Chapitre n°16
Polynômes

Notation C16.1 — Dans ce chapitre, $\mathbf{K}$ désigne un corps.

§ 1. Construction de l'algèbre $\mathbf{K}[X]$

Notation C16.2 — On note $\mathbf{K}^{(\mathbf{N})}$ l'ensemble des suites presque nulles d'éléments de $\mathbf{K}$, qui sont indexées par $\mathbf{N}$, i.e.

$$\mathbf{K}^{(\mathbf{N})} := \left\{(a_n)_{n\in\mathbf{N}} \in \mathbf{K}^{\mathbf{N}} \ : \ \exists\, n_0 \in \mathbf{N},\ \forall\, n \geqslant n_0,\ a_n = 0_{\mathbf{K}}\right\}.$$

Proposition-Définition C16.3 (addition sur $\mathbf{K}^{(\mathbf{N})}$)
Si $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ sont deux éléments de $\mathbf{K}^{(\mathbf{N})}$, alors la suite $(a_n+b_n)_{n\in\mathbf{N}}$ est presque nulle et on pose

$$(a_n)_{n\in\mathbf{N}} + (b_n)_{n\in\mathbf{N}} := (a_n +_{\mathbf{K}} b_n)_{n\in\mathbf{N}}$$

On définit ainsi une application :

$$+ \ \left|\ \begin{array}{ccc} \mathbf{K}^{(\mathbf{N})} \times \mathbf{K}^{(\mathbf{N})} & \longrightarrow & \mathbf{K}^{(\mathbf{N})} \\ \left((a_n)_{n\in\mathbf{N}}\ ,\ (b_n)_{n\in\mathbf{N}}\right) & \longmapsto & (a_n +_{\mathbf{K}} b_n)_{n\in\mathbf{N}}\ . \end{array}\right.$$

Proposition C16.4 (structure de $\left(\mathbf{K}^{(\mathbf{N})},+\right)$)
Le magma $\left(\mathbf{K}^{(\mathbf{N})},+\right)$ est un groupe abélien, dont l'élément neutre est la suite nulle. L'opposé d'un élément $(a_n)_{n\in\mathbf{N}}$ de $\mathbf{K}^{(\mathbf{N})}$ est

$$-(a_n)_{n\in\mathbf{N}} := (-a_n)_{n\in\mathbf{N}}$$

Proposition-Définition C16.5 (multiplication par un scalaire sur $\mathbf{K}^{(\mathbf{N})}$)
Si $(a_n)_{n\in\mathbf{N}}$ est un élément de $\mathbf{K}^{(\mathbf{N})}$ et $\lambda \in \mathbf{K}$, alors la suite $(\lambda \times_{\mathbf{K}} a_n)_{n\in\mathbf{N}}$ est presque nulle et on pose

$$\lambda \cdot (a_n)_{n\in\mathbf{N}} := (\lambda \times_{\mathbf{K}} a_n)_{n\in\mathbf{N}}$$

On définit ainsi une application

$$\cdot \ \left|\ \begin{array}{ccc} \mathbf{K} \times \mathbf{K}^{(\mathbf{N})} & \longrightarrow & \mathbf{K}^{(\mathbf{N})} \\ \left(\lambda\ ,\ (a_n)_{n\in\mathbf{N}}\right) & \longmapsto & (\lambda \times_{\mathbf{K}} a_n)_{n\in\mathbf{N}} \end{array}\right.$$

Proposition C16.6 (structure de $\left(\mathbf{K}^{(\mathbf{N})},+,\cdot\right)$)
Le magma $\left(\mathbf{K}^{(\mathbf{N})},+\right)$ est un groupe abélien et, pour tout $(a_n)_{n\in\mathbf{N}} \in \mathbf{K}^{(\mathbf{N})}$, $(b_n)_{n\in\mathbf{N}} \in \mathbf{K}^{(\mathbf{N})}$, $\lambda \in \mathbf{K}$ et $\mu \in \mathbf{K}$

1) $\lambda \cdot \left((a_n)_{n\in\mathbf{N}} + (b_n)_{n\in\mathbf{N}}\right) = \lambda \cdot (a_n)_{n\in\mathbf{N}} + \lambda \cdot (b_n)_{n\in\mathbf{N}}$
2) $(\lambda+\mu)\cdot (a_n)_{n\in\mathbf{N}} = \lambda \cdot (a_n)_{n\in\mathbf{N}} + \mu \cdot (a_n)_{n\in\mathbf{N}}$
3) $\left(\lambda \times_{\mathbf{K}} \mu\right) \cdot (a_n)_{n\in\mathbf{N}} = \lambda \cdot \left(\mu \cdot (a_n)_{n\in\mathbf{N}}\right)$
4) $1_{\mathbf{K}} \cdot (a_n)_{n\in\mathbf{N}} = (a_n)_{n\in\mathbf{N}}$

Proposition-Définition C16.7 (multiplication interne $\times$ sur $\mathbf{K}^{(\mathbf{N})}$)

Si $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ sont deux éléments de $\mathbf{K}^{(\mathbf{N})}$, alors la suite $\left(\sum_{k=0}^{n} a_k \times_{\mathbf{K}} b_{n-k}\right)_{n\in\mathbf{N}}$ est presque nulle et on pose

$$(a_n)_{n\in\mathbf{N}} \times (b_n)_{n\in\mathbf{N}} := \left(\sum_{k=0}^{n} a_k \times_{\mathbf{K}} b_{n-k}\right)_{n\in\mathbf{N}}$$

On définit ainsi une application

$$\times \left| \begin{array}{ccc} \mathbf{K}^{(\mathbf{N})} \times \mathbf{K}^{(\mathbf{N})} & \longrightarrow & \mathbf{K}^{(\mathbf{N})} \\ \left((a_n)_{n\in\mathbf{N}}\, ,\, (b_n)_{n\in\mathbf{N}}\right) & \longmapsto & \left(\sum_{k=0}^{n} a_k \times_{\mathbf{K}} b_{n-k}\right)_{n\in\mathbf{N}} \end{array} \right. .$$

Proposition C16.8 (structure de $\left(\mathbf{K}^{(\mathbf{N})}, +, \cdot, \times\right)$)

On vérifie alors que $\left(\mathbf{K}^{(\mathbf{N})}, +, \times\right)$ est un anneau commutatif, dont le neutre pour la multiplication est la suite

$$\left(\delta_{0,n}\right)_{n\in\mathbf{N}} = (1, 0, \dots, 0, \dots) \ .$$

De plus, pour tout $(a_n)_{n\in\mathbf{N}} \in \mathbf{K}^{(\mathbf{N})}$, $(b_n)_{n\in\mathbf{N}} \in \mathbf{K}^{(\mathbf{N})}$, $\lambda \in \mathbf{K}$

$$\left(\lambda \cdot (a_n)_{n\in\mathbf{N}}\right) \times (b_n)_{n\in\mathbf{N}} = (a_n)_{n\in\mathbf{N}} \times \left(\lambda \cdot (b_n)_{n\in\mathbf{N}}\right) = \lambda \cdot \left((a_n)_{n\in\mathbf{N}} \times (b_n)_{n\in\mathbf{N}}\right)$$

Proposition-Définition C16.9 (l'élément X de $\mathbf{K}^{(N)}$ et ses puissances)

Soit X la suite d'éléments de $\mathbf{K}$, dont tous les termes sont nuls, à l'exception de celui d'indice 1, qui vaut 1, i.e. :

$$X := \left(\delta_{1,n}\right)_{n\in\mathbf{N}} = (0, 1, 0, \dots, 0, \dots) \ .$$

La suite X est presque nulle et ses puissances sont données pas

$$\forall k \in \mathbf{N}, \qquad X^k = \left(\delta_{k,n}\right)_{n\in\mathbf{N}} = \left(0, \dots, 0, \underbrace{1}_{\text{indice } k}, 0, \dots, 0, \dots\right)$$

en d'autres termes, pour tout $k \in \mathbf{N}$, X^k est la suite d'éléments de $\mathbf{K}$ indexée par $\mathbf{N}$, dont tous les termes sont nuls, à l'exception de celui d'indice k qui vaut 1.

Proposition C16.10 (écriture canonique d'un élément de $\mathbf{K}^{(\mathbf{N})}$)

Si $(a_n)_{n\in\mathbf{N}}$ est un élément de $\mathbf{K}^{(\mathbf{N})}$, alors

$$(a_n)_{n\in\mathbf{N}} = \sum_{n=0}^{+\infty} a_n \cdot X^n \qquad \left[\text{somme finie puisque les coefficients } a_n \text{ sont nuls à partir d'un certain rang}\right] .$$

Exemple C16.11 — L'élément $(13, 0, 25, 18, 0, -61, 0, \dots, 0, \dots)$ de $\mathbf{K}^{(\mathbf{N})}$ s'écrit $13 + 25X^2 + 18X^3 - 61X^5$.

Définition C16.12 (polynôme et ensemble $\mathbf{K}[X]$)

1) L'ensemble $\mathbf{K}^{(\mathbf{N})}$ sera plutôt noté $\mathbf{K}[X]$.
2) Un polynôme à coefficient dans $\mathbf{K}$ est un élément de $\mathbf{K}[X]$, i.e. une suite presque nulle d'éléments de $\mathbf{K}$.

PROPOSITION C16.13 (ÉCRITURE CANONIQUE D'UN POLYNÔME)

1) Tout polynôme $P \in \mathbf{K}[X]$ s'écrit de manière unique sous la forme

$$P = \sum_{k=0}^{+\infty} a_k \cdot X^k \qquad \left[\text{somme finie puisque les coefficients } a_k \text{ sont nuls à partir d'un certain rang}\right].$$

où $(a_k)_{k\in\mathbf{N}}$ est un élément de $\mathbf{K}^{(\mathbf{N})}$.

2) Si $P = (a_k)_{k\in\mathbf{N}}$ est un élément non nul de $\mathbf{K}[X]$ et si $n := \max\{k \in \mathbf{N} \,:\, a_k \neq 0_{\mathbf{K}}\}$ alors

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

Dans toute la suite, nous écrirons les polynômes sous l'une des formes 1) ou 2) introduite en C16.13, plus jamais comme des suites presque nulles d'éléments de $\mathbf{K}$.

DÉFINITION C16.14 (COEFFICIENTS D'UN POLYNÔME)

Soit $P \in \mathbf{K}[X]$ d'écriture canonique

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

où $(a_k)_{k\in\mathbf{N}}$ est une suite presque nulle d'éléments de $\mathbf{K}$. Pour tout $k \in \mathbf{N}$, on appelle coefficient de P de degré k le scalaire noté $[P]_k$ défini par

$$[P]_k := a_k.$$

§ 2. SYNTHÈSE DES OPÉRATIONS DÉFINIES SUR $\mathbf{K}[X]$

1) Addition de deux polynômes

$$\forall (P,Q) \in \mathbf{K}[X]^2 \quad P+Q := \sum_{k=0}^{+\infty} \left([P]_k +_{\mathbf{K}} [Q]_k\right) X^k$$

donc

$$\forall k \in \mathbf{N} \quad [P+Q]_k = [P]_k +_{\mathbf{K}} [Q]_k.$$

2) Multiplication d'un polynôme par un scalaire

$$\forall (\lambda, P) \in \mathbf{K} \times \mathbf{K}[X] \quad \lambda \cdot P = \sum_{k=0}^{+\infty} \lambda [P]_k X^k$$

donc

$$\forall k \in \mathbf{N} \quad [\lambda \cdot P]_k = \lambda \times_{\mathbf{K}} [P]_k.$$

3) Multiplication de deux polynômes

$$\forall (P,Q) \in \mathbf{K}[X]^2 \quad P \times Q := \sum_{k=0}^{+\infty} \left(\sum_{i=0}^{k} [P]_i \times_{\mathbf{K}} [Q]_{k-i} \right) X^k$$

donc

$$\forall k \in \mathbf{N} \quad [P \times Q]_k = \sum_{i=0}^{k} [P]_i \times_{\mathbf{K}} [Q]_{k-i}.$$

4) Composition de deux polynômes

$$\forall\,(P,Q)\in\mathbf{K}[X]^2 \quad P\circ Q := \sum_{i=0}^{n} [P]_i \times Q^i\,.$$

Exemple C16.15 — Soient les deux polynômes $P = X^3 - 2X^2 + 1$ et $Q = X^2 - X + 3$ à coefficients dans $\mathbf{K}$. Alors

$$P\circ Q = \left(X^2 - X + 3\right)^3 - 2\left(X^2 - X + 3\right)^2 + 1 = X^6 - 3X^5 + 10X^4 - 15X^3 + 22X^2 - 15X + 10\,.$$

§ 3. Synthèse sur la structure de $(\mathbf{K}[X],+,\cdot,\times)$

1) $(\mathbf{K}[X],+)$ est un groupe abélien dont l'élément neutre est le polynôme noté $0_{\mathbf{K}[X]}$ dont tous les coefficients sont nuls et

$$\forall\,P\in\mathbf{K}[X] \quad -P = \sum_{k=0}^{+\infty} -[P]_k X^k\,.$$

2) $\forall\,(P,Q,\lambda)\in\mathbf{K}[X]\times\mathbf{K}[X]\times\mathbf{K} \quad \lambda\cdot(P+Q) = \lambda\cdot P + \lambda\cdot Q$

3) $\forall\,(P,\lambda,\mu)\in\mathbf{K}[X]\times\mathbf{K}\times\mathbf{K} \quad (\lambda+\mu)\cdot P = \lambda\cdot P + \mu\cdot P$

4) $\forall\,(P,\lambda,\mu)\in\mathbf{K}[X]\times\mathbf{K}\times\mathbf{K} \quad \left(\lambda\times_{\mathbf{K}}\mu\right)\cdot P = \lambda\cdot\left(\mu\cdot P\right)$

5) $\forall\,P\in\mathbf{K}[X] \quad 1_{\mathbf{K}}\cdot P = P$

6) $(\mathbf{K}[X],+,\times)$ est un anneau commutatif dont le neutre pour la multiplication est le polynôme noté $1_{\mathbf{K}[X]}$ dont tous les coefficients sont nuls, à l'exception de celui de degré 0 qui vaut 1.

7) $\forall\,(P,Q,\lambda)\in\mathbf{K}[X]\times\mathbf{K}[X]\times\mathbf{K} \quad (\lambda\cdot P)\times Q = P\times(\lambda\cdot Q) = \lambda\cdot(P\times Q)$

Théorème C16.16 (Formule du binôme de Newton dans $\mathbf{K}[X]$)
Pour tout $(n,P,Q)\in\mathbf{N}\times\mathbf{K}[X]\times\mathbf{K}[X]$

$$(P+Q)^n = \sum_{k=0}^{n}\binom{n}{k}P^kQ^{n-k} = \sum_{k=0}^{n}\binom{n}{k}Q^kP^{n-k}\,.$$

Théorème C16.17 (Factorisation d'une différence de deux puissances n-ièmes, où $n\in\mathbf{N}^*$)
Pour tout $(n,P,Q)\in\mathbf{N}^*\times\mathbf{K}[X]\times\mathbf{K}[X]$

$$P^n - Q^n = (P-Q)\sum_{k=0}^{n-1}P^kQ^{n-1-k}\,.$$

Exercice C16.18 — 1) Démontrer, pour tout $(P,Q,R)\in\mathbf{K}[X]^3$, $P(QR) = (PQ)R$.
2) Démontrer, pour tout $(P,Q)\in\mathbf{K}[X]^2$, $PQ = QP$.
3) A-t-on, $(P,Q)\in\mathbf{K}[X]^2$, $P\circ Q = Q\circ P$ pour tout $(P,Q)\in\mathbf{K}[X]^2$?

EXERCICE C16.19 — 2) Démontrer de deux manières la « formule des comités »

$$\forall n \in \mathbf{N} \qquad \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}.$$

l'une combinatoire, l'autre en appliquant la formule du binôme de Newton à $(X+1)^{2n}$ et à $(X+1)^n$. 2) Proposer une généralisation de la formule énoncée en 1).

§ 4. DEGRÉ

DÉFINITION C16.20 (DEGRÉ D'UN POLYNÔME)
Le degré d'un polynôme $P \in \mathbf{K}[X]$, noté $\deg(P)$, est l'élément de $\mathbf{N} \cup \{-\infty\}$ défini par

$$\deg(P) := \begin{cases} \max\{k \in \mathbf{N} \,:\, [P]_k \neq 0_{\mathbf{K}}\} & \text{si } P \neq 0_{\mathbf{K}[X]} \\ -\infty & \text{si } P = 0_{\mathbf{K}[X]}\,. \end{cases}$$

EXEMPLE C16.21 — $\deg\left(4X^5 - 3X^4 + X^3 - 7X^2 - 18X + 42\right) = 5$.

DÉFINITION C16.22 (COEFFICIENT DOMINANT D'UN POLYNÔME NON NUL)
Le coefficient dominant d'un polynôme P non nul est défini par

$$\operatorname{dom}(P) := [P]_{\deg(P)}\,.$$

EXEMPLE C16.23 — $\operatorname{dom}\left(1 + 4X^2 + 4X^5 - 3X^8\right) = -3$.

DÉFINITION C16.24 (POLYNÔME UNITAIRE)
Un polynôme P est dit unitaire s'il est non nul et si son coefficient dominant est $1_{\mathbf{K}}$.

EXEMPLE C16.25 — Le polynôme $X^4 - 4X^2 + 3X$ est unitaire, contrairement au polynôme $X^2 - 4X^5 + 3$.

EXERCICE C16.26 — Soit $P \in \mathbf{K}[X]$ un polynôme non nul. Donner une propriété remarquable du polynôme $\dfrac{1}{\operatorname{dom}(P)} \cdot P$.

DÉFINITION C16.27 (RELATION D'ORDRE ET ADDITION SUR $\mathbf{N} \cup \{-\infty\}$)
On étend la relation d'ordre usuelle $\leqslant$ et l'addition $+$ sur $\mathbf{N}$ à $\mathbf{N} \cup \{-\infty\}$ en posant, pour tout $(n,m) \in (\mathbf{N} \cup \{-\infty\})^2$:

$$n \leqslant m \iff \begin{cases} (n,m) \in \mathbf{N}^2 \text{ et } n \leqslant m \text{ au sens de la relation d'ordre usuelle sur } \mathbf{N} \\ \text{ou} \\ n = -\infty \end{cases}$$

$$n + m = \begin{cases} n+m \text{ au sens de l'addition usuelle sur } \mathbf{N}, \text{ si } (n,m) \in \mathbf{N}^2 \\ -\infty \text{ sinon}\,. \end{cases}$$

Théorème C16.28 (propriétés du degré)
Soit $(P,Q) \in \mathbf{K}[X]^2$.
1) $\deg(P+Q) \leqslant \max\left\{\deg(P),\deg(Q)\right\}$, avec égalité si et seulement si l'une des trois propriétés suivantes est vraie
(C1) $\deg(P) \neq \deg(Q)$
(C2) $\deg(P) = \deg(Q) = -\infty$
(C3) $\deg(P) = \deg(Q) \neq -\infty$ et $\mathrm{dom}(P) + \mathrm{dom}(Q) \neq 0_{\mathbf{K}}$.
2) $\deg(P \times Q) = \deg(P) + \deg(Q)$.

Corollaire C16.29 (intégrité de $\mathbf{K}[X]$)
L'anneau $(\mathbf{K}[X], +, \times)$ est intègre.

Exercice C16.30 — Soit $(P,Q) \in \mathbf{K}[X]^2$ un couple de polynômes non nuls. Démontrer que

$$\mathrm{dom}(PQ) = \mathrm{dom}(P)\,\mathrm{dom}(Q)\ .$$

Exercice C16.31 — Soit $(P,Q) \in \mathbf{K}[X]^2$ tel que $\deg(Q) \geqslant 1$.
1) Démontrer que $\deg(P \circ Q) = \deg(P)\deg(Q)$.
2) Conjecturer puis démontrer un résultat concernant le coefficient dominant de $P \circ Q$.

Exercice C16.32 — Résoudre $P \circ P = P$ d'inconnue $P \in \mathbf{K}[X]$.

Exercice C16.33 — Résoudre $Q^2 = XP^2$ d'inconnue $(P,Q) \in \mathbf{K}[X]^2$.

Exercice C16.34 — Résoudre $P\left(X^2\right) = X^2 P$ d'inconnue $P \in \mathbf{K}[X]$.

Exercice C16.35 — Donner une CNS sur $P \in \mathbf{K}[X]$ pour qu'il existe $Q \in \mathbf{K}[X]$ tel que $P \circ Q = X$.

Définition C16.36 (ensemble des combinaisons linéaires d'une famille finie de polynômes)
Soient $n \in \mathbf{N}^*$ et $(P_1,\ldots,P_n) \in \mathbf{K}[X]^n$. L'ensemble des combinaisons linéaires de $(P_1,\ldots,P_n)$ est noté $\mathrm{Vect}(P_1,\ldots,P_n)$, i.e.

$$\mathrm{Vect}(P_1,\ldots,P_n) = \left\{\sum_{k=1}^{n} \lambda_k \cdot P_k \ :\ (\lambda_1,\ldots,\lambda_n) \in \mathbf{K}^n\right\}\ .$$

Proposition C16.37 (propriétés de $\mathrm{Vect}(P_1,\ldots,P_n)$ où $(P_1,\ldots,P_n) \in \mathbf{K}[X]^n$)
Soient $n \in \mathbf{N}^*$ et $(P_1,\ldots,P_n) \in \mathbf{K}[X]^n$.
1) $0_{\mathbf{K}[X]} \in \mathrm{Vect}(P_1,\ldots,P_n)$
2) $\mathrm{Vect}(P_1,\ldots,P_n)$ est stable par combinaison linéaire.

Remarque C16.38 — Si $n \in \mathbf{N}$, alors l'ensemble des polynômes de $\mathbf{K}[X]$ de degré n n'est pas stable par combinaison linéaire. En effet $X^n - X^n = 0_{\mathbf{K}[X]}$ et $\deg\left(0_{\mathbf{K}[X]}\right) = -\infty \neq n$.

Définition C16.39 ($\mathbf{K}_n[X]$)
Pour tout $n \in \mathbf{N}$, on note $\mathbf{K}_n[X]$ l'ensemble des polynômes de $\mathbf{K}[X]$ de degré inférieur ou égal à n, i.e.

$$\mathbf{K}_n[X] := \{P \in \mathbf{K}[X] \ : \ \deg(P) \leqslant n\}.$$

Remarque C16.40 — $\mathbf{K}_0[X]$ est l'ensemble des polynômes constants.

Proposition C16.41 (structure de $\mathbf{K}_n[X]$ et base canonique)
Soit $n \in \mathbf{N}$.
1) $\mathbf{K}_n[X] = \mathrm{Vect}\left(1, X, X^2, \ldots, X^n\right)$
2) $\mathbf{K}_n[X]$ contient le polynôme nul $0_{\mathbf{K}[X]}$ et est stable par combinaison linéaire.
3) $\forall\, P \in \mathbf{K}_n[X] \quad \exists!\,(\lambda_0, \lambda_1, \ldots, \lambda_n) \in \mathbf{K}^{n+1} \quad P = \sum_{k=0}^{n} \lambda_k \cdot X^k$

Notation C16.42 — $U(\mathbf{K}[X])$ désigne l'ensemble des éléments inversibles de l'anneau $(\mathbf{K}[X], +, \times)$, i.e.

$$U(\mathbf{K}[X]) := \left\{P \in \mathbf{K}[X] \ : \ \exists\, Q \in \mathbf{K}[X] \quad PQ = 1_{\mathbf{K}[X]} = QP\right\}.$$

Proposition C16.43 (caractérisation des inversibles de l'anneau $(\mathbf{K}[X], +, \times)$)

$$U(\mathbf{K}[X]) = \left\{P \in \mathbf{K}[X] \ : \ \deg(P) = 0\right\} = \mathbf{K}^*$$

§ 5. Divisibilité et division euclidienne

Définition C16.44 (divisibilité, diviseur, multiple)
Soit $(A, B) \in \mathbf{K}[X]^2$.
1) Le polynôme A est divisible par le polynôme B si

$$\exists\, Q \in \mathbf{K}[X] \quad A = BQ\,.$$

Dans ce cas, on note $B \mid A$.
2) Si $B \mid A$, alors on dit que B est un diviseur de A ou que A est un multiple de B.

Exercice C16.45 — Donner une CNS sur $\lambda \in \mathbf{K}$ pour que $X^3 - 1$ divise $X^6 + \lambda$.

Exercice C16.46 — Soient A, B, C des polynômes de $\mathbf{K}[X]$.
1) Justifier que A divise A.
2) On suppose que A divise B et que B divise C. Démontrer que A divise C.
3) On suppose que A divise B et que B divise A. Les polynômes A et B sont-ils nécessairement égaux ?

Exercice C16.47 — Soient $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X] \setminus \left\{0_{\mathbf{K}[X]}\right\}$.
1) Démontrer que, si A divise B, alors $\deg(A) \leqslant \deg(B)$.
2) La réciproque est-elle vraie ?

DÉFINITION C16.48 (POLYNÔMES ASSOCIÉS)
Deux polynômes A et B de $\mathbf{K}[X]$ sont dits associés si $A \mid B$ et $A \mid B$.

PROPOSITION C16.49 (CRITÈRE POUR QUE DEUX POLYNÔMES SOIENT ASSOCIÉS)
Soit $(A,B) \in \mathbf{K}[X]^2$. Alors A et B sont associés si et seulement si

$$\exists \lambda \in \mathbf{K}^* \quad A = \lambda \cdot B\,.$$

REMARQUE C16.50 — La relation « être associés » sur $\mathbf{K}[X]$ est une relation d'équivalence.

THÉORÈME C16.51 (DIVISION EUCLIDIENNE DANS $\mathbf{K}[X]$)
Soit $(A,B) \in \mathbf{K}[X]^2$. On suppose $B \neq 0_{\mathbf{K}[X]}$. Alors, existe un unique couple $(Q,R) \in \mathbf{K}[X]^2$ tel que

$$\left\{\begin{array}{ll} & A = BQ + R \\ \text{et} & \\ & \deg(R) < \deg(B)\,. \end{array}\right.$$

Le polynôme Q (resp. R) est appelé quotient (resp. reste) de la division euclidienne de A par B.

EXEMPLE C16.52 — La division euclidienne de $A := X^5 - 2X^4 + 3X^3 - 4X^2 + 5X + 2$ par $B := 3X^2 - 2X + 1$ est

$$A = \underbrace{\left(\frac{X^3}{3} - \frac{4}{9}X^2 + \frac{16}{27}X - \frac{64}{81}\right)}_{\text{quotient}} B + \underbrace{\left(\frac{229}{81}X + \frac{226}{81}\right)}_{\text{reste}}.$$

EXERCICE C16.53 — Effectuer la division euclidienne de $A := X^5 + X^4 + X^3 + X^2 + X + \alpha$ par $B := X^2 + X + 1$, où $\alpha \in \mathbf{K}$.

ALGORITHME C16.54 (DIVISION EUCLIDIENNE DANS $\mathbf{K}[X]$)

donnée: $(A,B) \in \mathbf{K}[X]^2$ tel que $0 \leqslant \deg(B) \leqslant \deg(A)$
résultat: (Q,R) où Q (resp. R) est le quotient (resp. reste) de la division euclidienne de A par B
$A' \longleftarrow A$ /* copie de la valeur de A */
$Q \longleftarrow 0_{\mathbf{K}[X]}$ /* initialisation du quotient à $0_{\mathbf{K}[X]}$ */
tant que $\deg(A') \geqslant \deg(B)$ **faire**
  $M \longleftarrow \dfrac{\mathrm{dom}(A')}{\mathrm{dom}(B)} X^{\deg(A') - \deg(B)}$ /* nouveau monôme apparaissant dans le quotient */
  $Q \longleftarrow Q + M$ /* actualisation du quotient */
  $A' \longleftarrow A' - MB$ /* on retranche à A' un multiple de B en diminuant son degré */
fin
renvoie (Q, A')

PROPOSITION C16.55 (CORRECTION TOTALE DE L'ALGORITHME DE LA DIVISION EUCLIDIENNE DANS $\mathbf{K}[X]$)
1) Le degré de A' est un variant de boucle.
2) La relation $A = QB + A'$ est un invariant de boucle.

Proposition C16.56 (critère de divisibilité via la division euclidienne)
Soit $(A,B) \in \mathbf{K}[X]^2$. On suppose $B \neq 0_{\mathbf{K}[X]}$. Alors A est divisible par B si et seulement si le reste de la division euclidienne de A par B est nul.

Démonstration — Considérons la division euclidienne de A par B

$$(\star) \qquad A = BQ + R$$

où $(Q,R) \in \mathbf{K}[X]^2$ et $\deg(R) < \deg(B)$.
$\boxed{\Longleftarrow}$ Si $R = 0_{\mathbf{K}[X]}$ alors $(\star)$ se réécrit $A = BQ$ et donc B divise A.
$\boxed{\Longrightarrow}$ Supposons que A est divisible par B. Alors il existe $Q_1 \in \mathbf{K}[X]$ tel que $A = BQ_1$. Nous pouvons donc écrire

$$(\star\star) \qquad A = BQ_1 + R_1$$

en posant $R_1 := 0_{\mathbf{K}[X]}$. Comme $\deg(R_1) = -\infty < \deg(B)$, les identités $(\star)$ et $(\star\star)$ sont des divisions euclidiennes de A par B. Par unicité d'une telle, il vient $R = R_1 = 0_{\mathbf{K}[X]}$ (et $Q = Q_1$).

Exercice C16.57 — Donner une condition nécessaire et suffisante sur $\alpha \in \mathbf{K}$ pour que le polynôme $A := X^5 + X^4 + X^3 + X^2 + X + \alpha$ soit divisible par $B := X^2 + X + 1$.

Exercice C16.58 — Soit $(A,B) \in \mathbf{K}[X]^2$. On suppose $B \neq 0_{\mathbf{K}[X]}$. Écrire la division euclidienne de A par B, si $\deg(A) < \deg(B)$.

Exercice C16.59 — Soit $P \in \mathbf{K}[X]$ et soit $a \in \mathbf{K}$. Écrire le reste de la division euclidienne de P par $X - a$ en fonction de $P(a)$.

Exercice C16.60 — Soit $P \in \mathbf{K}[X]$ et soit $(a,b) \in \mathbf{K}^2$ tel que $a \neq b$. Écrire le reste de la division euclidienne de P par $(X-a)(X-b)$ en fonction de $P(a)$ et $P(b)$.

Exercice C16.61 — Soit $B \in \mathbf{K}[X]$ de degré $n \geqslant 1$. Soit

$$f \left| \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathbf{K}_{n-1}[X] \\ P & \longmapsto & \text{reste de la division euclidienne de } P \text{ par } B \end{array} \right. .$$

Démontrer que f est une application bien définie, qui est linéaire, i.e.

$$\forall (P,Q,\lambda,\mu) \in \mathbf{K}[X] \times \mathbf{K}[X] \times \mathbf{K} \times \mathbf{K} \quad f(\lambda \cdot P + \mu \cdot Q) = \lambda \cdot f(P) + \mu \cdot f(Q)$$

et surjective. Est-elle injective ?

§ 6. Fonctions polynomiales et racines

Définition C16.62 (fonction polynomiale associée à un polynôme)
Soit $P \in \mathbf{K}[X]$. La fonction polynomiale associée au polynôme P, notée $\widetilde{P}$, est définie par

$$\widetilde{P} \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ x & \longmapsto & \sum_{k=0}^{+\infty} [P]_k \, x^k \end{array} \right. .$$

Remarque C16.63 — Notons $\mathbf{Z}/2\mathbf{Z}$ le corps à deux éléments $\{\overline{0}, \overline{1}\}$, où $\overline{0}$ est le neutre de l'addition et $\overline{1}$ est le neutre de la multiplication. Alors les fonctions

$$\widetilde{P} \left| \begin{array}{ccc} \mathbf{Z}/2\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \\ x & \longmapsto & x+1 \end{array} \right. \quad \text{et} \quad \widetilde{Q} \left| \begin{array}{ccc} \mathbf{Z}/2\mathbf{Z} & \longrightarrow & \mathbf{Z}/2\mathbf{Z} \\ x & \longmapsto & x^3+x^2+x+1 \end{array} \right.$$

associée aux polynômes $P = X+1$ et $Q = X^3+X^2+X+1$ sont égales, bien que les polynômes P et Q soient différents.

Proposition C16.64 (propriétés algébriques de l'évaluation en un point)
Soit $x \in \mathbf{K}$. L'application

$$\mathrm{eval}_x \left| \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathbf{K} \\ P & \longmapsto & \widetilde{P}(x) := \sum_{k=0}^{+\infty} [P]_k \, x^k \end{array} \right.$$

est un morphisme d'anneaux, qui est de plus linéaire, i.e.

1) pour tout $(\lambda, \mu, P, Q) \in \mathbf{K} \times \mathbf{K} \times \mathbf{K}[X] \times \mathbf{K}[X]$, $\widetilde{\left(\lambda \cdot P + \mu \cdot Q\right)}(x) = \lambda \widetilde{P}(x) + \mu \widetilde{Q}(x)$;
2) pour tout $(P,Q) \in \mathbf{K}[X]^2$, $\widetilde{PQ}(x) = \widetilde{P}(x)\, \widetilde{Q}(x)$;
3) $\widetilde{1_{\mathbf{K}[X]}}(x) = 1_{\mathbf{K}}$.

Remarque C16.65 — Comme les opérations $+$, $\times$ et $\cdot$ sur les fonctions de $\mathbf{K}$ dans $\mathbf{K}$ sont définies point par point, nous déduisons de C16.64 que l'application

$$\varphi \left| \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathscr{F}(\mathbf{K}, \mathbf{K}) \\ P & \longmapsto & \widetilde{P} \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ x & \longmapsto & \sum_{k=0}^{+\infty} [P]_k \, x^k \end{array} \right. \end{array} \right.$$

est un morphisme d'anneaux, qui est de plus linéaire, i.e.

1) pour tout $(\lambda, \mu, P, Q) \in \mathbf{K} \times \mathbf{K} \times \mathbf{K}[X] \times \mathbf{K}[X]$, $\widetilde{\left(\lambda \cdot P + \mu \cdot Q\right)} = \lambda \cdot \widetilde{P} + \mu \cdot \widetilde{Q}$;
2) pour tout $(P,Q) \in \mathbf{K}[X]^2$, $\widetilde{PQ} = \widetilde{P}\, \widetilde{Q}$;
3) $\widetilde{1_{\mathbf{K}[X]}} = 1_{\mathscr{F}(\mathbf{K},\mathbf{K})}$.

Définition C16.66 (racine d'un polynôme et spectre d'un polynôme)
Soient $P \in \mathbf{K}[X]$.

1) Un élément $\alpha \in \mathbf{K}$ est appelé racine du polynôme P si $\widetilde{P}(\alpha) = 0$.
2) Le spectre de P dans $\mathbf{K}$, noté $\mathrm{Spec}_{\mathbf{K}}(P)$, est l'ensemble des racines du polynôme P dans $\mathbf{K}$, i.e.

$$\mathrm{Spec}_{\mathbf{K}}(P) = \left\{ \alpha \in \mathbf{K} \, : \, \widetilde{P}(\alpha) = 0 \right\} .$$

Exercice C16.67 — Soit $P := X^5 + 32$. Déterminer $\mathrm{Spec}_{\mathbf{C}}(P)$, puis $\mathrm{Spec}_{\mathbf{R}}(P)$.

Exercice C16.68 — Justifier qu'un polynôme à coefficients réels, de degré impair, possède une racine réelle.

Proposition C16.69 (caractérisation d'une racine par une relation de divisibilité)
Soient $P \in \mathbf{K}[X]$ et $\alpha \in \mathbf{K}$.

$$\alpha \text{ est racine de } P \iff X - a \text{ divise } P$$

Proposition C16.70 (factorisation d'un polynôme connaissant des racines distinctes)
Soient $P \in \mathbf{K}[X]$, $r \in \mathbf{N}^*$ et $\alpha_1, \ldots, \alpha_r$ des racines deux-à-deux distinctes de P. Alors

$$\prod_{k=1}^{r} (X - \alpha_k) \text{ divise } P\,.$$

Exercice C16.71 — Soient des entiers naturels r et n tels que $1 \leqslant r < n$ et $\alpha_1, \ldots, \alpha_r$ des nombres réels distincts. Déterminer l'ensemble

$$F = \{P \in \mathbf{R}_n[X] \ : \ \alpha_1, \ldots, \alpha_r \text{ sont racines de } P\}\,.$$

On écrira F comme l'ensemble des combinaisons linéaires d'une famille finie de polynômes.

Proposition C16.72 (majoration du nombre de racines d'un polynôme)
Soit P un polynôme non nul de $\mathbf{K}[X]$. L'ensemble $\mathrm{Spec}_{\mathbf{K}}(P)$ est fini et

$$\mathrm{card}\left(\mathrm{Spec}_{\mathbf{K}}(P)\right) \leqslant \deg(P)\,.$$

Exercice C16.73 — Soit $n \in \mathbf{N}$. Que dire d'un polynôme P de $\mathbf{K}_n[X]$ qui possède $n+1$ racines ?

Proposition C16.74 (polynôme versus fonction polynomiale associé lorsque K est infini)
Supposons le corps $\mathbf{K}$ infini. L'application

$$\varphi \left| \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathscr{F}(\mathbf{K},\mathbf{K}) \\ P & \longmapsto & \widetilde{P} \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ x & \longmapsto & \displaystyle\sum_{k=0}^{+\infty} [P]_k\, x^k \end{array} \right. \end{array} \right.$$

que l'on sait être un morphisme d'anneaux, qui est de plus linéaire, est en outre injective. La fonction polynomiale associée à un polynôme détermine donc le polynôme.

Proposition-Définition C16.75 (multiplicité d'une racine)
Soient $P \in \mathbf{K}[X]$ un polynôme de degré $n \geqslant 1$ et $\alpha \in \mathbf{K}$ une racine de P.

1) L'ensemble $\left\{k \in \mathbf{N}^* \ : \ (X - a)^k \text{ divise } P\right\}$ est une partie non vide de $\mathbf{N}$, incluse dans $[\![1, n]\!]$.
2) On définit la multiplicité de la racine α de P, notée $\mathrm{mult}(P, \alpha)$, par

$$\mathrm{mult}(P,\alpha) := \max\left\{k \in \mathbf{N}^* \ : \ (X - \alpha)^k \text{ divise } P\right\} \in [\![1, n]\!]$$

Démonstration — Posons $\mathscr{E} := \left\{k \in \mathbf{N}^* \ : \ (X-a)^k \text{ divise } P\right\}$.

- L'ensemble $\mathscr{E}$ est par définition une partie de $\mathbf{N}$.
- Comme α est une racine de P, le polynôme $X-\alpha$ divise n, donc $1 \in \mathscr{E}$.
- Si $k \in \mathscr{E}$ alors il existe $Q \in \mathbf{K}[X]$ tel que

$$P = (X-\alpha)^k Q\,.$$

En analysant les degrés il vient

$$k + \deg(Q) = \deg(P) \in \mathbf{N}^*$$

Nous en déduisons que $\deg(Q) \in \mathbf{N}^*$ puis $k \leqslant n$. Ainsi $\mathscr{E} \subset [\![1, n]\!]$ et $\mathscr{E}$ est finie.

Proposition C16.76 (Une caractérisation de la multiplicité d'une racine)
Soient P un polynôme non constant de $\mathbf{K}[X]$, $\alpha \in \mathbf{K}$ une racine de P et $k \in \mathbf{N}^*$. Alors

$$k = \operatorname{mult}(P, \alpha) \iff \begin{cases} (X-\alpha)^k \text{ divise } P \\ \text{et} \\ (X-\alpha)^{k+1} \text{ ne divise pas } P \end{cases}$$

Démonstration — Posons $\mathscr{E} := \left\{k \in \mathbf{N}^* \ : \ (X-a)^k \text{ divise } P\right\}$.

$\boxed{\Longrightarrow}$ Supposons $k = \operatorname{mult}(P, \alpha)$.
Comme $k \in \mathscr{E}$, $(X-\alpha)^k$ divise P.
Puisque k est le plus grand élément de $\mathscr{E}$, $k+1$ n'appartient pas à $\mathscr{E}$ et donc $(X-\alpha)^{k+1}$ ne divise pas P.
$\boxed{\Longleftarrow}$ Supposons que $(X-\alpha)^k$ divise P et $(X-\alpha)^{k+1}$ ne divise pas P.
Nous en déduisons que $k \in \mathscr{E}$. Démontrons que k est le plus grand élément de $\mathscr{E}$, en raisonnant par l'absurde.
Supposons que k n'est pas le plus grand élément de $\mathscr{E}$. Alors il existe un élément ℓ de $\mathscr{E}$ tel que $\ell > k$. Ainsi $k+1 \leqslant \ell$ et

$$(\star) \quad (X-\alpha)^\ell \text{ divise } P$$

Comme $k+1 \leqslant \ell$, $(X-\alpha)^{\ell-k-1} \in \mathbf{K}[X]$ et, de la factorisation

$$(X-\alpha)^\ell = (X-\alpha)^{k+1}\,(X-\alpha)^{\ell-k-1}$$

nous déduisons

$$(\star\star) \quad (X-\alpha)^{k+1} \text{ divise } (X-\alpha)^\ell$$

De $(\star)$, $(\star\star)$ et de la transitivité de la relation de divisibilité dans $\mathbf{K}[X]$, nous déduisons que $(X-\alpha)^{k+1}$ divise P. Contradiction.

Exemple C16.77 — Soit le polynôme $P := X^5 - X^4 - 2X^3 + 2X^2 + X - 1$. Nous observons 1 est racine de P et savons donc que $X-1$ divise P. Nous effectuons la division euclidienne de P par $X-1$ pour trouver

$$P = (X-1)Q$$

où

$$Q := X^4 - 2X^2 + 1 = (X^2-1)^2 = (X-1)^2(X+1)^2\,.$$

Ainsi $P = (X-1)^3(X+1)^2$. Nous en déduisons que $(X-1)^3$ divise P et que $(X-1)^4$ ne divise pas P. Nous avons établi $\operatorname{mult}(P, \alpha) = 3$.

DÉFINITION C16.78 (POLYNÔME SCINDÉ)
Soit P un polynôme de $\mathbf{K}[X]$ de degré $n \geqslant 1$. On dit que P est scindé sur le corps $\mathbf{K}$ s'il existe des éléments $\alpha_1, \ldots, \alpha_n$ de $\mathbf{K}$, non nécessairement deux-à-deux distincts, tels que

$$P = \operatorname{dom}(P) \cdot \prod_{k=1}^{n} (X - \alpha_k) \ .$$

EXEMPLE C16.79 — Le polynôme $X^2 - 2$ n'est pas scindé sur $\mathbf{Q}$, mais est scindé sur $\mathbf{R}$.

EXEMPLE C16.80 — Si $n \in \mathbf{N}_{\geqslant 2}$ alors le polynôme $X^n - 1$ est scindé sur $\mathbf{C}$.

$$X^n - 1 = \prod_{\zeta \in \mathbf{U}_n} (X - \zeta) = \prod_{k=0}^{n-1} \left(X - e^{i\frac{2k\pi}{n}} \right)$$

PROPOSITION C16.81 (MULTIPLICITÉS DES RACINES D'UN POLYNÔME SCINDÉ SUR UN CORPS)
Soit P un polynôme non nul de $\mathbf{K}[X]$, scindé sur le corps $\mathbf{K}$. Alors, en regroupant les racines de P égales, on peut écrire le polynôme P sous la forme

$$P = \operatorname{dom}(P) \cdot \prod_{k=1}^{r} (X - \alpha_k)^{m_k}$$

$r \in \mathbf{N}^*$, $\alpha_1, \ldots, \alpha_r$ sont des éléments de $\mathbf{K}$ deux-à-deux distincts et $m_1, \ldots, m_r$ sont des entiers naturels non nuls. Alors
1) $\operatorname{Spec}_{\mathbf{K}}(P) = \{\alpha_1, \ldots, \alpha_r\}$ est de cardinal r ;
2) pour tout $k \in [\![1, r]\!]$, $\operatorname{mult}(P, \alpha_k) = m_k$.

EXERCICE C16.82 — Soient $(\lambda, \alpha_1, \alpha_2, \alpha_3) \in \mathbf{K}^* \times \mathbf{K} \times \mathbf{K} \times \mathbf{K}$ et

$$P := \lambda \cdot \prod_{k=1}^{3} (X - \alpha_k) \, .$$

Exprimer les coefficients de P en fonction de son coefficient dominant λ et de ses racines $\alpha_1, \alpha_2, \alpha_3$.

THÉORÈME C16.83 (FORMULES DE VIÈTE OU RELATIONS COEFFICIENTS-RACINES)
Soit P un polynôme de degré $n \geqslant 2$, scindé sur $\mathbf{K}$. Alors P peut être écrit sous la forme

$$P = \operatorname{dom}(P) \cdot \prod_{k=1}^{n} (X - \alpha_k)$$

où $\alpha_1, \ldots, \alpha_n$ sont des éléments de $\mathbf{K}$. Alors

$$\forall\, k \in [\![1, n]\!] \quad [P]_{n-k} = (-1)^k \operatorname{dom}(P) \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k}$$

et

$$\prod_{k=1}^{n} \alpha_k = \frac{(-1)^n \, [P]_0}{\operatorname{dom}(P)} \qquad \text{et} \qquad \sum_{k=1}^{n} \alpha_k = \frac{-[P]_{n-1}}{\operatorname{dom}(P)} \, .$$

EXERCICE C16.84 — Déterminer les couples (x, y) de nombres complexes tels que $x+y=2i$ et $xy=1+i$.

EXERCICE C16.85 — Déterminer les triplets (x, y, z) de nombres complexes non nuls vérifiant les trois équations suivantes.

$$\begin{cases} x+y+z &= 1 \\ \dfrac{1}{x}+\dfrac{1}{y}+\dfrac{1}{z} &= 1 \\ xyz &= -4 \end{cases}$$

EXEMPLE C16.86 — Si $n \in \mathbf{N}_{\geqslant 2}$ alors du scindage de $X^n - 1$ sur $\mathbf{C}$

$$X^n - 1 = \prod_{\zeta \in \mathbf{U}_n} (X - \zeta) = \prod_{k=0}^{n-1} \left(X - e^{i\frac{2k\pi}{n}}\right)$$

et des formules de Viète, nous déduisons

$$\prod_{\zeta \in \mathbf{U}_n} \zeta = \prod_{k=0}^{n-1} e^{i\frac{2k\pi}{n}} = (-1)^{n+1} \qquad \text{et} \qquad \sum_{\zeta \in \mathbf{U}_n} \zeta = \sum_{k=0}^{n-1} e^{i\frac{2k\pi}{n}} = 0\,.$$

THÉORÈME C16.87 (DE D'ALEMBERT-GAUSS)
Tout polynôme $P \in \mathbf{C}[X]$ tel que $\deg(P) \geqslant 1$ possède une racine dans $\mathbf{C}$.

COROLLAIRE C16.88 (SCINDAGE SUR C D'UN POLYNÔME DE $\mathbf{C}[X]$)
Pour tout $P \in \mathbf{C}[X]$ tel que $n := \deg(P) \geqslant 1$, il existe $(\alpha_1, \dots, \alpha_n) \in \mathbf{C}^n$ tel que

$$P = \operatorname{dom}(P) \cdot \prod_{k=1}^{n} (X - \alpha_k)$$

Démonstration — Nous raisonnons par récurrence. Nous notons, pour tout $n \in \mathbf{N}^*$

$$\mathscr{P}(n) \ : \ \text{« tout polynôme de } \mathbf{C}[X] \text{ de degré } n \text{ est scindé sur } \mathbf{C} \text{ »}$$

• Initialisation à $n = 1$. Soit P un polynôme de degré n. Alors il existe $(a_1, a_0) \in \mathbf{C}^* \times \mathbf{C}$ tel que $P = a_1 X + a_0$. Ainsi

$$P = a_1 \cdot \left(X - \frac{a_0}{a_1}\right) = \operatorname{dom}(P) \cdot (X - \alpha_1)$$

où $\alpha_1 := \dfrac{a_0}{a_1} \in \mathbf{C}$.

• Hérédité. Soit $n \in \mathbf{N}^*$ tel que, tout polynôme de $\mathbf{C}[X]$ de degré n est scindé sur $\mathbf{C}$.
Soit P un polynôme de $\mathbf{C}[X]$ de degré $n+1$. D'après le théorème de d'Alembert-Gauß, il existe $\alpha_{n+1} \in \mathbf{C}$ tel que $\widetilde{P}(\alpha_{n+1}) = 0$. D'après C16.69, il existe $Q \in \mathbf{C}[X]$ tel que

$$(\star) \qquad P = Q\,(X - \alpha_{n+1})\,.$$

En analysant les degrés et coefficients dominants de chacun des membres de cette identité, nous observons que $\deg(Q) = n$ et $\operatorname{dom}(Q) = \operatorname{dom}(P)$. D'après l'hypothèse de récurrence il existe $(\alpha_1, \dots, \alpha_n) \in \mathbf{C}^n$ tel que

$$(\star\star) \qquad Q = \operatorname{dom}(Q) \cdot \prod_{k=1}^{n} (X - \alpha_k) = \operatorname{dom}(P) \cdot \prod_{k=1}^{n} (X - \alpha_k)$$

D'après $(\star)$ et $(\star\star)$, il vient

$$P = \operatorname{dom}(P) \cdot \prod_{k=1}^{n+1} (X - \alpha_k)$$

§ 7. Polynômes interpolateurs de Lagrange

Proposition C16.89 (Existence et unicité des interpolateurs élémentaires de Lagrange)
Soient un entier naturel $n \geqslant 2$ et $x_1, \dots, x_n$ des éléments de $\mathbf{K}$ deux-à-deux distincts.

1) Pour tout $i \in [\![1, n]\!]$, il existe un unique polynôme $L_i \in \mathbf{K}[X]$ tel que

$$\begin{cases} & \deg(L_i) = n - 1 \\ \text{et} & \\ & \forall j \in [\![1, n]\!] \quad L_i(x_j) = \delta_{i,j} \, . \end{cases}$$

2) Pour tout $i \in [\![1, n]\!]$, $L_i = \displaystyle\prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{X - x_j}{x_i - x_j}$.

Théorème C16.90 (Polynôme interpolateur de Lagrange)
Soient un entier naturel $n \geqslant 2$, $x_1, \dots, x_n$ des éléments de $\mathbf{K}$ deux-à-deux distincts et $y_1, \dots, y_n$ des éléments de $\mathbf{K}$.

1) Il existe un unique polynôme $L \in \mathbf{K}_{n-1}[X]$ tel que, pour tout $i \in [\![1, n]\!]$, $L(x_i) = y_i$.
2) Si $L_1, \dots, L_n$ sont les polynômes interpolateurs associés aux points $x_1, \dots, x_n$ introduits en C16.89 alors

$$L = \sum_{i=1}^{n} y_i \cdot L_i = \sum_{i=1}^{n} y_i \cdot \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{X - x_j}{x_i - x_j} \, .$$

Exercice C16.91 — Déterminer l'unique polynôme $P \in \mathbf{K}_3[X]$ tel que $P(0) = 5$, $P(1) = -2$, $P(2) = 7$, $P(3) = -1$.

Exercice C16.92 — Soient un entier naturel $n \geqslant 2$ et $x_1, \dots, x_n$ des éléments de $\mathbf{K}$ deux-à-deux distincts. Démontrer que l'application

$$\varphi \left| \begin{array}{ccc} \mathbf{K}_{n-1}[X] & \longrightarrow & \mathbf{K}^n \\ P & \longmapsto & \left(\widetilde{P}(x_1), \widetilde{P}(x_2), \dots, \widetilde{P}(x_n)\right) \end{array} \right.$$

est bijective et expliciter son application réciproque.

§ 8. Dérivation

Notation C16.93 — Dans cette partie, $\mathbf{K}$ n'est pas un corps quelconque, mais désigne $\mathbf{R}$ ou $\mathbf{C}$.

Définition C16.94 (polynôme dérivé formel et polynômes dérivés itérés formels)
Soit $P \in \mathbf{K}[X]$.
1) Le polynôme dérivé formel P' de P est l'unique élément de $\mathbf{K}[X]$ défini par

$$\forall\, k \in \mathbf{N} \quad \left[P'\right]_k = (k+1)\,[P]_{k+1}$$

de sorte que

$$P' = \sum_{k=0}^{+\infty} (k+1)\,[P]_{k+1}\,X^k = \sum_{k=1}^{+\infty} k\,[P]_k\,X^{k-1}$$

2) On définit par récurrence les polynômes dérivés itérés (ou successifs) formels de P en posant

$$\left\{\begin{array}{ll} & P^{(0)} = P \\ \text{et} & \\ & \forall\, k \in \mathbf{N} \quad P^{(k+1)} = \left(P^{(k)}\right)' \end{array}\right.$$

Exemple C16.95 — Si $P = 2X^4 - 7X^3 + 4X^2 - 3X + 1$ alors

$$\begin{array}{rclrcl} P' & = & P^{(1)} = 8X^3 - 21X^2 + 8X - 3 & P^{(2)} & = & 24X^2 - 42X + 8 \\ P^{(3)} & = & 48X - 42 & P^{(4)} & = & 48 \end{array}$$

et, pour tout $k \geqslant 5 = \deg(P) + 1$, $P^{(k)} = 0$.

Remarque C16.96 — Soit $P \in \mathbf{R}[X]$.
1) Nous pouvons dériver formellement le polynôme P pour obtenir $P' \in \mathbf{R}[X]$, puis considérer la l'application $\widetilde{(P')} \in \mathscr{F}(\mathbf{K},\mathbf{K})$ canoniquement associée à P'.
2) Il est également possible de d'abord introduire la fonction $\widetilde{P} \in \mathscr{F}(\mathbf{R},\mathbf{R})$, puis de la dériver au sens du calcul différentiel pour obtenir la fonction $\left(\widetilde{P}\right)'$.
Les deux constructions livrent la même fonction de $\mathbf{R}$ dans $\mathbf{R}$, i.e. $\widetilde{(P')} = \left(\widetilde{P}\right)'$.

Proposition C16.97 (degré du polynôme dérivé)
Soit $P \in \mathbf{K}[X]$. Alors

$$\deg\left(P'\right) = \left\{\begin{array}{cl} -\infty & \text{si } P \in \mathbf{K}_0[X] \\ \deg(P) - 1 & \text{si } \deg(P) \geqslant 1\,. \end{array}\right.$$

Démonstration — • Supposons que $P \in \mathbf{K}_0[X]$. Alors, pour tout $k \in \mathbf{N}^*$, $[P]_k = 0_{\mathbf{K}}$. Nous en déduisons que, pour tout $k \in \mathbf{N}$

$$\left[P'\right]_k = (k+1)\,[P]_{k+1} = 0_{\mathbf{K}}$$

Le polynôme P' est donc nul.
• Supposons que $n := \deg(P) \geqslant 1$. Alors

$$P = \sum_{k=0}^{n} [P]_k \cdot X^k \quad \text{et} \quad [P]_n \neq 0_{\mathbf{K}}\,.$$

Nous en déduisons

$$P' = \sum_{k=1}^{n} k\,[P]_k \cdot X^{k-1} = \sum_{k=0}^{n-1} (k+1)\,[P]_{k+1} \cdot X^k \in \mathrm{Vect}\left(1, X, \ldots, X^{n-1}\right) = \mathbf{K}_{n-1}[X]$$

d'où $\deg\left(P'\right) \leqslant n-1$. Comme de plus

$$\left[P'\right]_{n-1} = n\,[P]_n \neq 0_{\mathbf{K}}$$

il vient $\deg\left(P'\right) = n-1$.

PROPOSITION C16.98 (DE L'ANNULATION DES DÉRIVÉES ITÉRÉES D'UN POLYNÔME)
Soit P un polynôme non nul de $\mathbf{K}[X]$ dont le degré est noté n.

1) $P^{(n+1)} = 0_{\mathbf{K}[X]}$
2) Pour tout $k \geqslant n+1$, $P^{(k)} = 0_{\mathbf{K}[X]}$.

Démonstration — L'assertion 2) est conséquence immédiate de 1). Nous établissons 1) en raisonnant par récurrence sur le degré $n \in \mathbf{N}$ du polynôme P. Posons, pour tout $n \in \mathbf{N}$

$$\mathscr{P}(n) \;:\; « \; P^{(n+1)} = 0_{\mathbf{K}[X]} \; »$$

• Initialisation à $n = 0$. Soit P un polynôme de $\mathbf{K}[X]$ de degré 0. Nous avons déjà établi en C16.97 qu'alors $P^{(1)} = P' = 0_{\mathbf{K}[X]}$.
• Hérédité. Soit $n \in \mathbf{N}$ tel que $\mathscr{P}(n)$ est vrai. Considérons un polynôme P de $\mathbf{K}[X]$ de degré $n+1$. Comme $n+1 \geqslant 1$, C16.97 livre $\deg\left(P'\right) = n$. D'après l'hypothèse de récurrence

$$\left(P'\right)^{(n+1)} = 0_{\mathbf{K}[X]}\,.$$

Nous concluons à $P^{(n+2)} = 0_{\mathbf{K}[X]}$ en remarquant que $P^{(n+2)} = \left(P'\right)^{(n+1)}$.

PROPOSITION C16.99 (PROPRIÉTÉS ALGÉBRIQUES DE LA DÉRIVATION DES POLYNÔMES)

1) Dérivée d'une combinaison linéaire

$$\forall\,(P, Q, \lambda, \mu) \in \mathbf{K}[X] \times \mathbf{K}[X] \times \mathbf{K} \times \mathbf{K} \qquad \left(\lambda \cdot P + \mu \cdot Q\right)' = \lambda \cdot P' + \mu \cdot Q'$$

2) Dérivée d'un produit de deux polynômes

$$\forall\,(P, Q) \in \mathbf{K}[X]^2 \qquad (P \times Q)' = P' \times Q + P \times Q'$$

3) Dérivée de produit d'un nombre fini de polynômes

$$\forall\, n \in \mathbf{N}_{\geqslant 2} \quad \forall\,(P_1, P_2, \ldots, P_n) \in \mathbf{K}[X]^n \quad \left(\prod_{i=1}^{n} P_i\right)' = \sum_{i=1}^{n} \left(P_i' \times \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j\right)$$

Démonstration — 1) Soient $(P, Q, \lambda, \mu) \in \mathbf{K}[X] \times \mathbf{K}[X] \times \mathbf{K} \times \mathbf{K}$ et $k \in \mathbf{N}$. Nous calculons les coefficients de degré k des polynômes $\left(\lambda \cdot P + \mu \cdot Q\right)'$ et $\lambda \cdot P' + \mu \cdot Q'$.

$$\left[\left(\lambda \cdot P + \mu \cdot Q\right)'\right]_k = (k+1)\,\left[\lambda \cdot P + \mu \cdot Q\right]_{k+1} = (k+1)\,\left(\lambda \cdot [P]_{k+1} + \mu \cdot [Q]_{k+1}\right)$$

$$\left[\lambda \cdot P' + \mu \cdot Q'\right]_k = \lambda\,\left[P'\right]_k + \mu\,\left[Q'\right]_k = \lambda\,(k+1)\,[P]_{k+1} + \mu\,(k+1)\,[Q]_{k+1} = (k+1)\,\left(\lambda \cdot [P]_{k+1} + \mu \cdot [Q]_{k+1}\right)$$

et observons qu'ils sont égaux.

2) Soit $(P,Q) \in \mathbf{K}[X]^2$. Soit $k \in \mathbf{N}$. Nous calculons les coefficients des polynômes $(P \times Q)'$ et $P' \times Q + P \times Q'$

$$\begin{array}{rcl} \left[(P \times Q)'\right]_k & = & (k+1)\ [P \times Q]_{k+1} \\ & = & (k+1) \displaystyle\sum_{i=0}^{k+1} [P]_i [Q]_{k+1-i} \end{array}$$

$$\begin{array}{rcll} \left[P' \times Q + P \times Q'\right]_k & = & \left[P' \times Q\right]_k + \left[P \times Q'\right]_k & \\ & = & \displaystyle\sum_{i=0}^{k} \left[P'\right]_i [Q]_{k-i} + \sum_{i=0}^{k} [P]_i \left[Q'\right]_{k-i} & \\ & = & \displaystyle\sum_{i=0}^{k} (i+1)\, [P]_{i+1}\, [Q]_{k-i} + \sum_{i=0}^{k} (k-i+1)\, [P]_i\, [Q]_{k-i+1} & \\ & = & \displaystyle\sum_{i=1}^{k+1} i\, [P]_i\, [Q]_{k-i+1} + \sum_{i=0}^{k} (k-i+1)\, [P]_i\, [Q]_{k-i+1} & \text{[changement d'indice]} \\ & = & \displaystyle\sum_{i=0}^{k+1} i\, [P]_i\, [Q]_{k-i+1} + \sum_{i=0}^{k+1} (k-i+1)\, [P]_i\, [Q]_{k-i+1} & \text{[ajout de deux termes nuls]} \\ & = & \displaystyle\sum_{i=0}^{k+1} (i+k-i+1)\, [P]_i\, [Q]_{k-i+1} & \\ & = & (k+1) \displaystyle\sum_{i=0}^{k+1} [P]_i [Q]_{k+1-i} & \end{array}$$

et observons qu'ils sont égaux.

3) Nous raisonnons par récurrence sur le nombre $n \geqslant 2$ de facteurs. Posons, pour tout $n \in \mathbf{N}_{\geqslant 2}$

$$\mathscr{P}(n) : \text{« } \forall (P_1, P_2, \ldots, P_n) \in \mathbf{K}[X]^n \quad \left(\prod_{i=1}^{n} P_i\right)' = \sum_{i=1}^{n} \left(P_i' \times \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j\right) \text{ »}$$

• Initialisation à $n = 2$. Soient P_1 et P_2 des polynômes de $\mathbf{K}[X]$. On observe que

$$\left(\prod_{i=1}^{2} P_i\right)' = (P_1 P_2)' \quad \text{et} \quad \sum_{i=1}^{2} \left(P_i' \times \prod_{\substack{j=1 \\ j \neq i}}^{n} P_j\right) = P_1' P_2 + P_2' P_1$$

L'identité à établir résulte de 2).

• Hérédité. Soit $n \geqslant 2$ tel que $\mathscr{P}(n)$ est vrai. Considérons des polynômes $P_1, \ldots, P_n, P_{n+1}$ de $\mathbf{K}[X]$. D'après 2)

$$\left(\prod_{i=1}^{n+1} P_i\right)' = \left(\left(\prod_{i=1}^{n} P_i\right) P_{n+1}\right)' = \left(\prod_{i=1}^{n} P_i\right)' P_{n+1} + \left(\prod_{j=1}^{n} P_j\right) P_{n+1}'$$

Grâce à l'hypothèse de récurrence, nous pouvons réécrire le polynôme $\left(\prod_{i=1}^{n} P_i\right)'$ et obtenir

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

EXEMPLE C16.100 — Soient $a \in \mathbf{K}$ et $k \in \mathbf{N}_{\geqslant 2}$. Nous avons

$$(X-a)' = 1$$

et nous en déduisons

$$\left((X-a)^k\right)' = \left(\prod_{i=1}^{k}(X-a)\right)' = \sum_{i=1}^{k}\left((X-a)' \times \prod_{\substack{j=1\\ j\neq i}}^{k}(X-a)\right) = \sum_{i=1}^{k}\left(1\times(X-a)^{k-1}\right) = k\,(X-a)^{k-1}$$

PROPOSITION C16.101 (FORMULE DE LEIBNIZ)

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

Démonstration — Soient P et Q des polynômes de $\mathbf{K}[X]$. Nous démontrons le résultat en raisonnant par récurrence sur $n \in \mathbf{N}$. Posons, pour tout $n \in \mathbf{N}$

$$\mathscr{P}(n)\ :\ \text{« } (PQ)^{(n)} = \sum_{k=0}^{n}\binom{n}{k} P^{(k)}\,Q^{(n-k)} \text{ »}$$

• Initialisation à $n=0$. Comme

$$(PQ)^{(0)} = PQ \quad \text{et} \quad \sum_{k=0}^{0}\binom{0}{k} P^{(0)}\,Q^{(0-k)} = PQ$$

l'identité à démontrer est vraie.
• Hérédité. Soit $n \in \mathbf{N}$ tel que $\mathscr{P}(n)$ est vrai. D'après l'hypothèse de récurrence

$$(PQ)^{(n+1)} = \left((PQ)^{(n)}\right)' = \left(\sum_{k=0}^{n}\binom{n}{k} P^{(k)}\,Q^{(n-k)}\right)'$$

D'après C16.99

$$(PQ)^{(n+1)} = \sum_{k=0}^{n}\binom{n}{k}\left(\left(P^{(k)}\right)' Q^{(n-k)} + P^{(k)}\left(Q^{(n-k)}\right)'\right) = \sum_{k=0}^{n}\binom{n}{k} P^{(k+1)}\,Q^{(n-k)} + \sum_{k=0}^{n}\binom{n}{k} P^{(k)}\,Q^{(n+1-k)}$$

Grâce à un changement d'indice

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

Comme $\binom{n}{n} = 1 = \binom{n+1}{n+1}$, $\binom{n}{0} = 1 = \binom{n+1}{0}$ et, pour tout $k \in [\![1, n]\!]$

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \qquad \text{[relation de Pascal]}$$

il vient

$$(PQ)^{(n+1)} = \binom{n+1}{n+1} P^{(n+1)}\, Q^{(0)} + \sum_{k=1}^{n} \binom{n+1}{k} P^{(k)}\, Q^{(n+1-k)} + \binom{n+1}{0} P^{(0)}\, Q^{(n+1)} = \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)}\, Q^{(n+1-k)}$$

THÉORÈME C16.102 (FORMULE DE TAYLOR EXACTE DANS $\mathbf{K}[X]$ EN UN POINT DE $\mathbf{K}$)
Soit $a \in \mathbf{K}$. Alors, pour tout $n \in \mathbf{N}$, pour tout $P \in \mathbf{K}_n[X]$

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

Démonstration — Nous raisonnons par récurrence sur $n \in \mathbf{N}$. Posons, pour tout $n \in \mathbf{N}$

$$\mathscr{P}(n) \,:\, \forall\, P \in \mathbf{K}_n[X] \quad P = \sum_{k=0}^{n} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k\,.$$

• Initialisation à $n = 0$. Soit $P \in \mathbf{K}_0[X]$. Alors P est constant et nous pouvons l'écrire sous la forme $P = \lambda$, où $\lambda \in \mathbf{K}$. Comme

$$\sum_{k=0}^{0} \frac{\widetilde{P^{(k)}}(a)}{k!} (X-a)^k = \frac{\widetilde{P^{(0)}}(a)}{0!} (X-a)^0 = \widetilde{P^{(0)}}(a) = \lambda \qquad \text{[évaluer le polynôme constant } \lambda \text{ en } a \text{ donne } \lambda]$$

l'identité est établie pour ce polynôme P.
• Hérédité. Soit $n \in \mathbf{N}$ tel que $\mathscr{P}(n)$ est vrai. Soit $P \in \mathbf{K}_{n+1}[X]$. D'après le résultat sur le degré d'un polynôme dérivé (C16.97), $\deg(P') \leqslant n$. L'hypothèse de récurrence nous livre alors

$$(\star) \quad P' = \sum_{k=0}^{n} \frac{\widetilde{(P')^{(k)}}(a)}{k!} (X-a)^k = \sum_{k=0}^{n} \frac{\widetilde{P^{(k+1)}}(a)}{k!} (X-a)^k$$

Introduisons le polynôme

$$Q := \sum_{k=0}^{n} \frac{\widetilde{P^{(k+1)}}(a)}{(k+1)!} (X-a)^{k+1}$$

À l'aide des propriétés algébriques de la dérivation (C16.99) et

$$\forall\, k \in [\![0, n]\!] \quad \left((X-a)^{k+1}\right)' = (k+1)\,(X-a)^k \qquad \text{[cf. C16.100]}$$

nous calculons

$$(\star\star) \quad Q' = \sum_{k=0}^{n} \frac{\widetilde{P^{(k+1)}}(a)}{k!} (X-a)^k$$

Des propriétés algébriques de la dérivation, $(\star)$ et $(\star\star)$, nous déduisons

$$(P-Q)' = P' - Q' = 0_{\mathbf{K}[X]}$$

D'après le résultat sur le degré d'un polynôme dérivé (C16.97), le polynôme $P-Q$ est constant. Il existe donc un scalaire $\lambda \in \mathbf{K}$ tel que

$$(\star\star\star) \quad P = \lambda + \sum_{k=0}^{n} \frac{\widetilde{P^{(k+1)}}(a)}{(k+1)!}(X-a)^{k+1} = \lambda + \sum_{k=1}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^{k}$$

En évaluant au point a (eval_a est un morphisme de $\mathbf{K}$-algèbres, cf. C16.64), il vient

$$\widetilde{P}(a) = \lambda + \sum_{k=1}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!} 0^k = \lambda$$

d'où $\lambda = \widetilde{P}(a) = \widetilde{P}^{(0)}(a) = \dfrac{\widetilde{P}^{(0)}(a)}{0!}(X-a)^0$. L'identité $(\star\star\star)$ se réécrit alors

$$P = \frac{\widetilde{P}^{(0)}(a)}{0!}(X-a)^0 + \sum_{k=1}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^{k} = \sum_{k=0}^{n+1} \frac{\widetilde{P^{(k)}}(a)}{k!}(X-a)^{k}$$

Exemple C16.103 — Soit $P \in X^4 + X^3 + X^2 + X + 1$. Nous calculons

$$\begin{array}{rcllrcl} & & & & P^{(0)}(1) & = & 5 \\ P^{(1)} & = & 4X^3+3X^2+2X+1 & \text{et} & P^{(1)}(1) & = & 10 \\ P^{(2)} & = & 12X^2+6X+2 & \text{et} & P^{(2)}(1) & = & 20 \\ P^{(3)} & = & 24X+6 & \text{et} & P^{(3)}(1) & = & 30 \\ P^{(4)} & = & 24 & \text{et} & P^{(4)}(1) & = & 24 \end{array}$$

D'après la formule de Taylor exacte dans $\mathbf{K}[X]$ (cf. C16.102)

$$P = 5 + 10\,(X-1) + 20\,\frac{(X-1)^2}{2} + 30\,\frac{(X-1)^3}{6} + 24\,\frac{(X-1)^4}{24} = 5 + 10\,(X-1) + 10\,(X-1)^2 + 5\,(X-1)^3 + (X-1)^4$$

Exercice C16.104 — Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{K}$. Démontrer que l'application

$$\varphi \left| \begin{array}{ccc} \mathbf{K}_n[X] & \longrightarrow & \mathbf{K}^{n+1} \\ P & \longmapsto & \left(\widetilde{\left(P^{(0)}\right)}(a), \widetilde{\left(P^{(1)}\right)}(a), \widetilde{\left(P^{(2)}\right)}(a), \ldots, \widetilde{\left(P^{(n)}\right)}(a)\right) \end{array} \right.$$

est bijective et expliciter son application réciproque.

Théorème C16.105 (caractérisation de l'ordre de multiplicité d'une racine via les dérivées)
Soient $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$ et $\alpha \in \mathrm{Spec}_{\mathbf{K}}(P)$. L'ensemble $\left\{k \in \mathbf{N}^* \ : \ \widetilde{P^{(k)}}(\alpha) \neq 0_{\mathbf{K}}\right\}$ possède un minimum et

$$\mathrm{mult}(\alpha, P) = \min\left\{k \in \mathbf{N}^* \ : \ \widetilde{P^{(k)}}(\alpha) \neq 0_{\mathbf{K}}\right\}$$

La multiplicité de la racine α de P est donc le premier rang k où le polynôme dérivé itéré $P^{(k)}$ prend une valeur non nulle en α.

Démonstration — • La formule de Taylor exacte dans $\mathbf{K}[X]$ appliquée à P au point α livre

$$(\star) \quad P = \sum_{k=0}^{+\infty} \frac{\widetilde{P^{(k)}}(\alpha)}{k!}(X-\alpha)^{k} = \sum_{k=1}^{+\infty} \frac{\widetilde{P^{(k)}}(\alpha)}{k!}(X-\alpha)^{k} \qquad [\alpha \text{ est racine de } P]$$

De la non-nullité de P et de $(\star)$ nous déduisons que la partie

$$I := \left\{ k \in \mathbf{N}^* \; : \; \widetilde{P^{(k)}}(\alpha) \neq 0_{\mathbf{K}} \right\}$$

de $\mathbf{N}^*$ est non vide. D'après l'axiome du bon ordre, I possède un minimum. Posons

$$\nu := \min(I) \in \mathbf{N}^*$$

et démontrons que $\nu = \operatorname{mult}(\alpha, P)$, i.e. que $(X-\alpha)^\nu$ divise P et $(X-\alpha)^{\nu+1}$ ne divise pas P.

- D'après la définition de ν, l'identité $(\star)$ se réécrit

$$(\star\star) \qquad P = \sum_{k=\nu}^{+\infty} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^k = (X-\alpha)^\nu \underbrace{\sum_{k=\nu}^{+\infty} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} (X-\alpha)^{k-\nu}}_{=:Q \in \mathbf{K}[X]}$$

De la factorisation $(\star\star)$ nous déduisons que $(X-\alpha)^\nu$ divise P.

- Démontrons que $(X-\alpha)^{\nu+1}$ ne divise pas P, en raisonnant par l'absurde. Supposons donc qu'il existe un polynôme R de $\mathbf{K}[X]$ tel que

$$(\star\star\star) \qquad P = (X-\alpha)^{\nu+1} R$$

De $(\star\star)$, $(\star\star\star)$ et de la régularité de $\mathbf{K}[X]$ (conséquence de son intégrité), nous déduisons

$$(X-\alpha) R = Q$$

puis, en évaluant en α

$$0_{\mathbf{K}} = \widetilde{Q}(\alpha) = \sum_{k=\nu}^{+\infty} \frac{\widetilde{P^{(k)}}(\alpha)}{k!} 0_{\mathbf{K}}^{k-\nu} = \frac{\widetilde{P^{(\nu)}}(\alpha)}{\nu!} \qquad [0_{\mathbf{K}}^0 = 1_{\mathbf{K}}]$$

ce qui contredit $\nu \in I$.

Exemple C16.106 — Soit $P := X^5 + 7X^4 + 19X^3 + 26X^2 + 20X + 8$. Nous calculons

$$\begin{array}{lllllll} & & & & P^{(0)}(-2) & = & 0 \\ P^{(1)} & = & 5X^4 + 28X^3 + 57X^2 + 52X + 20 & \text{et} & P^{(1)}(-2) & = & 0 \\ P^{(2)} & = & 20X^3 + 84X^2 + 114X + 52 & \text{et} & P^{(2)}(-2) & = & 0 \\ P^{(3)} & = & 60X^2 + 168X + 114 & \text{et} & P^{(3)}(-2) & = & 18 \end{array}$$

Ainsi -2 est racine de P et $\operatorname{mult}(-2, P) = 3$.