Anneau des polynômes

Emmanuel Vieillard-Baron[1], Alain Soyeur[2], and François Capaces[3]

[1]Enseignant en CPGE, Lycée Kléber, Strasbourg
[2]Enseignant en CPGE, Lycée Pierre de Fermat, Toulouse
[3], ,

30 janvier 2022

1 Anneau des polynômes

N. H. Abel

Etude de l'anneau des polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$

> . . . polynomials are notoriously untrustworthy when extrapolated.
> WG Cochran, GM Cox Experimental designs.

Dans tout ce chapitre :

— $\mathbb{K}$ désigne un corps ($\mathbb{R}$ ou $\mathbb{C}$).

— $\mathbb{K}^{\mathbb{N}}$ ou $\mathscr{S}(\mathbb{K})$ représente l'ensemble des suites à coefficients dans $\mathbb{K}$.

— m, n, p, q, $r \in \mathbb{N}$ sont des entiers.

Pour bien aborder ce chapitre

Les polynômes sont étudiés depuis la plus haute antiquité. Les babyloniens savaient résoudre les équations du second degré. Plus généralement, la résolution des équations polynomiales a été un moteur de l'étude des polynômes. Nous avons déjà évoqué Tartaglia et Cardano éprouvant le besoin d'introduire les nombres complexes pour résoudre les équations du troisième et quatrième degré, ainsi que Galois aux prises avec les équations du cinquième degré.

François Viète (1540-1603) semble être le premier à les avoir ainsi dénommés.

Pour autant, qu'est-ce qu'un polynôme ? Prenons un exemple. Soit

$$f : \begin{array}{rcl} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & f(x) = 3x^4 - 2x^2 + x + 1 \end{array}.$$

On peut résumer toute l'information contenue dans $f(x)$ à l'aide de la liste de ses coefficients : 1 ; 1 ; -2 ; 0 et 3. Un autre polynôme $g(x) = x^2 - x - 2$ se verra attribuer -2 ; -1 et 2 comme liste des coefficients. On voit par là que la liste est à longueur variable ce qui n'est pas confortable.

Pour que tous les polynômes soient logés à la même enseigne, on considère une suite (donc infinie) de coefficients pour chaque polynôme en rajoutant des zéros. Autrement dit, un polynôme est assimilé à une suite de coefficients tous nuls sauf (peut-être) un nombre fini d'entre eux.

C'est cette définition purement algébrique qui va être suivie dans ce chapitre. Faudra-t-il pour autant oublier nos bonnes vieilles fonctions polynomiales ? Certes non ! D'abord elles sont à la base de cette nouvelle définition et elles permettent d'établir, via le théorème des valeurs intermédiaires, que tout polynôme réel de degré impair admet au moins une racine réelle.

Ce chapitre a beaucoup de points communs avec le précédent. Cependant, il faudra une fois de plus attendre les espaces vectoriels pour bien comprendre les tenants et les aboutissants de celui-ci.

1.1 Polynômes à une indéterminée

1.1.1 Définitions

DÉFINITION 0.1 **Polynômes**
On appelle *polynôme à coefficients dans* $\mathbb{K}$ une suite (a_n) d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang :

$$(a_n) = (a_0, a_1, \dots, a_k, 0, \dots)$$

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

DÉFINITION 0.2 **Opérations sur** $\mathbb{K}[X]$
On définit les opérations suivantes sur les polynômes : Soient les polynômes $P = (a_0, a_1, \dots, a_n, 0, \dots) \in \mathbb{K}[X]$, $Q = (b_0, b_1, \dots, b_n, 0, \dots) \in \mathbb{K}[X]$ et le scalaire $\lambda \in \mathbb{K}$:

$$P + Q = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, 0, \dots)$$
$$\lambda \cdot P = (\lambda \cdot a_0, \lambda \cdot a_1, \dots, \lambda \cdot a_n, 0, \dots)$$
$$P \times Q = (c_0, c_1, \dots, c_n, \dots) \text{ où : } \forall k \in \mathbb{N}, \quad c_k = \sum_{k=0}^{+\infty} a_k b_{n-k}$$

Remarque 0.1

— A partir d'un certain rang (exercice !), la suite (c_k) est nulle. La multiplication est donc bien définie dans $\mathbb{K}[X]$.

— L'addition et la multiplication par un scalaire précédemment définies coïncident avec l'addition et la multiplication définies sur l'espace des suites à coefficients dans $\mathbb{K}$: $\mathbb{K}^{\mathbb{N}}$. Ce n'est par contre pas le cas de la multiplication entre polynômes, qui ne coïncide pas avec celle définie entre les suites.

— Pour une suite de nombres (a_k) qui sont tous nuls sauf un nombre fini, le nombre

$$\sum_{k=0}^{+\infty} a_k$$

est la somme de tous les nombres non nuls de cette suite.

En prenant un peu d'avance sur le chapitre **??**, on peut énoncer la proposition suivante.

PROPOSITION 0.1 **Structure de $\mathbb{K}[X]$**

- $(\mathbb{K}[X], +, \cdot)$ est un sous-espace vectoriel du $\mathbb{K}$-espace vectoriel $\mathbb{K}^{\mathbb{N}}$. Le vecteur nul est le polynôme $(0, \dots)$.
- $(\mathbb{K}[X], +, \times)$ est un anneau commutatif unitaire. L'élément neutre de la loi $\times$ est le polynôme $(1, 0, \dots)$.

Remarque 0.2

- Attention, en raison de la remarque précédente, $(\mathbb{K}, +, \times)$ n'est pas un sous-anneau de $\left(\mathbb{K}^{\mathbb{N}}, +, \times\right)$.
- Comme $(\mathbb{K}[X], +, \times)$ est un anneau commutatif, la formule du binôme est vraie dans $\mathbb{K}[X]$.

Notations définitives :
On note :

- 1 le polynôme $(1, 0, \dots)$.
- X le polynôme $(0, 1, 0, \dots)$.

En multipliant le polynôme X par lui-même, on obtient pour X^n, le polynôme :

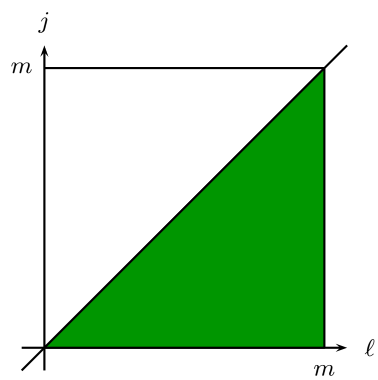
$$\begin{array}{c} (0, \dots, 0, \dots \qquad , 1, \qquad 0, \dots) \, . \\ \uparrow \\ \text{place d'indice } n \end{array}$$

Avec ces notations, si $P \in \mathbb{K}[X]$ est donné par $P = (a_0, a_1, \dots, a_n, 0, \dots)$, on a :

$$\begin{aligned} P = & \; a_0 (1, 0, \dots) + a_1 (0, 1, \dots) + \dots + a_n (0, \dots, 0, 1, 0, \dots) \\ = & \; a_0 \cdot 1 + a_1 \cdot X + \dots + a_n \cdot X^n = \; a_0 + a_1 X + \dots + a_n X^n. \end{aligned}$$

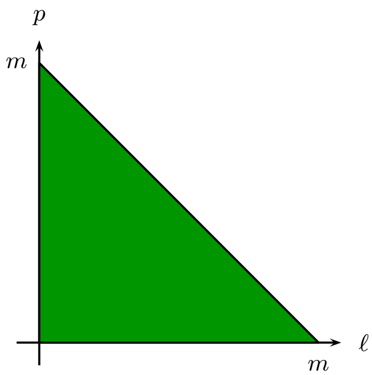
Démonstration *Du fait que la multiplication des polynômes est abstraite, il est nécessaire d'effectuer un certain nombre de vérifications qui n'auraient pas lieu d'être avec des fonctions polynomiales. La plupart de ces vérifications sont immédiates.*
La multiplication est commutative : Soient $P = a_0 + \dots + a_p X^p \in \mathbb{K}[X]$ et $Q = b_0 + \dots + b_p X^q \in \mathbb{K}[X]$, on a : $PQ = c_0 + \dots + c_{p+q} X^{p+q}$ avec, pour $k = 0, \dots, p+q$, $c_k = \sum_{\ell=0}^{k} a_\ell b_{n-\ell} = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$. En effectuant la somme de droite à gauche, c'est-à-dire en effectuant le changement d'indice $p = k - \ell$, $c_k = a_k b_0 + a_{k-1} b_1 + \ldots + a_1 b_{k-1} + a_0 b_k$ ce qui est le coefficient d'indice k du polynôme QP. Donc $PQ = QP$.
Associativité : Soit $P = \sum_i a_i X^i$, $Q = \sum_j b_j X^j$, $R = \sum_k b_k X^k$. On a $PQ = \sum_\ell d_\ell X^\ell$ avec $c_\ell = \sum_{i=0}^{\ell} a_i b_{\ell-i}$. On a alors $(PQ)R = \sum_m f_m X^m$ avec

$$
\begin{aligned}
f_m &= \sum_{\ell=0}^{m} d_\ell c_{m-\ell} \\
&= \sum_{\ell=0}^{m} \left(\sum_{j=0}^{\ell} a_{\ell-j} b_j \right) c_{m-\ell} \\
&= \sum_{\ell=0}^{m} \sum_{j=0}^{\ell} a_{\ell-j} b_j c_{m-\ell} \\
&= \sum_{j=0}^{m} \sum_{\ell=j}^{m} a_{\ell-j} b_j c_{m-\ell}.
\end{aligned}
$$



On effectue un changement d'indice $p = \ell - j$ c'est-à-dire $\ell = p + j$.

$$
\begin{aligned}
f_m &= \sum_{j=0}^{m} \sum_{p=0}^{m-j} a_p b_j c_{m-p-j} \\
&= \sum_{p=0}^{m} \sum_{j=0}^{m-p} a_p b_j c_{m-p-j} \\
&= \sum_{p=0}^{m} a_p \sum_{j=0}^{m-p} b_j c_{m-p-j} \\
&= \sum_{p=0}^{m} a_p g_{m-p}
\end{aligned}
$$



où $g_n = \sum_{q=0}^{n} b_q c_{n-q}$ désigne le n-ième coefficient de QR. Autrement dit f_m est aussi le m-ième coefficient de $P(QR)$.
Le principal intérêt de l'algèbre linéaire (qui ne va plus tarder maintenant) est d'éviter ce genre de démonstration particulièrement indigeste. Voici comment nous pourrons rédiger une démonstration très bientôt.
Soit Q et R deux polynômes. On cherche à démontrer que $\begin{array}{rccl} \Phi_{Q,R} & : \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & P & \longmapsto & (PQ)R - P(QR) \end{array}$ *est l'application nulle. Or $\Phi_{Q,R}$ est une application linéaire. Pour démontrer que son image est réduite au vecteur nul, il suffit de démontrer que toutes les images d'une famille génératrice sont nulles. Par exemple que $\forall\, n \in \mathbb{N}, \Phi_{Q,R}(X^n) = (X^n Q)R - X^n(QR) = 0$.*
Pour cela, soit $n \in \mathbb{N}$ et $R \in \mathbb{K}[X]$ On cherche donc à démontrer que $\begin{array}{rccl} \Psi_{n,R} & : \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X] \\ & Q & \longmapsto & (X^n Q)R - X^n(QR) \end{array}$ *est l'application nulle. Or $\Psi_{n,R}$ est une application linéaire. Pour démontrer que son image est réduite au vecteur nul, il suffit de démontrer que toutes les images d'une famille génératrice sont nulles. Par exemple que $\forall\, m \in \mathbb{N}, \Psi_{n,R}(X^m) = (X^n X^m)R - X^n(X^m R) = 0$.*
Pour cela, soit $n \in \mathbb{N}$ et $m \in \mathbb{N}$ On cherche donc à démontrer que $\begin{array}{rccl} \Theta_{n,m} & : \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]\, Q \\ & & \longmapsto & (X^n X^m)R - X^n(X^m R) \end{array}$ *est l'application nulle. Or $\Theta_{n,m}$ est une application linéaire. Pour démontrer que son image est réduite au vecteur nul, il suffit de démontrer que toutes les images d'une famille génératrice sont nulles. Par exemple que $\forall\, p \in \mathbb{N}, \Psi_{n,R}(X^p) = (X^n X^m)X^p - X^n(X^m X^p) = 0$. Or cette dernière égalité est vérifiée immédiatement. Ce qui établit le résultat.*

1.1.2 Degré d'un polynôme

Définition 0.3 **Degré d'un polynôme, terme dominant**
Soit un polynôme $P = a_0 + \cdots + a_p X^p \in \mathbb{K}[X]$ avec $a_p \neq 0$.

- On appelle *degré de P* et on note $\deg(P)$ l'entier p.
- Par convention, le *degré du polynôme nul* est $-\infty$.
- On appelle *terme dominant* de P le monôme $a_p X^p$.

Définition 0.4 **Polynôme normalisé**
On appelle polynôme *normalisé* un polynôme dont le terme dominant est égal à 1.

Théorème 0.2 **Degré d'un produit, degré d'une somme**
Soient P, $Q \in \mathbb{K}[X]$, on a :

1. $\boxed{\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))}$;
2. $\boxed{\deg(P \times Q) = \deg(P) + \deg(Q)}$.

Démonstration

1. — *Si* $P = Q = 0$ *alors* $\deg P = \deg Q = -\infty$, $\deg(P+Q) = -\infty$ *et la formule est prouvée dans ce cas.*
   — *Si* P *ou* Q *est non nul alors, supposant, quitte à interchanger* P *et* Q*, que* $P \neq 0$*, on a :* $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{n} b_k X^k$ *où* $n = \max(\deg P, \deg Q)$ *et où les* a_k *pour* $k \in [\![1, n]\!]$ *ne sont pas tous nuls (en l'occurrence, les* b_k *peuvent être tous nuls). On a donc :* $P + Q = \sum_{k=0}^{n} (a_k + b_k) X^k$*. Si* $a_n + b_n \neq 0$ *alors* $\deg(P+Q) = \max(\deg P, \deg Q)$ *et sinon* $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$.
2. — *Si* $P = 0$ *ou* $Q = 0$ *alors* $PQ = 0$ *et* $\deg(PQ) = -\infty = \deg P + \deg Q$ *d'après les lois d'addition dans*

R.

— *Sinon, on suppose que* $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{m} b_k X^k$ *où* $a_n \neq 0$ *et où* $b_m \neq 0$*. Par conséquent,* $n = \deg P$ *et* $m = \deg Q$*. Quitte à échanger le rôle de* P *et de* Q*, on peut supposer que* $n \geqslant m$*. Soit* $l \in \mathbb{N}$*. Notons* c_l *le coefficient d'indice* l *dans* PQ*. D'après la définition du produit de deux polynômes 0.2 et d'après la remarque suivant cette définition, on a :*

$$c_l = \begin{cases} \sum_{k=0}^{l} a_k b_{l-k} & \text{si } l < m + n0 \\ \text{si } l \geqslant m + n \end{cases} .$$

Nécessairement, $\deg(PQ) \leqslant m + n$*. Mais le coefficient d'indice* $m + n$ *dans* PQ *est* $a_n b_m \neq 0$ *donc* $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Remarque 0.3 Si $\deg(P) \neq \deg(Q)$ alors $\deg(P+Q) = \max(\deg(P), \deg(Q))$.

Proposition 0.3 **Intégrité de l'anneau des polynômes** $\mathbb{K}[X]$
Soient P, $Q \in \mathbb{K}[X]$.

$$\boxed{P \times Q = 0 \Rightarrow P = 0 \text{ ou } Q = 0}$$

Démonstration *Si* $P \times Q = 0$ *alors* $\deg(P \times Q) = -\infty = \deg P + \deg Q$ *ce qui n'est possible que si* $\deg P = -\infty$ *ou* $\deg Q = -\infty$ *et donc que si* $P = 0$ *ou* $Q = 0$.

Proposition 0.4 Éléments inversibles de l'anneau $\mathbb{K}[X]$
Les seuls éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes de degré 0, c'est-à-dire les polynômes constants non nuls.
Autrement dit, si $P, Q \in \mathbb{K}[X]$ et si $P \times Q = 1$ alors il existe $\alpha \in \mathbb{K}^*$ tel que $P = \alpha$ et $Q = \alpha^{-1}$.

Démonstration *Soit $P \in \mathbb{K}[X]$ un polynôme inversible. Il existe alors un polynôme $Q \in \mathbb{K}[X]$ tel que : $P \times Q = 1$. On a donc : $\deg P + \deg Q = 0$. Cette égalité n'est possible que si $\deg P = \deg Q = 0$ et donc que si P est un polynôme constant non nul. Réciproquement, si P est un polynôme constant non nul alors il est clair que P est inversible.*

1.1.3 Valuation d'un polynôme

Définition 0.5 Valuation d'un polynôme
Soit un polynôme $P = a_0 + \cdots + a_p X^p \in \mathbb{K}[X]$ non nul. On appelle *valuation de P* le plus petit entier k tel que $a_k \neq 0$. On le note $\mathrm{val}(P)$.
Par définition, la valuation du polynôme nul est $\mathrm{val}(0) = +\infty$

Théorème 0.5 Valuation d'un produit, valuation d'une somme
Soient $P, Q \in \mathbb{K}[X]$, on a :

1. $\boxed{\mathrm{val}(P+Q) \geqslant \min(\mathrm{val}(P), \mathrm{val}(Q))}$;
2. $\boxed{\mathrm{val}(P \times Q) = \mathrm{val}(P) + \mathrm{val}(Q)}$.

1.1.4 Composition de polynômes

Définition 0.6 Composition de deux polynômes
Soient deux polynômes $P, Q \in \mathbb{K}[X]$. On suppose que $P = a_0 + a_1 X + \cdots + a_n X^n$. On définit le *polynôme composé* de Q par P, noté $P \circ Q$, par :

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

Proposition 0.6
Soient deux polynômes non nuls $P, Q \in \mathbb{K}[X]$. Alors :

$$\boxed{\deg(P \circ Q) = \deg(P) \times \deg(Q)}.$$

Démonstration *Supposons que $P = a_0 + a_1 X + \cdots + a_n X^n$. Comme $P \neq 0$, on a $a_n \neq 0$. Alors $P \circ Q = \sum_{k=0}^{n} a_k Q^k$ et $\deg(P \circ Q) = \deg Q^n = n \deg Q = \deg P \times \deg Q$ car $Q \neq 0$.*

1.1.5 Division euclidienne

DÉFINITION 0.7 **Divisibilité**
Soient deux polynômes $A, B \in \mathbb{K}[X]$. On dit que A *divise* B si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $B = QA$. On le note $A|B$.

Exemple 0.1

— $(X-1)$ divise $X^2 - 2X + 1$. En effet : $X^2 - 2X + 1 = (X-1)^2$
— $(X-1)$ divise $X^2 - 1$. En effet : $X^2 - 1 = (X-1)(X+1)$.
— $(1-X)$ divise $1 - X^{n+1}$. En effet : $1 - X^{n+1} = \left(1 + X + X^2 + \cdots + X^n\right)(1-X)$.

PROPOSITION 0.7 **Polynômes associés**
Soient $A, B \in \mathbb{K}[X]$ deux polynômes non nuls. On a équivalence entre :

1. $A|B$ et $B|A$.
2. $\exists \lambda \in \mathbb{K}^* : \quad B = \lambda A$.

Deux tels polynômes sont dits *associés*.

Démonstration

— *Supposons que $A|B$ et $B|A$. Alors il existe des polynômes $Q_1, Q_2 \in \mathbb{K}[X]$ tels que : $A = Q_1 B$ et $B = Q_2 A$. On a alors : $A = (Q_1 Q_2) A$ ou encore : $A(1 - Q_1 Q_2) = 0$. Par intégrité de $\mathbb{K}[X]$ 0.3, comme $A \neq 0$, ceci n'est possible que si $1 - Q_1 Q_2 = 0$ c'est-à-dire si : $Q_1 Q_2 = 1$. Par conséquent, Q_1 et Q_2 sont des polynômes inversibles inverses l'un de l'autre. Appliquant la proposition 0.4, il existe $\alpha \in \mathbb{K}^*$ tel que $Q_1 = \alpha$ et $Q_2 = \alpha^{-1}$. On a alors $B = \alpha A$. A et B snt donc bien associés.*
— *La réciproque est triviale.*

THÉORÈME 0.8 **Division euclidienne**
Soient $A, B \in \mathbb{K}[X]$ deux polynômes. On suppose que $B \neq 0$. Alors il $\boxed{\textbf{existe}}$ un $\boxed{\textbf{unique}}$ couple (Q, R) de polynômes de $\mathbb{K}[X]$ vérifiant :

$$\boxed{\left\{ \quad 1 \quad A = BQ + R \quad 2 \quad \deg(R) < \deg(B) \right.}.$$

Démonstration

— *Soient $(Q_1, R_1) \in (\mathbb{K}[X])^2$ et $(Q_2, R_2) \in (\mathbb{K}[X])^2$ tels que :*

$$\begin{cases} A = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases} \qquad et \qquad \begin{cases} A = BQ_2 + R_2 \\ \deg(R_2) < \deg(B) \end{cases}$$

alors $B(Q_1 - Q_2) = R_1 - R_2$ et donc, si $Q_1 - Q_2 \neq 0$, $\deg(B(Q_1 - Q_2)) = \deg(R_1 - R_2) < \deg B$. Par ailleurs $\deg(B(Q_1 - Q_2)) = \deg B + \deg(Q_1 - Q_2) \geqslant \deg B$ ce qui constitue une contradiction. Si $Q_1 = Q_2$ alors $R_1 - R_2 = 0$ et $R_1 = R_2$.

— *La démonstration se fait par récurrence sur $n = \deg A$. Fixons pour toute la suite $B = b_0 + b_1 X + \cdots + b_m X^m$ avec $b_m \neq 0$ et pour tout $n \in \mathbb{N}$, notons P_n la propriété :*

$$P_n : \text{ pour tout } A \in \mathbb{K}[X] \text{ de degré } n, \text{ il existe } (Q,R) \in (\mathbb{K}[X])^2 \text{ tels que } \begin{cases} 1 & A = BQ + R \\ 2 & \deg(R) < \deg(B) \end{cases}$$

— *$P_0, P_1, \ldots, P_{m-1}$ sont vraies. Si A est un polynôme de degré $n \in [\![0, m-1]\!]$, il suffit de prendre $Q = 0$ et $R = A$. On a bien : $A = BQ + R$ et $\deg R = \deg A = n < m$.*

— *Soit $n \geqslant m$.*

— *Supposons que la propriété P_n est vraie. C'est notre hypothèse de récurrence et montrons que P_{n+1} est vraie. Soit $A = a_0 + a_1 X + \cdots + a_{n+1} X^{n+1}$ un polynôme de degré $n+1$. Posons $A_1 = A - \frac{a_{n+1}}{b_m} X^{n-m} B$. Le polynôme A_1 est de degré n. On lui applique alors l'hypothèse de récurrence. Il existe $(Q_1, R_1) \in (\mathbb{K}[X])^2$ tels que $\{ \; 1 \quad A_1 = Q_1 B + R_1 \quad 2 \quad \deg(R_1) < \deg(B)$. Posons $Q = Q_1 + \frac{a_{n+1}}{b_m} X^{n-m}$ et $R = R_1$. On a :*

$$QB + R = \left(Q_1 + \frac{a_{n+1}}{b_m} X^{n-m}\right) B + R_1 = BQ_1 + R + \frac{a_{n+1}}{b_m} X^{n-m} B = A_1 + \frac{a_{n+1}}{b_m} X^{n-m} B = A$$

et $\deg R < \deg B$.

— *Le théorème est alors prouvé par application du théorème de récurrence.*

Exemple 0.2

$$\begin{array}{rrrrr|l}
X^3 & + & & X & + \; 1 & X+1 \\ \cline{6-6}
-(X^3 & + & X^2) & & & X^2 - X + 2 \\ \cline{1-3}
 & & -X^2 & + \; X & & \\
 & & -(-X^2 & - \; X) & & \\ \cline{3-4}
 & & & 2X & + \; 1 & \\
 & & & -(2X & + \; 2) & \\ \cline{1-3}
 & & & & -1 &
\end{array}$$

On a donc : $X^3 + X + 1 = (X+1)\left(X^2 - X + 2\right) - 1$ et $\deg(-1) = 0 < \deg(X+1) = 1$.

1.1.6 Division selon les puissances croissantes

La division des polynômes suivant les puissances croissantes est hors programme mais est utile dans de nombreux cas. Nous la présentons à titre complémentaire.

> Théorème 0.9 **Division selon les puissances croissantes**
> Soient A et B deux polynômes à coefficients dans $\mathbb{K}$. On suppose que le terme constant de B n'est pas nul et on note p un entier supérieur ou égal au degré de B. Il existe un unique couple de polynômes (Q,R) tels que $A = BQ + X^{p+1} R$ et $\deg Q \leqslant p$.

Exemple 0.3 $\quad A = 1 + 3X + 2X^2 - 7X^3, \quad B = 1 + X - 2X^2 \quad p = 3$. La présentation est celle de la division des nombres décimaux lorsqu'on veut un quotient à 10^{-p}. Le rôle de X étant joué par 10^{-1}.

$$
\begin{array}{cccccc|cccc}
1 & +3X & +2X^2 & -7X^3 & & & 1 & +X & -2X^2 & \\
\hline
 & +2X & +4X^2 & -7X^3 & & & 1 & +2X & +2X^2 & -5X^3 \\
 & & +2X^2 & -3X^3 & & & & & & \\
 & & & -5X^3 & +4X^4 & & & & & \\
 & & & & +9X^4 & -10X^5 & & & &
\end{array}
$$

Ce qui s'écrit :

$$\underbrace{1+3X+2X^2-7X^3}_{A} = \underbrace{(1+X-2X^2)}_{B}\underbrace{(1+2X+2X^2-5X^3)}_{Q} + X^4\underbrace{(9-10X)}_{R}.$$

On peut l'interpréter en termes de développements limités en zéro :

$$\frac{1+3x+2x^2-7x^3}{1+x-2x^2} = 1+2x+2x^2-5x^3+o(x^3).$$

Démonstration

1. $\boxed{\text{Unicité}}$
On suppose l'existence de deux couples $(Q_1, R_1), (Q_2, R_2)$ résultat de la division selon les puissances croissantes de A par B à l'ordre p, on va montrer qu'ils sont égaux. On dispose des égalités :

$$A = BQ_1 + X^{p+1}R_1, \quad A = BQ_2 + X^{p+1}R_2 \quad \text{donc} \quad B(Q_1 - Q_2) = X^{p+1}(R_2 - R_1).$$

On regarde les valuations des deux membres. Par hypothèse $\text{val}\, B = 0$. Donc $\text{val}\, B(Q_1 - Q_2) = \text{val}\, B + \text{val}\,(Q_1 - Q_2) = \text{val}\,(Q_1 - Q_2)$. D'autre part $\text{val}\, X^{p+1}(R_2 - R_1) \geqslant p+1$. Conclusion : $Q_1 - Q_2$ est un polynôme dont la valuation est supérieure au degré, c'est donc le polynôme nul. Donc $Q_1 = Q_2$ et par suite $R_1 = R_2$.

2. $\boxed{\text{Existence}}$ *Comme dans l'exemple, on va poser notre division, supposer qu'on a réussi à l'ordre p et passer à l'ordre $p+1$.*

$$A = a_0 + \cdots + a_{n-1}X^{n-1} + a_nX^n \quad \text{et} \quad B = b_0 + \cdots + b_{n-1}X^{n-1} + b_nX^n \quad \text{avec} \quad b_0 \neq 0$$

On raisonne donc par récurrence sur p. Si $p = 0$:

$$A = \frac{a_0}{b_0}B + X.R_0 \quad \text{avec} \quad R_0 = \left(a_1 - \frac{a_0b_1}{b_0}\right) + \left(a_2 - \frac{a_0b_2}{b_0}\right)X + \cdots + \left(a_n - \frac{a_0b_n}{b_0}\right)X^{n-1}$$

$Q_0 = \dfrac{a_0}{b_0}$ et on a bien $\deg Q_0 \leqslant p$.
On suppose maintenant le résultat vrai pour l'ordre p et montrons le à l'ordre $p+1$. L'hypothèse de récurrence montre l'existence d'un couple (Q_p, R_p) tel que :

$$A = Q_pB + X^{p+1}R_p \quad \text{avec} \quad \deg Q_p \leqslant p.$$

On applique la division selon les puissances croissantes à l'ordre 0 pour R_p et B :

$$\exists\, \lambda_p \in \mathbb{K},\ \exists\, R_{p+1} \in \mathbb{K}[X] \ : \qquad R_p = \lambda_pB + XR_{p+1}$$

En remplaçant la valeur de R_p dans l'égalité au-dessus on obtient :

$$A = Q_pB + X^{p+1}(\lambda_pB + XR_{p+1}) \quad \text{et si} \quad Q_{p+1} = Q_p + \lambda_pX^{p+1} \quad \text{alors} \quad A = Q_{p+1}B + X^{p+2}R_{p+1} \quad \text{avec} \quad \deg Q_{p+1} \leqslant p$$

Ce qu'il fallait vérifier.

1.2 Fonctions polynomiales

On cherche à démontrer que tout polynôme qui admet une infinité de racines est le polynôme nul. On peut le démontrer par récurrence grâce au théorème de Rolle dans le cas où $\mathbb{K} = \mathbb{R}$ ou $\mathbb{Q}$. Dans le cas de $\mathbb{C}$, il n'y a plus de théorème de Rolle...

1.2.1 Fonctions polynomiales

DÉFINITION 0.8 **Fonctions polynomiales**
Soit $P = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$ un polynôme. On appelle *fonction polynomiale associée à P* la fonction donnée par :

$$\widetilde{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K}x \\ \longmapsto & a_0 + a_1 x + \dots + a_n x^n & \end{array} \right. .$$

Nous noterons $\mathscr{P}$ le sous-espace vectoriel de $\mathscr{F}(\mathbb{K}, \mathbb{K})$ des fonctions polynomiales.

Remarque 0.4 $\mathscr{P}$ est à la fois un sous-espace vectoriel et un sous-anneau de $\mathscr{F}(\mathbb{K}, \mathbb{K})$

PROPOSITION 0.10
L'application

$$\theta : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathscr{F}(\mathbb{K}, \mathbb{K})\, P \\ \longmapsto & \widetilde{P} & \end{array} \right.$$

est un morphisme de $\mathbb{K}$-espaces vectoriels et d'anneau. En particulier, si P, $Q \in \mathbb{K}[X]$ et si λ, $\mu \in \mathbb{K}$, on a :

$$\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q},$$

$$\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q},$$

$$\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}.$$

De plus $\operatorname{Im} \theta = \theta(\mathbb{K}[X]) = \mathscr{P}$.

Démonstration *Laissée en exercice.*

1.2.2 Racines d'un polynôme

DÉFINITION 0.9 **Racine d'un polynôme**
Soit $P \in \mathbb{K}[X]$ un polynôme. Soit $\alpha \in \mathbb{K}$. On dit que α est une *racine* de P si et seulement si $\widetilde{P}(\alpha) = 0$.

Théorème 0.11
Soient $P \in \mathbb{K}[X]$ un polynôme et $\alpha \in K$ un scalaire. On a équivalence entre :

1. α est une racine de P.
2. On peut factoriser P par $X-\alpha$, c'est-à-dire : $(X-\alpha)\,|P$.

Démonstration

- *Soit α une racine de P. Alors $\widetilde{P}(\alpha)=0$. Par division euclidienne, il existe $(Q,R)\in(\mathbb{K}[X])^2$ tels que : $\begin{cases} P=(X-\alpha)\,Q+R \deg(R)<\deg(X-\alpha)=1\end{cases}$. On a alors deux possibilités, soit $\deg R=0$, soit $\deg R=-\infty$, c'est-à-dire $R=0$. Montrons que la première n'est pas possible. Si on avait $\deg R=0$ alors il existerait $\gamma\in\mathbb{K}^*$ tel que $R=\gamma$ et on aurait $A=(X-\alpha)\,Q+\gamma$, mais alors $P=(X-\alpha)\,Q+\gamma$ et $0=\widetilde{P}(\alpha)=\widetilde{R}(\alpha)=\gamma\neq 0$ ce qui est une contradiction. On a donc bien $R=0$ et $P=(X-\alpha)\,Q$.*
- *Supposons que $(X-\alpha)\,|P$. Alors il existe $Q\in\mathbb{K}[X]$ tel que $P=(X-\alpha)\,Q$. Par conséquent, $P=(X-\alpha)\,Q$ et $\widetilde{P}(\alpha)=0$ ce qui prouve que α est une racine de P.*

Corollaire 0.12
Si $\alpha_1,\dots,\alpha_p$ sont p racines distinctes d'un polynôme $P\in\mathbb{K}[X]$ alors le polynôme

$$\boxed{(X-\alpha_1)\dots(X-\alpha_p)=\prod_{k=1}^{p}(X-\alpha_k)}$$

divise P.

Démonstration *La démonstration se fait par récurrence sur le nombre p de racines distinctes de P considérées.*

La propriété vient d'être prouvée au rang 1 dans le théorème précédent. Soit $p>1$. On suppose que la propriété est vraie au rang $p-1$. Prouvons-la au rang p. Soient $\alpha_1,\dots,\alpha_p$ p racines de P. Par application de l'hypothèse de récurrence, il existe $B\in\mathbb{K}[X]$ tel que $P=(X-\alpha_1)\dots(X-\alpha_{p-1})\,B$. Comme α_p est une racine de P, on a :

$$0=\widetilde{P}(\alpha)=(\alpha_p-\alpha_1)\dots(\alpha_p-\alpha_{p-1})\,\widetilde{B}(\alpha)\,.$$

Comme : $\forall i\in[\![1,p-1]\!],\quad \alpha_i\neq\alpha_p$, le nombre $(\alpha_p-\alpha_1)\dots(\alpha_p-\alpha_{p-1})$ est non nul et donc nécessairement $\widetilde{B}(\alpha)=0$, c'est-à-dire α_p est une racine de B. Appliquant le théorème précédent, il existe $C\in\mathbb{K}[X]$ tel que : $B=(X-\alpha_p)\,C$ et donc $P=(X-\alpha_1)\dots(X-\alpha_p)\,C$. On a alors prouvé que $(X-\alpha_1)\dots(X-\alpha_p)$ divise P. Le théorème est alors prouvé par application du principe de récurrence.

Théorème 0.13 **Un polynôme <u>non nul</u> de degré $\leqslant n$ admet au plus n racines**
Soit $P\in\mathbb{K}[X]$ un polynôme non nul de degré $\leqslant n$. Si P admet au moins $n+1$ racines distinctes alors P est nul.

Démonstration *Supposons qu'il existe $\alpha_1,\dots,\alpha_{n+1}$ $n+1$ racines distinctes du polynôme P non nul de degré $\geqslant n$. D'après le théorème précédent, le polynôme de degré $n+1$: $(X-\alpha_1)\dots(X-\alpha_{n+1})$ divise P. Il existe donc $B\in\mathbb{K}[X]$ tel que : $P=B\,(X-\alpha_1)\dots(X-\alpha_{n+1})$. On a alors $n=\deg P=\deg B+n+1$. Comme $\deg P\geqslant 0$, cette égalité n'est pas possible et donc notre hypothèse de départ est absurde.*

On en déduit :

Théorème 0.14
Tout polynôme qui admet une infinité de racines est le polynôme nul.

Théorème 0.15 **Identification polynômes et fonctions polynomiales**
L'application

$$\theta : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathscr{F}(\mathbb{K},\mathbb{K})\, P \\ \longmapsto & \widetilde{P} \end{cases}$$

qui envoie un polynôme sur sa fonction polynomiale associée est injective.

Démonstration *Soit P et Q deux polynômes vérifiant $\theta(P) = \theta(Q)$ soit $\widetilde{P-Q} = 0$. Le polynôme $P - Q$ possède donc une infinité de racines (tous les éléments de $\mathbb{K}$), ce qui n'est possible, d'après la proposition précédente, que si $P - Q = 0$.*

Ce théorème permet de confondre polynômes et applications polynomiales. Attention, ceci est vrai à condition que $\mathbb{K}$ contienne une infinité d'éléments, ce qui est bien notre cas car $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

On convient désormais de confondre les notations P et $\widetilde{P}$.

1.2.3 Schéma de Horner

C'est une façon de calculer les valeurs d'un polynôme en minimisant le nombre d'opérations, en particulier les multiplications. Soit $P = a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1} + a_nX^n$. On a $P = a_0 + X(a_1 + X(a_2 + X(a_3 + \ldots + X(a_{n-2} + X(a_{n-1} + a_nX))\ldots)))$. Donc pour calculer $P(\alpha)$ on initialise avec a_n ensuite on effectue une boucle : multiplier par α puis ajouter le coefficient a_k. Cet algorithme utilise n additions et n multiplications pour un polynôme de degré n.

On peut aussi obtenir le quotient de la division euclidienne de P par $X - \alpha$: $P = (X - \alpha)\,Q + P(\alpha)$ avec $Q = b_0 + b_1X + \ldots + b_{n-1}X^{n-1}$. En effet, on a

$$\begin{aligned} P(X) - P(\alpha) &= (X-\alpha)(b_{n-1}X^{n-1} + \ldots + b_1X + b_0), \\ a_nX^n + \ldots + a_1X + a_0 - P(\alpha) &= (X-\alpha)(b_{n-1}X^{n-1} + \ldots + b_1X + b_0), \\ a_nX^n + \ldots + a_1X + a_0 - P(\alpha) &= b_{n-1}X^n + (b_{n-2} - \alpha b_{n-1})X^{n-1} + \ldots + (b_0 - \alpha b_1)X - \alpha b_0. \end{aligned}$$

Par identification, on obtient le système (d'inconnues $b_0, b_1, ..., b_{n-1}, P(\alpha)$) :

$$\begin{cases} b_{n-1} & = & a_n \\ b_{n-2} - \alpha b_{n-1} & = & a_{n-1} \\ \ldots \\ b_0 - \alpha b_1 & = & a_1 \\ -\alpha b_0 & = & a_0 - P(\alpha) \end{cases}$$

soit

$$\begin{cases} b_{n-1} & = & a_n \\ b_{n-2} & = & a_{n-1} + \alpha b_{n-1} \\ \ldots \\ b_0 & = & a_1 + \alpha b_1 P(\alpha) \\ = & a_0 + \alpha b_0 \end{cases}$$

Autrement dit, les différents coefficients du polynôme quotient Q sont les nombres obtenus à chaque étape de la boucle.

1.2.4 Racines multiples

DÉFINITION 0.10 **Racine d'ordre p, racine multiple**
Soient $P \in \mathbb{K}[X]$ un polynôme, $\alpha \in \mathbb{K}$, $p \in \mathbb{N}^*$.

- On dit que α est une *racine d'ordre* p (ou de *multiplicité* p) de P si et seulement si $(X-\alpha)^p$ divise P et $(X-\alpha)^{p+1}$ ne divise pas P.
- Si α est une racine d'ordre 1 de P, on dit que α est une *racine simple* de P.
- Si α est une racine d'ordre $\geqslant 2$ de P, on dit que α est une *racine multiple* de P.

PROPOSITION 0.16 **Caractérisation de l'ordre d'une racine**
Soient $\alpha \in \mathbb{K}$ un scalaire et $P \in \mathbb{K}[X]$ un polynôme. On a équivalence entre :

1. α est une racine multiple de P d'ordre p.
2. Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^p Q$ et $Q(\alpha) \neq 0$.

Démonstration

- *Supposons que α est une racine multiple de P d'ordre p. Comme $(X-\alpha)^p$ divise P, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^p Q$. Si on avait $Q(\alpha) = 0$, alors α serait une racine de Q et il existerait $Q' \in \mathbb{K}[X]$ tel que $Q = (X-\alpha)Q'$. Par suite, on aurait $P = (X-\alpha)^{p+1} Q'$ et $(X-\alpha)^{p+1}$ diviserait P, ce qui n'est, par hypothèse, pas possible. Donc $Q(\alpha) \neq 0$.*
- *On suppose qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^p Q$ et $Q(\alpha) \neq 0$. Donc $(X-\alpha)^p$ divise P. Si c'est aussi le cas de $(X-\alpha)^{p+1}$, alors il existe $\widetilde{Q} \in \mathbb{K}[X]$ tel que $P = (X-\alpha)^{p+1}\widetilde{Q}$. Mais alors $Q = (X-\alpha)\widetilde{Q}$ et $Q(\alpha) = 0$, ce qui contredit notre hypothèse.*

1.3 Polynômes dérivés

1.3.1 Définitions et propriétés de base

DÉFINITION 0.11 **Polynôme dérivé**
Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ un polynôme. On définit le *polynôme dérivé* de P par :

$$P' = \quad a_1 + 2a_2 X + \cdots + n a_n X^{n-1} = \quad \sum_{k=1}^{n} k a_k X^{k-1}.$$

Remarque 0.5

- Cette définition est purement algébrique.
- Elle coïncide avec la dérivée des fonctions polynomiales sur le corps $\mathbb{K}$·

Proposition 0.17
Soit $P \in \mathbb{K}[X]$ un polynôme. On a :

1. Si $\deg(P) > 0$ alors $\deg(P') = \deg(P) - 1$.
2. P est constant si et seulement si $P' = 0$.

Démonstration

1. *Si $\deg(P) = p > 0$ alors $P = \sum_{k=0}^{p} a_k X^k$ avec $a_p \neq 0$ et $P' = \sum_{k=0}^{p-1} k a_k X^k$. Le coefficient de terme dominant de P' est pa_p qui est non nul. Par conséquent $\deg P' = p - 1$.*
2. *Si P est constant, il est clair que $P' = 0$. Réciproquement, si P n'est pas constant, alors $\deg P > 0$ et $\deg P' \geqslant 0$ ce qui prouve que P' est non nul.*

Proposition 0.18 **Linéarité de la dérivation**
Soient $P, Q \in \mathbb{K}[X]$ deux polynômes et $\alpha, \beta \in \mathbb{K}$ deux scalaires. On a :

$$\boxed{(\alpha P + \beta Q)' = \alpha P' + \beta Q'}.$$

On dit que l'opération de dérivation est linéaire.

Démonstration *Laissée en exercice.*

Proposition 0.19 **Dérivée d'un produit**
Soient $P, Q \in \mathbb{K}[X]$ deux polynômes. On a :

$$\boxed{(PQ)' = P'Q + PQ'}.$$

Démonstration *Supposons que $P = \sum_{k \in \mathbb{N}} a_k X^k$ et $Q = \sum_{k \in \mathbb{N}} b_k X^k$. On a donc $PQ = \sum_{i+j=0}^{+\infty} a_i b_j X^{i+j}$ et*

$$\begin{aligned}(PQ)' &= \sum_{i+j=0}^{+\infty} (i+j)\, a_i b_j X^{i+j-1} \text{ par linéarité de la dérivation} \\ &= \sum_{i+j=0}^{+\infty} i a_i b_j X^{i-1} X^j + \sum_{i+j=0}^{+\infty} j a_i b_j X^i X^{j-1} = P'Q + PQ'.\end{aligned}$$

1.3.2 Dérivées successives

Définition 0.12 **Polynôme dérivé d'ordre n**
Soit $P \in \mathbb{K}[X]$ un polynôme. On définit par récurrence la *dérivée n-ième* (ou *d'ordre n*) de P par :

— $P^{(0)} = P$
— $\forall n \in \mathbb{N}, \quad P^{(n+1)} = \left[P^{(n)}\right]'$

Remarque 0.6 Prenant un peu d'avance sur le chapitre **??**, on peut dire que l'application

$$D_n : \begin{cases} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]\,P \\ \longmapsto & P^{(n)} \end{cases}$$

est linéaire comme composée de n applications linéaires.

THÉORÈME 0.20 **Formule de Leibniz pour les polynômes**
Soient P, $Q \in \mathbb{K}[X]$ deux polynômes. On a :

$$\boxed{(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(n-k)} Q^{(k)}}.$$

Démonstration *C'est la même démonstration que celle écrite pour les fonctions n fois dérivables, voir page **??**, proposition **??**.*

Remarque 0.7 Il est important de bien comprendre le calcul suivant :

$$(X^p)^{(n)} = \begin{cases} 0 & \text{si } n > p \frac{p!}{(p-n)!} X^{p-n} = A_n^p X^{p-n} \\ \text{sinon} \end{cases}.$$

THÉORÈME 0.21 **Formule de Taylor pour les polynômes**
Soit P un polynôme de degré inférieur ou égal à n et $a \in \mathbb{K}$. Alors :

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

Démonstration *Soit $P = \sum_{p=0}^{n} a_p X^p = \sum_{p=0}^{n} a_p Q_p$.*

— *Soit $p \leqslant n$. La formule est vraie pour le polynôme $Q_p = X^p$. En effet, $Q_p' = pX^{p-1}, \dots, Q_p^{(k)} = p(p-1)\dots(p-k+1)X^{p-k}$.*

— *Maintenant, grâce à la formule du binôme de Newton :*

$$Q_p = X^p = ((X-a)+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} (X-a)^k = \sum_{k=0}^{p} \frac{(X-a)^k}{k!} \frac{p!}{(p-k)!} a^{p-k} = \sum_{k=0}^{p} \frac{(X-a)^k}{k!} Q_p^{(k)}(a).$$

— *En rajoutant des termes nuls, $Q_p = \sum_{k=0}^{n} \frac{(X-a)^k}{k!} Q_p^{(k)}(a)$.*

— *Enfin, par linéarité,*

$$\begin{aligned}
P &= \sum_{p=0}^{n} a_p Q_p \\
&= \sum_{p=0}^{n} a_p \sum_{k=0}^{n} \frac{(X-a)^k}{k!} Q_p^{(k)}(a) \\
&= \sum_{k=0}^{n} \frac{(X-a)^k}{k!} \sum_{p=0}^{n} a_p Q_p^{(k)}(a) \quad = \sum_{k=0}^{n} \frac{(X-a)^k}{k!} P^{(k)}(a).
\end{aligned}$$

LEMME 0.22
Soient $r \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$. Soit $a \in \mathbb{K}$. Si a est une racine d'ordre r de P alors a est une racine d'ordre $r-1$ de P'.

Démonstration *Comme a est une racine d'ordre r de P, il existe $Q \in \mathbb{K}[X]$ tel que : $P = (X-a)^r Q$ et $Q(a) \neq 0$. Par conséquent :*

$$P'(a) = r(X-a)^{r-1} Q + (X-a)^r Q' = (X-a)^{r-1} \underbrace{\left(rQ + (X-a) Q'\right)}_{=B}$$

et on a clairement $B(a) \neq 0$ ce qui prouve le lemme.

THÉORÈME 0.23 **Caractérisation des racines multiples**
Soient un polynôme $P \in \mathbb{K}[X]$, un scalaire $a \in \mathbb{K}$ et un entier $r > 0$. On a équivalence entre :

1. a est une racine d'ordre r de P.
2. $\boxed{P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0}$ et $\boxed{P^{(r)}(a) \neq 0}$.

Démonstration

— *Par application du lemme, si a est une racine d'ordre r de P alors a est une racine d'ordre 1 de $P^{(r-1)}$ et d'ordre 0 de $P^{(r)}$ donc $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$ et $P^{(r)}(a) \neq 0$.*

— *Réciproquement, si $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$ alors, par application de la formule de Taylor :*

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

avec $B \in \mathbb{K}[X]$ tel que $B(a) \neq 0$.

1.4 Polynômes scindés

1.4.1 Définition

Définition 0.13 **Polynôme scindé sur $\mathbb{K}$**
Soit $P \in \mathbb{K}[X]$ de degré p. On dit que P est *scindé* sur $\mathbb{K}$ si et seulement si il s'écrit :

$$P = a_p (X - \alpha_1) \dots (X - \alpha_p) = a_p \prod_{k=0}^{p} (X - \alpha_k)$$

où les scalaires $\alpha_k \in \mathbb{K}$ sont les racines de P comptées avec leur multiplicité et a_p est le coefficient du terme dominant de P.

1.4.2 Factorisation dans $\mathbb{C}[X]$

Jean le Rond D'Alembert, né à Paris le 16 novembre 1717 et mort à Paris le 29 octobre 1783*Mathématicien Français. Il fut avec Diderot à l'origine de l'Encyclopédie qui se voulait une synthèse et une vulgarisation des connaissances de l'époque. Tous deux durent jouer à cache-cache avec la censure pour faire paraître cette œuvre monumentale. D'Alembert abandonna le projet, fatigué des controverses et se consacra à la partie mathématique. Son œuvre fut considérable en mécanique, astronomie et mathématiques. Il énonce le théorème fondamental de l'algèbre dans son Traité de dynamique en 1743. Musicien, il établit l'équation des cordes vibrantes. Enfant trouvé sur les marches d'une église, il n'eut pas droit aux obsèques religieuses, car considéré comme athée.*

Théorème 0.24 **Théorème fondamental de l'algèbre**
Soit P un polynôme de $\mathbb{C}[X]$ de degré $\geqslant 1$ (c'est-à-dire non constant) alors P possède au moins une racine dans $\mathbb{C}$.

Démonstration *Il existe de nombreuses démonstrations. L'une d'entre elles est proposée dans l'exercice* **??** *page* **??**. *La première démonstration rigoureuse est due à Gauss (1799). Ce théorème est aussi appelé théorème de d'Alembert-Gauss.*

Remarque 0.8 Attention ce théorème est faux dans $\mathbb{R}$. Par exemple $P = X^2 + 1$ est non constant mais ne possède aucune racine dans $\mathbb{R}$.

COROLLAIRE 0.25 **Factorisation dans $\mathbb{C}[X]$**
Tout polynôme de $\mathbb{C}[X]$ est *scindé sur* $\mathbb{C}$, c'est-à-dire tout polynôme $P \in \mathbb{C}[X]$ s'écrit sous la forme :

$$\boxed{P = a_p.(X - \alpha_1)\dots(X - \alpha_p)}$$

où les scalaires α_k sont les racines de P comptées avec leur multiplicité et a_p est le coefficient du terme dominant de P.

Démonstration *Supposons que P est non constant, sinon la propriété est évidente. Soient $\alpha_1, \dots, \alpha_p \in \mathbb{C}$ la liste des racines de P. Par application du théorème fondamental de l'algèbre cette liste est non vide. Il existe $Q \in \mathbb{C}[X]$ tel que : $P = \prod_{i=1}^{p}(X - \alpha_i)\,Q$. Si Q est non constant alors il possède une racine α et α est nécessairement aussi une racine de P. Donc la liste $\alpha_1, \dots, \alpha_p$ n'était pas celle de toutes les racines de P, ce qui constitue une contradiction. Par conséquent, Q est un polynôme constant et la proposition est démontrée.*

Une formulation équivalente du théorème fondamental de l'algèbre est la suivante :

THÉORÈME 0.26
Un polynôme $P \in \mathbb{C}[X]$ de degré p possède p racines (comptées avec leur multiplicité) dans $\mathbb{C}$.

Démonstration *C'est un corollaire immédiat de la proposition précédente.*

Exemple 0.4 Soit $P = X^n - 1$. Pour tout $k \in [\![0, n-1]\!]$, $\zeta_k = \exp\left(\frac{2ik\pi}{n}\right)$ est une racine de P. Donc P est divisible par chacun des $X - \zeta_k$. Comme les ζ_k sont distincts deux à deux, P est aussi divisible par leur produit : $X^n - 1 = K \displaystyle\prod_{k=0}^{n-1}(X - \zeta_k)$. En regardant les degrés des deux membres, on a $\deg K = 0$ c'est-à-dire que K est constant. En regardant les coefficients dominants on en déduit que $K = 1$ et donc $\boxed{X^n - 1 = \displaystyle\prod_{k=0}^{n-1}(X - \zeta_k)}$.

1.4.3 Interlude : polynômes conjugués

DÉFINITION 0.14 **Polynômes conjugués**
Soit $P = a_0 + a_1X + \dots + a_pX^p \in \mathbb{C}[X]$ un polynôme. On appelle *conjugué* de P le polynôme, noté $\bar{P}$ et donné par :

$$\overline{P} = \overline{a_0} + \overline{a_1}X + \dots + \overline{a_p}X^p.$$

PROPOSITION 0.27
Soient P, $Q \in \mathbb{C}[X]$ et $r \in \mathbb{N}$. On a :

1. $\overline{P+Q} = \overline{P} + \overline{Q}$,
2. $\overline{P \times Q} = \overline{P} \times \overline{Q}$,
3. $\forall \alpha \in \mathbb{C}, \quad \overline{P(\alpha)} = \overline{P}(\overline{\alpha})$,
4. $\overline{P^{(r)}} = \overline{P}^{(r)}$,
5. $P \in \mathbb{R}[X] \Longleftrightarrow P = \overline{P}$.

Démonstration *Démontrons par exemple le troisième point : Soient $\alpha \in \mathbb{C}$ et $P = a_0 + a_1 X + \cdots + a_p X^p \in \mathbb{C}[X]$. On a :*

$$\overline{P(\alpha)} = \overline{a_0} + \overline{a_1 \alpha} + \cdots + \overline{a_p \alpha^p} \quad \text{et} \quad \overline{P}(\overline{\alpha}) = \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \cdots + \overline{a_p}\ \overline{\alpha}^p$$

d'où l'égalité.

Lemme 0.28
Soient $P \in \mathbb{C}[X]$ et $r \in \mathbb{N}^*$. Soit $\alpha \in \mathbb{C}$. On a équivalence entre :

1. α est une racine de P d'ordre r.
2. $\overline{\alpha}$ est une racine de $\overline{P}$ d'ordre r.

Démonstration *On a la série d'équivalences :*

$$\begin{aligned} & \alpha \text{ est une racine d'ordre } r \text{ de } P \\ \Leftrightarrow \quad & P(\alpha) = P'(\alpha) = \cdots = P^{(r-1)}(\alpha) = 0 \quad \text{et} \quad P^{(r)}(\alpha) \neq 0 \\ \Leftrightarrow \quad & \overline{P}(\overline{\alpha}) = \overline{P'}(\overline{\alpha}) = \cdots = \overline{P^{(r-1)}}(\overline{\alpha}) = 0 \quad \text{et} \quad \overline{P^{(r)}}(\overline{\alpha}) \neq 0 \Leftrightarrow \quad \overline{\alpha} \text{ est une racine d'ordre } r \text{ de } \overline{P}. \end{aligned}$$

Corollaire 0.29
Soit $P \in \mathbb{R}[X]$ un polynôme à *coefficients réels*. Si α est une racine d'ordre r de P alors $\overline{\alpha}$ est aussi une racine d'ordre r de P.

Démonstration *C'est un corollaire immédiat de la proposition précédente.*

Remarque 0.9 On en déduit que les racines de $P \in \mathbb{R}[X]$ sont ou réelles ou complexes conjuguées.

1.4.4 Factorisation dans $\mathbb{R}[X]$

Théorème 0.30 **Factorisation dans $\mathbb{R}[X]$**
Soit $P \in \mathbb{R}[X]$ un polynôme non nul. Alors, il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ non nécessairement deux à deux distincts, $(b_1, c_1), \ldots, (b_s, c_s) \in \mathbb{R}^2$ non nécessairement deux à deux distincts tels que $\Delta_l = b_l^2 - 4c_l < 0$ pour tout $\ell \in [\![1, s]\!]$, et $\lambda \in \mathbb{R}^*$ tels que :

$$\boxed{P = a \prod_{k=1}^{r} (X - \alpha_k) \prod_{\ell=1}^{s} \left(X^2 + b_\ell X + c_\ell\right)}.$$

Démonstration *D'après la proposition 0.25, P est scindé sur $\mathbb{C}$ et ses racines sont, d'après la dernière remarque, ou réelles ou complexes conjuguées :*

$$P = a\,(X-\alpha_1)\dots(X-\alpha_p)\,(X-\omega_1)\,(X-\overline{\omega_1})\dots(X-\omega_r)\,(X-\overline{\omega_r})$$

où $\alpha_1,\dots,\alpha_p \in \mathbb{R}$ sont les racines réelles de P et où $\omega_1,\overline{\omega_1},\dots,\omega_r,\overline{\omega_r}$ sont les racines complexes conjuguées de P. On a, pour tout $k \in [\![1,r]\!]$:

$$(X-\omega_k)\,(X-\overline{\omega_k}) = X^2 - (\omega_k+\overline{\omega_k}) + \omega_k\overline{\omega_k} = X^2 - 2\,\mathrm{Re}\,(\omega_k)\,X + |\omega_k|^2 = X^2 - p_kX + q_k$$

avec $p_k, q_k \in \mathbb{R}$. Le résultat annoncé s'en suit.

1.4.5 Polynômes irréductibles, partie 1

DÉFINITION 0.15 **Polynôme irréductible**
Soit $P \in \mathbb{K}[X]$ un polynôme $\boxed{\text{non constant}}$. On dit que P est *irréductible* si et seulement si :

$$P = QH \Rightarrow Q \in \mathbb{K} \quad \text{ou} \quad H \in \mathbb{K}.$$

Autrement dit, un polynôme P non constant est irréductible si et seulement si ses seuls diviseurs sont les polynômes constants et les polynômes proportionnels à P.

PROPOSITION 0.31 **Les polynômes de degré 1 sont irréductibles**
Soient $\alpha \in \mathbb{K}$ un scalaire et $P = (X-\alpha)$ un polynôme de degré 1. Alors P est irréductible.

Démonstration *Soit P un polynôme de degré 1. P est clairement non constant et si $Q \in \mathbb{K}[X]$ est un diviseurs de P alors il existe $H \in \mathbb{K}[X]$ tel que : $P = QH$. Par conséquent : $1 = \deg P = \deg Q + \deg H$. Une des deux possibilités suivantes est alors vraie :*

- *$\deg Q = 1$ et $\deg H = 0$ donc Q est un polynôme proportionnel à P*
- *$\deg Q = 0$ (et $\deg H = 1$) et Q est un polynôme constant.*

Par conséquent P est irréductible.

THÉORÈME 0.32 **Polynômes irréductibles de $\mathbb{C}[X]$**
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration *On vient de prouver que les polynômes de degré 1 sont irréductibles dans $\mathbb{C}[X]$. Réciproquement, si $P \in \mathbb{C}[X]$ est un polynôme irréductible de $\mathbb{C}[X]$, montrons qu'il est de degré 1. Si ce n'était pas le cas, alors comme P est non nul :*

- *soit $\deg P > 1$ et par application du théorème fondamental de l'algèbre, P possède au moins une racine α dans $\mathbb{C}$. Par conséquent le polynôme $X-\alpha$ divise P et donc P n'est pas irréductible.*
- *soit $\deg P = 0$ et dans ce cas P est un polynôme constant non nul et ne peut être irréductible.*

Dans les deux cas, on aboutit à une contradiction et la proposition est alors prouvée par l'absurde.

Théorème 0.33 — Polynômes irréductibles de $\mathbb{R}[X]$

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

- les polynômes de degré 1.
- les polynômes de degré 2 dont le discriminant est négatif.

Démonstration

- *Les polynômes de degré 1 sont irréductibles dans $\mathbb{R}[X]$.*
- *Soit $P \in \mathbb{R}[X]$ un polynôme de degré 2. Il est irréductible si et seulement si il n'est pas divisible par un polynôme de degré 1, c'est-à-dire si et seulement si il n'a pas de racine réelle, ce qui est équivalent à dire que son discriminant est strictement négatif.*
- *Tout polynôme de degré $\geqslant 3$ se décompose, d'après le théorème 0.30 de factorisation dans $\mathbb{R}[X]$, comme le produit de polynômes de degré 1 et de degré 2. Un tel polynôme ne peut être irréductible.*

1.4.6 Relations coefficients-racines

Définition 0.16 — Polynômes symétriques élémentaires

Soit $\alpha_1, \dots, \alpha_p \in \mathbb{K}$. On définit les *polynômes symétriques élémentaires* en les variables $\alpha_1, \dots, \alpha_p$ par :

$$\begin{aligned} \sigma_1 &= \alpha_1 + \cdots + \alpha_p, \\ \sigma_2 &= \sum_{i_1 < i_2} \alpha_{i_1}\alpha_{i_2}, \\ &\vdots \\ \sigma_p &= \alpha_1 \cdots \alpha_p. \end{aligned}$$

Plus précisément, pour tout $k \in [\![1, p]\!]$

$$\sigma_k = \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}.$$

Théorème 0.34 — Relations entre les coefficients et les racines d'un polynôme

Soit $P = a_0 + a_1 X + \cdots + a_p X^p \in \mathbb{K}[X]$ un polynôme scindé de degré p. Soient $\alpha_1, \dots, \alpha_p \in \mathbb{K}$ les p racines de p. On a :

$$\forall k \in [\![1, p]\!], \quad \boxed{\sigma_k = (-1)^k \frac{a_{p-k}}{a_p}}.$$

Démonstration *On démontre ces égalités en identifiant les coefficients des monômes de même degré dans l'égalité :*

$$P = a_p(X - \alpha_1)\dots(X - \alpha_p) = a_p\left(X^p - \sigma_1 X^{p-1} + \sigma_2 X^{p-2} + \cdots + (-1)^p \sigma_p\right)$$

Remarque 0.10

— En particulier, si $p = 2$, on a

$$P = a_2 (X - \alpha_2) (X - \alpha_1) = a_2 \left(X^2 - (\alpha_1 + \alpha_2) X + \alpha_1\alpha_2\right)$$

et donc

$$\sigma_1 = \alpha_1 + \alpha_2 = -\frac{a_1}{a_2} \quad \text{et} \quad \sigma_2 = \alpha_1\alpha_2 = \frac{a_0}{a_2}$$

— Si $p = 3$,

$$P = a_3 (X - \alpha_1) (X - \alpha_2) (X - \alpha_3) = a_3 \left(X^3 - (\alpha_1 + \alpha_2 + \alpha_3) X^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) X - \alpha_1\alpha_2\alpha_3\right)$$

et

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = -\frac{a_2}{a_3}, \quad \sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = \frac{a_1}{a_3} \quad \text{et} \quad \sigma_3 = \alpha_1\alpha_2\alpha_3 = -\frac{a_0}{a_3}.$$

On en tire les deux relations remarquables

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \sigma_1^2 - 2\sigma_2 \quad \text{et} \quad \frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} = \frac{\sigma_3}{\sigma_2}.$$

1.5 Arithmétique dans $\mathbb{K}[X]$

Nous allons définir le PGCD de deux polynômes, comme pour les entiers relatifs. Ici il y a une difficulté : que veut dire "plus grand" ? Cela veut dire avec le plus grand degré. Mais que se passe-t-il lorsqu'il y a deux polynômes de même degré en concurrence ? Cela ne se produit pas (ou alors ils sont associés) et c'est ce qu'il faut établir.

1.5.1 Diviseurs communs

PROPOSITION 0.35 **Propriétés de la divisibilité**

— La relation « divise » est transitive : $\forall (P, Q, R) \in \mathbb{K}[X]^3, \quad [P \mid Q \quad \text{et} \quad Q \mid R] \Rightarrow P \mid R.$

— Soit $P, Q, R \in \mathbb{K}[X]$ et $U, V \in \mathbb{K}[X]$. Alors : $[P \mid Q \quad \text{et} \quad P \mid R] \Rightarrow P \mid (UQ + VR).$

Démonstration *Elle se fait comme celle de la proposition* **??** *page* **??**.

✎ *Notation 0.5* On note pour la suite :

— $d(P)$ l'ensemble des diviseurs du polynôme P.

— $d(P, Q) = d(P) \cap d(Q)$ l'ensemble des diviseurs communs à P et à Q.

On remarque que si $D \in d(P, Q)$, alors tout polynôme associé à D est aussi dans $d(P, Q)$.

Proposition 0.36
Soit P un polynôme non nul. Alors $d(P, 0) = d(P)$.

Démonstration *Laissée en exercice.*

Proposition 0.37
Si $P = BQ + R$ alors $d(P, Q) = d(Q, R)$.

Démonstration *En effet, si $D \in d(P, Q)$, alors $D \mid Q$ et $D \mid P - BQ$ donc $D \mid Q$ et $D \mid R$ donc $D \in d(Q, R)$. On a montré que $d(P, Q) \subset d(Q, R)$. Inversement, si $D \in d(Q, R)$, alors $D \mid Q$ et $D \mid BQ + R$ donc $D \mid Q$ et $D \mid P$ donc $D \in d(P, Q)$. Il s'ensuit que $d(Q, R) \subset d(P, Q)$.*

Théorème 0.38
Soient $P, Q \in \mathbb{K}[X]$, non tous les deux nuls. Alors il existe un unique polynôme $D \in \mathbb{K}[X]$ unitaire tel que $d(P, Q) = d(D)$.

Démonstration
Unicité *Si D_1 et D_2 sont solutions alors $d(D_1) = d(D_2)$ donc $D_1 \mid D_2$ et $D_2 \mid D_1$ donc ils sont associés. Ils sont unitaires et associés donc égaux.*
Existence
Quitte à échanger P et Q on peut supposer $Q \neq 0$. Posons $P_0 = P$ et $P_1 = Q$. On réalise ensuite les divisions euclidiennes suivantes tant que les restes obtenus sont non nuls (c'est l'algorithme d'Euclide) :

$$\begin{array}{ccc} P_0 & = & P_1 B_1 + P_2 \quad \text{avec } \deg P_2 < \deg P_1, \\ \dots \\ P_{m-2} & = & P_{m-1} B_{m-1} + P_m \quad \text{avec } \deg P_m < \deg P_{m-1}, P_{m-1} \\ = & P_m B_m + 0. \end{array}$$

Ce processus s'arrête puisqu'on a une suite strictement décroissante d'entiers naturels $\deg P_1 > \deg P_2 > \dots$. On a alors $d(P, Q) = d(P_0, P_1) = \dots = d(P_m, 0) = d(P_m)$ Le polynôme D unitaire associé à P_m convient.

1.5.2 PGCD, théorèmes d'Euclide et de Bézout

Suivant les notations du précédent théorème, on considère le polynôme D unitaire tel que $d(P, Q) = d(D)$. Tout diviseur commun à P et à Q divise D. Donc son degré est inférieur ou égal à celui de D. Ces considérations justifient la définition suivante.

Définition 0.17 PGCD de deux polynômes
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. L'ensemble des diviseurs communs à P et Q admet un polynôme unitaire de plus grand degré noté $P \wedge Q$. C'est le *plus grand commun diviseur* des polynômes P et Q.

Remarque 0.11 L'algorithme d'Euclide fournit un moyen de calcul du PGCD : on normalise le dernier reste non nul.

PROPOSITION 0.39
$P \wedge Q = Q \wedge P$. Si un polynôme divise deux polynômes, alors il divise leur PGCD.

THÉORÈME 0.40 **Théorème de Bézout**
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. Il existe deux polynômes U et V tels que

$$PU + QV = P \wedge Q.$$

Avant d'en donner une preuve, étudions un exemple.

Exemple 0.6 $P = X^5 - 2X^3 - 2X^2 - 3X - 2,\ Q = X^5 - 3X^4 + 2X^3 - 3X^2 + X$. On descend avec l'algorithme d'Euclide :

dividende		quotient		diviseur		reste
$X^5 - 2X^3 - 2X^2 - 3X - 2$	$=$	1	$\times$	$(X^5 - 3X^4 + 2X^3 - 3X^2 + X)$	$+$	$(3X^4 - 4X^3 + X^2 - 4X$
$X^5 - 3X^4 + 2X^3 - 3X^2 + X$	$=$	$(\frac{1}{3}X - \frac{5}{9})$	$\times$	$(3X^4 - 4X^3 + X^2 - 4X - 2)$	$+$	$(-\frac{5}{9}X^3 - \frac{10}{9}X^2 - \frac{5}{9}X -$
$3X^4 - 4X^3 + X^2 - 4X - 2$	$=$	$(-\frac{27}{5}X + 18)$	$\times$	$(-\frac{5}{9}X^3 - \frac{10}{9}X^2 - \frac{5}{9}X - \frac{10}{9})$	$+$	$(18X^2 + 18)$
$-\frac{5}{9}X^3 - \frac{10}{9}X^2 - \frac{5}{9}X - \frac{10}{9}$	$=$	$(-\frac{5}{162}X - \frac{5}{81})$	$\times$	$(18X^2 + 18)$	$+$	0

Le dernier reste non nul est $18X^2 + 18$, qui normalisé, donne $X^2 + 1$ comme PGCD de P et Q.
Maintenant on remonte en partant de l'avant-dernière ligne :
$18X^2 + 18 = 3X^4 - 4X^3 + X^2 - 4X - 2 - (-\frac{27}{5}X + 18) \times (-\frac{5}{9}X^3 - \frac{10}{9}X^2 - \frac{5}{9}X - \frac{10}{9})$ d'où
$18X^2 + 18 = 3X^4 - 4X^3 + X^2 - 4X - 2 - (-\frac{27}{5}X + 18) \times \Big[X^5 - 3X^4 + 2X^3 - 3X^2 + X - (\frac{1}{3}X - \frac{5}{9}) \times (3X^4 - 4X^3 + X^2 - 4$
d'où
$18X^2 + 18 = (1 + (-\frac{27}{5}X + 18) \times (\frac{1}{3}X - \frac{5}{9})) \times (3X^4 - 4X^3 + X^2 - 4X - 2) - (-\frac{27}{5}X + 18) \times (X^5 - 3X^4 + 2X^3 - 3X^2 + X)$ soit
$18X^2 + 18 = (-\frac{9}{5}X^2 + 9X - 9) \times (3X^4 - 4X^3 + X^2 - 4X - 2) - (-\frac{27}{5}X + 18) \times (X^5 - 3X^4 + 2X^3 - 3X^2 + X)$
d'où
$18X^2 + 18 = (-\frac{9}{5}X^2 + 9X - 9) \times \big[(X^5 - 2X^3 - 2X^2 - 3X - 2) - (X^5 - 3X^4 + 2X^3 - 3X^2 + X)\big] - (-\frac{27}{5}X + 18) \times (X^5 - 3X^4 + 2X^3 - 3X^2 + X)$ soit
$18X^2 + 18 = (-\frac{9}{5}X^2 + 9X - 9) \times (X^5 - 2X^3 - 2X^2 - 3X - 2) + \Big[(-\frac{9}{5}X^2 + 9X - 9) - (-\frac{27}{5}X + 18)\Big] \times (X^5 - 3X^4 + 2X^3 - 3X^2 + X)$
$18X^2 + 18 = (-\frac{9}{5}X^2 + 9X - 9) \times (X^5 - 2X^3 - 2X^2 - 3X - 2) + (-\frac{9}{5}X^2 + \frac{82}{5}X - 27) \times (X^5 - 3X^4 + 2X^3 - 3X^2 + X)$

En divisant par 18 :
$(-\frac{1}{10}X^2 + \frac{1}{2}X - \frac{1}{2})(X^5 - 2X^3 - 2X^2 - 3X - 2) + (\frac{1}{10}X^2 - \frac{1}{5}X - \frac{1}{2})(X^5 - 3X^4 + 2X^3 - 3X^2 + X) = X^2 + 1$.

Démonstration *L'exemple montre comment conduire la démonstration. On effectue une récurrence sur* $n = \min(\deg P, \deg Q)$.

Si $n = -\infty$ *ou* $n = 0$ *la propriété est claire.*

Pour fixer les idées, on suppose que $\deg P \geqslant \deg Q = n + 1$. *On écrit la division euclidienne de* P *par* Q. *Il existe des polynômes* B *et* R *tels que* $P = BQ + R$ *avec* $\deg R \leqslant n$. *En utilisant la propriété de récurrence, on sait qu'il existe aussi deux polynômes* U_1 *et* V_1 *de* $\mathbb{K}[X]$ *tels que* $\Delta = U_1 Q + V_1 R$ *avec* $\Delta = Q \wedge R$. *Or* $\Delta = P \wedge Q$ *d'une part, et d'autre part* $\Delta = U_1 Q + V_1(P - BQ) = V_1 P + (U_1 - BV_1)Q$. *D'où le résultat en prenant* $U = V_1$ *et* $V = U_1 - BV_1$.

Remarque 0.12 Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. S'il existe trois polynômes U, V et D vérifiant $PU + QV = D$, alors D est un multiple de $\Delta = P \wedge Q$.
En effet on écrit $P = P_1 \Delta$ et $Q = Q_1 \Delta$. On obtient alors $D = (P_1 U + Q_1 V)\Delta$ donc $\Delta \mid D$.

PROPOSITION 0.41
Soient $A, B, C \in \mathbb{K}[X]$. Si C est unitaire alors $AC \wedge BC = C(A \wedge B)$.

Démonstration *Posons* $\Delta = AC \wedge BC$ *et* $D = A \wedge B$. *On a* $DC \mid AC$ *et* $DC \mid BC$ *donc* $DC \mid \Delta$. *Réciproquement* $D = AU + BV$ *donc* $DC = ACU + BCV$ *d'où* $\Delta \mid DC$.

1.5.3 Polynômes premiers entre eux

DÉFINITION 0.18 **Polynômes premiers entre eux**
On dit que deux polynômes de $\mathbb{K}[X]$ sont *premiers entre eux* si leur PGCD est égal à 1.

PROPOSITION 0.42 **Caractérisation des polynômes premiers entre eux**
Soient P et Q deux polynômes de $\mathbb{K}[X]$.
Deux polynômes P et Q de $\mathbb{K}[X]$ sont premiers entre eux si et seulement s'il existe deux polynômes U et V de $\mathbb{K}[X]$ tels que
$$PU + QV = 1.$$

Démonstration *Dans un sens c'est le théorème de Bézout. Dans l'autre, comme* $PU + QV = 1$, *on en déduit que* $P \wedge Q$ *divise* 1. *Il n'y a qu'un seul polynôme unitaire qui divise* 1, *c'est* 1 *lui-même.*

PROPOSITION 0.43 **Lemme de Gauss**
Si P, Q et R sont trois polynômes vérifiant $\left\{ \quad 1 \quad P \mid QR \quad 2 \quad P \wedge Q = 1 \right.$ alors $P \mid R$.

Démonstration *La condition* $P \wedge Q = 1$ *permet d'écrire une relation de Bézout :* $PU + QV = 1$ *qui multipliée par* R *donne* $PUR + QRV = R$. *Maintenant la condition* $P \mid QR$ *assure l'existence d'un polynôme* A *tel que* $AP = QR$ *et donc* $PUR + APV = P(UR + AV) = R$ *et donc* P *divise* R.

PROPOSITION 0.44
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$. Alors $\dfrac{P}{D}$ et $\dfrac{Q}{D}$ sont des polynômes et ils sont premiers entre eux.

Démonstration *On écrit* $P = P_1 D$ *et* $Q = Q_1 D$. *On a* $\dfrac{P}{D} = P_1$ *et* $\dfrac{Q}{D} = Q_1$. *De plus, d'après la proposition 0.41,*

$$D = P \wedge Q = P_1 D \wedge Q_1 D = D(P_1 \wedge Q_1)$$

puisque D *est unitaire. Le résultat découle alors de l'intégrité de* $\mathbb{K}[X]$.

PROPOSITION 0.45 **Polynôme premier avec un produit**
Si un polynôme P est premier avec Q_1 et avec Q_2 alors il est premier avec Q_1Q_2.

Démonstration *On écrit une relation de Bézout pour* (P, Q_1) : $PU_1 + Q_1V_1 = 1$ *puis une autre pour* (P, Q_2) : $PU_2 + Q_2V_2 = 1$. *On effectue le produit de ces deux égalités :* $P^2U_1U_2 + PU_1Q_2V_2 + PU_2Q_1V_1 + Q_1Q_2U_1U_2 = 1$ *soit* $P(PU_1U_2 + U_1Q_2V_2 + U_2Q_1V_1) + Q_1Q_2(U_1U_2) = 1$, *ce qui donne le résultat.*
Autre démonstration : Soit D *un diviseur commun à* P *et à* Q_1Q_2. D *est premier avec* Q_1, *En effet, soit* d *diviseur commun à* Q_1 *et* D. *Comme* $d \mid D$ *et* $D \mid P$, *on a* $d \mid P$ *et donc* d *diviseur commun à* P *et* Q *donc* $\deg d = 0$. *Maintenant d'après le lemme de Gauss,* $D \mid Q_1Q_2$ *et* $D \wedge Q_1 = 1$ *donc* $D \mid Q_2$, *donc* $D \mid P \wedge Q_2$, *ce qu'il fallait démontrer.*

PROPOSITION 0.46
Si un polynôme P est premier avec $Q_1, Q_2, \dots, Q_m$ alors il est premier avec leur produit.

Démonstration *Par une récurrence sans malice.*

COROLLAIRE 0.47
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et premiers entre eux. Alors

1. Pour tout entier m, P est premier avec Q^m.
2. Pour tous entiers m et n, P^n est premier avec Q^m.

1.5.4 PPCM

PROPOSITION 0.48
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$. Alors $\dfrac{PQ}{D}$ est un polynôme, multiple commun à P et à Q.

Démonstration *On écrit* $P = P_1D$ *et* $Q = Q_1D$. *On a* $\dfrac{PQ}{D} = P_1Q = PQ_1$ *ce qui établit le résultat.*

PROPOSITION 0.49
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls et soit $D = P \wedge Q$.
Tout multiple commun à P et à Q est multiple de $\dfrac{PQ}{D}$.

Démonstration *Soit M un multiple commun à P et à Q. On écrit $M = AP = AP_1D = BQ = BQ_1D$. Après simplification par D on a $AP_1 = BQ_1$ avec P_1 et Q_1 premiers entre eux. Maintenant P_1 divise BQ_1 et $P_1 \wedge Q_1$. Donc d'après le lemme de Gauss, $P_1 \mid B$. Autrement dit, on peut écrire $B = B_1P_1$. Donc $M = BQ_1D = B_1P_1Q_1D = B_1\dfrac{PQ}{D}$. Ce qu'il fallait démontrer.*

Cette propriété permet d'énoncer la

DÉFINITION 0.19 **PPCM**
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls.
L'ensemble des polynômes de $\mathbb{K}[X]$ multiples communs de P et Q admet un polynôme unitaire de plus petit degré μ noté : $\mu = P \vee Q$. C'est le *plus petit commun multiple* des polynômes P et Q.

ainsi que la

PROPOSITION 0.50
Soient P et Q deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls.

$$(P \wedge Q) \times (P \vee Q) \text{ est associé à } PQ.$$

ce qui fournit un procédé de calcul au PPCM de deux polynômes.

1.5.5 Polynômes irréductibles, partie 2

Où l'on revient vers les polynômes irréductibles. Nous avions vu quels étaient les polynômes irréductibles de $\mathbb{C}[X]$ ou ceux de $\mathbb{R}[X]$. Le théorème fondamental de l'algèbre permet de décomposer tout polynôme de $\mathbb{C}[X]$ ou $\mathbb{R}[X]$ en produit de facteurs irréductibles. Mais qu'en est-il des polynômes irréductibles de $\mathbb{Q}[X]$? Nous ne répondrons pas à cette (difficile) question, mais nous allons établir un résultat à la fois plus général et plus élémentaire (il se passe du théorème fondamental de l'algèbre que nous avons dû admettre). C'est le pendant pour les polynômes de la décomposition en facteurs premiers.

PROPOSITION 0.51
Soient P et Q deux polynômes irréductibles de $\mathbb{K}[X]$. P et Q sont soit associés, soit premiers entre eux.

Démonstration *Soit $D = P \wedge Q$. Comme $D \mid P$ et que P est irréductible, alors $D = 1$ ou D est associé à P. Dans le deuxième cas, comme $D \mid Q$ et que Q est irréductible, alors $D = 1$ (impossible) ou D est associé à Q. Donc P est associé à Q.*

THÉORÈME 0.52 **Décomposition en produit de facteurs irréductibles.**
Soit P un polynômes de $\mathbb{K}[X]$ non nul.
Il existe $\alpha \in \mathbb{K}^*$, il existe $m \in \mathbb{N}$, $v_1, \dots, v_m \in \mathbb{N}^*$, m polynômes $P_1, \dots, P_m$ unitaires, irréductibles et deux à deux distincts tels que

$$P = \alpha \prod_{k=1}^{m} P_k^{v_k}.$$

De plus, les α, m, v_k sont uniques et les P_k sont uniques à l'ordre près.

Démonstration

— $\boxed{\text{Unicité :}}$ *Le résultat est évident si P est constant. On suppose donc que P n'est pas constant et qu'il s'écrit*

$$P = \alpha \prod_{k=1}^{m} P_k^{v_k} = \beta \prod_{\ell=1}^{n} Q_\ell^{w_\ell}$$

où les P_k et les Q_ℓ sont des facteurs irréductibles, unitaires, deux à deux distincts et où $v_1, \ldots, v_m, w_1, \ldots, w_n \in \mathbb{N}^*$.

Déjà, α est égal au coefficient dominant de P, ainsi que β, donc $\alpha = \beta$. Nous allons établir que $m = n$ et que la liste des P_k égale celle des Q_ℓ .

Remarquons que pour tout $\ell \in [\![1, n]\!]$, comme Q_ℓ est irréductible et divise P, il divise un des P_k. Mais d'après la proposition précédente, comme les P_k sont irréductibles, Q_ℓ est associé à un des P_k et les polynômes considérés étant tous unitaires, il est égal à un des P_k.

La liste des P_k est donc égale à celle des Q_ℓ et on peut écrire

$$P = \alpha \prod_{k=1}^{m} P_k^{v_k} = \alpha \prod_{\ell=1}^{m} P_\ell^{w_\ell}.$$

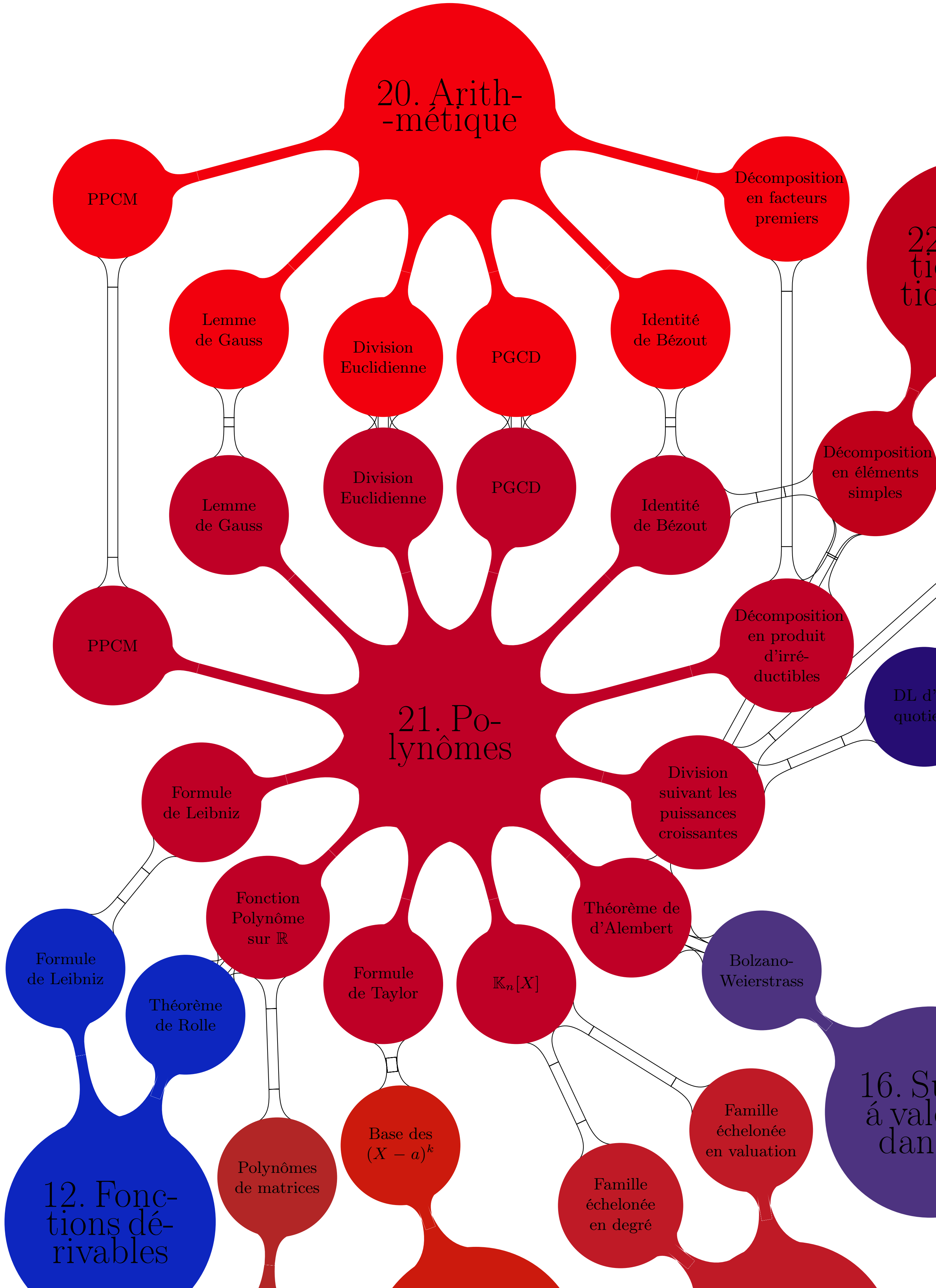
Il reste à montrer que pour tout $k \in [\![1, m]\!]$, $v_k = w_k$. Si tel n'était pas le cas, alors il existerait $k_0 \in [\![1, m]\!]$ tel que, par exemple, $v_{k_0} < w_{k_0}$. Alors on aurait

$$\prod_{k \in [\![1,m]\!], k \neq k_0} P_k^{v_k} = P_{k_0}^{w_{k_0} - v_{k_0}} \prod_{\ell \in [\![1,m]\!], \ell \neq k_0}^{m} P_\ell^{w_\ell}$$

et P_{k_0} diviserait P_{k_1} pour un certain $k_1 \in [\![1, m]\!]$, $k_1 \neq k_0$. Mais P_{k_0} et P_{k_1} étant irréductibles et unitaires, ceci amènerait que $P_{k_0} = P_{k_1}$ et contredirait le fait que les P_i sont deux à deux distincts. L'unicité de la décomposition est ainsi prouvée.

— $\boxed{\text{Existence :}}$ *Elle se démontre par récurrence sur le degré. Tout polynôme non nul de degré $\leqslant 1$ est soit constant, soit irréductible. On considère donc un polynôme non nul. Soit il est irréductible et il n'y a rien à faire, soit il peut s'écrire comme produit de deux polynômes de degré strictement inférieur et alors on applique la propriété de récurrence à chacun de ces deux polynômes.*

Le chapitre fut copieux. Pour s'en convaincre, il convient de jeter un coup d'œ il au diagramme :


20. Arith-
-métique
PPCM
Décomposition en facteurs premiers
Lemme de Gauss
Division Euclidienne
PGCD
Identité de Bézout
Lemme de Gauss
Division Euclidienne
PGCD
Identité de Bézout
Décomposition en éléments simples
PPCM
Décomposition en produit d'irré-ductibles
21. Po-
lynômes
Formule de Leibniz
Division suivant les puissances croissantes
Fonction Polynôme sur $\mathbb{R}$
Théorème de d'Alembert
Formule de Leibniz
Théorème de Rolle
Formule de Taylor
$\mathbb{K}_n[X]$
Bolzano-Weierstrass
Famille échelonée en valuation
Base des $(X-a)^k$
Polynômes de matrices
Famille échelonée en degré
12. Fonc-
tions dé-
rivables

Références