et donc $\deg(Q.(S_2 - S_1)) = \deg(R_1 - R_2) < \deg(Q)$. Mais par ailleurs, $\deg(Q.(S_2 - S_1)) = \deg(Q) + \deg(S_2 - S_1) \geq \deg(Q)$ sauf si $\deg(S_2 - S_1) = -\infty$. On en déduit donc que $S_2 - S_1 = 0$, c'est-à-dire $S_2 = S_1$, et donc $R_1 = P - S_1.Q = P - S_2.Q = R_2$. $\square$

Corollaire 2.2.7. Soit $P, Q \in \mathbb{R}[X] \subset \mathbb{C}[X]$ avec $Q \neq 0$. Alors les divisions euclidiennes de P par Q dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$ donnent les mêmes résultats.

Démonstration. Soit $R, S \in \mathbb{R}[X]$ donnés par la division euclidienne de P par Q dans $\mathbb{R}[X]$. Alors $P = S.Q + R$ avec $R, S \in \mathbb{C}[X]$ et $\deg(R) < \deg(Q)$. Par unicité, cela correspond donc également à la division euclidienne de P par Q dans $\mathbb{C}[X]$. $\square$

Dès lors, on peut, toujours à l'image des entiers, définir une notion de divisibilité.

Définition 2.2.8. On dit que $Q \in \mathbb{K}[X]^*$ *divise* $P \in \mathbb{K}[X]$, ou encore que P est un *multiple* de Q , si le reste de la division euclidienne de P par Q est nul.

Remarque 2.2.9. Dire que $Q \in \mathbb{K}[X]^*$ divise $P \in \mathbb{K}[X]$, cela revient à dire que P s'écrit sous la forme $Q.S$ avec $S \in \mathbb{K}[X]$, ou encore que P appartient à (Q) , l'idéal de $\mathbb{K}[X]$ engendré par Q .