

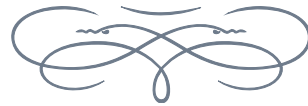
M P

Lycée Chrestien de Troyes

Mathématique



Chapitre 6 Polynômes



David BLOTTIÈRE

Table des matières

1	Rappels sur la construction de la \mathbf{K}-algèbre des polynômes à coefficients dans \mathbf{K}	3
1.1	L'addition $+$ sur $\mathbf{K}^{(\mathbf{N})}$	3
1.2	La multiplication par un scalaire \cdot sur $\mathbf{K}^{(\mathbf{N})}$	3
1.3	La multiplication interne \times sur $\mathbf{K}^{(\mathbf{N})}$	3
1.4	L'élément X de $\mathbf{K}^{(\mathbf{N})}$	4
1.5	La base canonique de $\mathbf{K}^{(\mathbf{N})}$	4
1.6	Notion de polynôme et l'ensemble $\mathbf{K}[X]$	4
1.7	Écriture d'un polynôme comme combinaison linéaire de puissances de X	4
1.8	Coefficients d'un polynôme à coefficients dans \mathbf{K}	5
1.9	Expression des opérations sur les polynômes, écrits comme combinaisons linéaires de puissances de X	5
1.9.1	Addition $+$	5
1.9.2	Multiplication par un scalaire	5
1.9.3	Multiplication interne \times	5
1.9.4	Composition \circ	6
1.10	Synthèse sur la structure de l'ensemble des polynômes à coefficients dans \mathbf{K}	6
2	Degré	7
3	Division euclidienne	9
4	Polynôme dérivé	10
5	Racines d'un polynômes	16
6	Idéaux de $\mathbf{K}[X]$	25
6.1	Idéal d'un anneau commutatif	25
6.2	Exemples d'idéaux de $\mathbf{K}[X]$	25
6.3	Description des idéaux de $\mathbf{K}[X]$	26
7	PGCD et PPCM	27
7.1	Notions de PGCD et de PPCM	27
7.2	Primalité relative	28
7.3	Une méthode de calcul du PGCD et du PPCM	29
8	Décomposition d'un polynôme en produit d'irréductibles	31
8.1	Notion de polynôme irréductible sur un corps	31
8.2	Décomposition d'un polynôme en produit de polynômes irréductibles	32
8.3	Irréductibles de $\mathbf{C}[X]$ et irréductibles de $\mathbf{R}[X]$	34
8.4	Décomposition en produit d'irréductibles dans $\mathbf{C}[X]$	34
8.5	Décomposition en produit d'irréductibles dans $\mathbf{R}[X]$	35
9	Une sélection d'exercices	36

1 Rappels sur la construction de la \mathbf{K} -algèbre des polynômes à coefficients dans \mathbf{K}

C6.1. Notation. — La lettre \mathbf{K} désigne un sous-corps de \mathbf{C} . 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. :

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

1.1 L'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 :

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

On définit ainsi une application :

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

On vérifie alors que $(\mathbf{K}^{(\mathbf{N})}, +)$ 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 :

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

1.2 La multiplication par un scalaire \cdot 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 $(\lambda a_n)_{n \in \mathbf{N}}$ est presque nulle et on pose :

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

On définit ainsi une application :

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

On vérifie alors que $(\mathbf{K}^{(\mathbf{N})}, +, \cdot)$ est un \mathbf{K} -espace vectoriel.

1.3 La 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 $\left(\sum_{k=0}^n a_k b_{n-k} \right)_{n \in \mathbf{N}}$ est presque nulle et on pose :

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

On définit ainsi une application :

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

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

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

Comme on vérifie de plus :

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

pour toutes suites $(a_n)_{n \in \mathbb{N}}$ et $(b_n)_{n \in \mathbb{N}}$ presque nulles d'éléments de \mathbf{K} et tout scalaire λ , $(\mathbf{K}^{(\mathbb{N})}, +, \times, \cdot)$ est une \mathbf{K} -algèbre.

1.4 L'élément X de $\mathbf{K}^{(\mathbb{N})}$

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. :

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

La suite X est presque nulle et on calcule ses puissances (à l'aide d'un raisonnement par récurrence) pour trouver :

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

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

1.5 La base canonique de $\mathbf{K}^{(\mathbb{N})}$

La famille $(X^i)_{i \in \mathbb{N}}$ forme une base de $\mathbf{K}^{(\mathbb{N})}$, nommée base canonique. Si $(a_n)_{n \in \mathbb{N}}$ est un élément de $\mathbf{K}^{(\mathbb{N})}$, alors :

$$(a_n)_{n \in \mathbb{N}} = \sum_{i=1}^{+\infty} a_i \cdot X^i$$

Notons que, la suite $(a_n)_{n \in \mathbb{N}}$ étant presque nulle, la somme précédente est une somme **finie**.

1.6 Notion de polynôme et l'ensemble $\mathbf{K}[X]$

L'ensemble $\mathbf{K}^{(\mathbb{N})}$ sera plutôt noté $\mathbf{K}[X]$. 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} .

1.7 Écriture d'un polynôme comme combinaison linéaire de puissances de X

Puisque $(X^i)_{i \in \mathbb{N}}$ est une base de $\mathbf{K}[X]$, un polynôme P à coefficients dans \mathbf{K} s'écrit d'une unique manière sous la forme

$$(\star) \quad P = \sum_{i=0}^{+\infty} a_i X^i$$

où $(a_i)_{i \in \mathbb{N}} \in \mathbf{K}^{(\mathbb{N})}$, i.e. où $(a_i)_{i \in \mathbb{N}}$ est une famille presque nulle d'éléments de \mathbf{K} . Puisque toute partie finie de \mathbb{N} est incluse dans $\llbracket 0, n \rrbracket$ pour un certain $n \in \mathbb{N}$, P peut se réécrire sous la forme

$$(\star\star) \quad P = \sum_{i=0}^n a_i X^i .$$

C6.2. Remarque. — Dans la suite, nous écrivons les polynômes sous l'une des formes (\star) ou $(\star\star)$, et plus comme des suites presque nulles d'éléments de \mathbf{K} .

1.8 Coefficients d'un polynôme à coefficients dans \mathbf{K}

Les $a_i, i \in \mathbf{N}$, apparaissant dans l'écriture (\star) sont uniques et on pose :

$$\forall i \in \mathbf{N} \quad [P]_i := a_i.$$

On nomme coefficient d'indice $i, i \in \mathbf{N}$, le scalaire $[P]_i := a_i$. Ainsi la famille $([P]_i)_{i \in \mathbf{N}}$ est presque nulle et

$$P = \sum_{i=0}^{+\infty} [P]_i X^i.$$

1.9 Expression des opérations sur les polynômes, écrits comme combinaisons linéaires de puissances de X

1.9.1 Addition +

Pour tout $(P, Q) \in \mathbf{K}[X]^2$

$$P + Q := \sum_{i=0}^{+\infty} ([P]_i + [Q]_i) X^i.$$

On a donc

$$\forall i \in \mathbf{N} \quad [P + Q]_i = [P]_i + [Q]_i.$$

1.9.2 Multiplication par un scalaire .

Pour tout $\lambda \in \mathbf{K}$, pour tout $P \in \mathbf{K}[X]$

$$\lambda P = \sum_{i=0}^{+\infty} \lambda [P]_i X^i.$$

On a donc

$$\forall i \in \mathbf{N} \quad [\lambda P]_i = \lambda [P]_i.$$

1.9.3 Multiplication interne \times

Pour tout $(P, Q) \in \mathbf{K}[X]^2$

$$PQ := \sum_{i=0}^{+\infty} \left(\sum_{j=0}^i [P]_j [Q]_{i-j} \right) X^i.$$

On a donc

$$\forall i \in \mathbf{N} \quad [PQ]_i = \sum_{j=0}^i [P]_j [Q]_{i-j}.$$

1.9.4 Composition ◦

Soit $P = \sum_{i=0}^n a_i X^i$ et Q dans $\mathbf{K}[X]$. Alors

$$P \circ Q = \sum_{i=0}^n a_i Q^i.$$

1.10 Synthèse sur la structure de l'ensemble des polynômes à coefficients dans \mathbf{K}

C6. 3. THÉORÈME (STRUCTURES SUR L'ENSEMBLE DES POLYNÔMES À COEFFICIENTS DANS \mathbf{K}). — L'ensemble de tous les polynômes à coefficients dans \mathbf{K} est noté $\mathbf{K}[X]$.

1. $(\mathbf{K}[X], +, \cdot)$ est un \mathbf{K} -espace vectoriel dont $(X^i)_{i \in \mathbf{N}}$ est une base.
2. $(\mathbf{K}[X], +, \times)$ est un anneau commutatif.
3. $(\mathbf{K}[X], +, \times, \cdot)$ est une \mathbf{K} -algèbre.

C6. 4. Remarque (Formule du binôme de Newton dans $\mathbf{K}[X]$). — Comme $\mathbf{K}[X]$ est un anneau commutatif, la formule du binôme de Newton vaut dans $\mathbf{K}[X]$, sans hypothèse sur les éléments dont on veut développer une puissance de leur somme.

C6. 5. Exercice. —

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

C6. 6. Exercice (Formule des comités). —

1. Démontrer de deux manières la « formule des comités »

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

l'une combinatoire, l'autre à l'aide de la formule du binôme de Newton.

2. Proposer une généralisation de la formule énoncée en Q1.

2 Degré

C6. 7. DÉFINITION (DEGRÉ). — Soit

$$(*) \quad P = \sum_{i=0}^{+\infty} a_i X^i \in \mathbf{K}[X].$$

1. Si dans $(*)$ tous les a_i , $i \in \mathbf{N}$, sont nuls alors P s'écrit simplement $P = 0$. On définit alors son degré par

$$\text{Deg}(0) = -\infty.$$

2. Si dans $(*)$ un des a_i , $i \in \mathbf{N}$, est non nul (i.e. si $P \neq 0$), alors l'ensemble $\{i \in \mathbf{N} : a_i \neq 0\}$ est une partie finie et non vide de \mathbf{N} . Elle possède donc un maximum et on définit le degré de P par

$$\text{Deg}(P) := \max(\{i \in \mathbf{N} : a_i \neq 0\}).$$

Le degré de P est donc le plus grand exposant de X qui apparaît avec un coefficient non nul, dans $(*)$.

C6. 8. Remarque. — Le degré d'un polynôme est un élément de l'ensemble $\mathbf{N} \cup \{-\infty\}$ et :

$$\forall P \in \mathbf{K}[X], \quad P = 0 \iff \text{Deg}(P) = -\infty.$$

C6. 9. DÉFINITION (COEFFICIENT DOMINANT ET POLYNÔME UNITAIRE). — Soit $P = \sum_{i=0}^{+\infty} a_i X^i \in$

$\mathbf{K}[X]$. On suppose P non nul.

1. Le coefficient $[P]_{\text{Deg}(P)}$, qui est par définition non nul, est appelé coefficient dominant de P . On le note $\text{Dom}(P)$.
2. Si $\text{Dom}(P) = 1$, alors P est dit unitaire.

C6. 10. Remarque (Polynôme normalisé). — Si $P \in \mathbf{K}[X] \setminus \{0\}$, alors le polynôme

$$\widehat{P} := \frac{1}{\text{Dom}(P)} P$$

est unitaire. On dit parfois que ce dernier polynôme est obtenu en normalisant le polynôme P ou que le polynôme $\widehat{P} := \frac{1}{\text{Dom}(P)} P$ est le polynôme normalisé de P .

C6. 11. PROPOSITION (PROPRIÉTÉS DU DEGRÉ). — On étend la relation d'ordre usuelle \leq et l'addition $+$ sur \mathbf{N} à $\mathbf{N} \cup \{-\infty\}$ en posant, pour tout $(n, m) \in (\mathbf{N} \cup \{-\infty\})^2$:

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

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

Soit $(P, Q) \in \mathbf{K}[X]^2$.

1. $\text{Deg}(P + Q) \leq \max(\text{Deg}(P), \text{Deg}(Q))$, avec égalité si et seulement si l'une des trois propriétés suivantes est vraie
 - (a) $\text{Deg}(P) \neq \text{Deg}(Q)$
 - (b) $\text{Deg}(P) = \text{Deg}(Q) = -\infty$
 - (c) $\text{Deg}(P) = \text{Deg}(Q) \neq -\infty$ et la somme des coefficients dominants de P et Q n'est pas nulle.
2. $\text{Deg}(PQ) = \text{Deg}(P) + \text{Deg}(Q)$.

C6. 12. PROPOSITION (INTÉGRITÉ DE $\mathbf{K}[X]$). — L'anneau $(\mathbf{K}[X], +, \times)$ est intègre.

C6. 13. Exercice (Coefficient dominant d'un produit de polynômes). — Soient $P, Q \in \mathbf{K}[X]$ des polynômes non nuls. Démontrer : $\text{Dom}(PQ) = \text{Dom}(P) \text{ Dom}(Q)$.

C6. 14. Exercice (Degré et coefficient dominant d'une composée de polynômes). — Soit $(P, Q) \in \mathbf{K}[X]^2$. On suppose que $\text{Deg}(Q) \geq 1$.

1. Démontrer que : $\text{Deg}(P \circ Q) = \text{Deg}(P) \text{ Deg}(Q)$.
2. Conjecturer puis démontrer un résultat concernant $\text{Dom}(P \circ Q)$.

C6. 15. Exercice (Quelques équations dans $\mathbf{K}[X]$). —

1. Résoudre $P \circ P = P$ d'inconnue $P \in \mathbf{K}[X]$.
2. Résoudre $Q^2 = XP^2$ d'inconnue $(P, Q) \in \mathbf{K}[X]^2$.
3. Résoudre $P(X^2) = X^2P$ d'inconnue $P \in \mathbf{K}[X]$.
4. Donner une condition nécessaire et suffisante sur $P \in \mathbf{K}[X]$ pour qu'il existe $Q \in \mathbf{K}[X]$ tel que $P \circ Q = X$.

C6. 16. Question. — Soit $n \in \mathbf{N}$. L'ensemble $\{P \in \mathbf{K}[X] : \text{Deg}(P) = n\}$ est-il un sous-espace vectoriel de $\mathbf{K}[X]$?

C6. 17. DÉFINITION ($\mathbf{K}_n[X]$). — Pour tout $n \in \mathbf{N}$ on pose

$$\mathbf{K}_n[X] := \{P \in \mathbf{K}[X] : \text{Deg}(P) \leq n\}.$$

C6. 18. THÉORÈME (STRUCTURE SUR $\mathbf{K}_n[X]$). — Soit $n \in \mathbf{N}$. $\mathbf{K}_n[X]$ est un sous-espace vectoriel de $\mathbf{K}[X]$ dont $(1, X, \dots, X^n)$ est une base. Sa dimension est donc $n + 1$.

C6. 19. Exercice ($\mathbf{K}[X]$ n'est pas de dimension finie). — Justifier $\bigcup_{n \in \mathbf{N}} \mathbf{K}_n[X] = \mathbf{K}[X]$ et en déduire que $\mathbf{K}[X]$ n'est pas de dimension finie.

C6. 20. Exercice (Version forte du théorème des degrés échelonnés). — Soit $(P_i)_{i \in \mathbf{N}}$ une famille de polynômes de $\mathbf{K}[X]$ telle que pour tout $i \in \mathbf{N}$, $\text{deg}(P_i) = i$. Démontrer que la famille $(P_i)_{i \in \mathbf{N}}$ est une base de $\mathbf{K}[X]$.

3 Division euclidienne

C6. 21. THÉORÈME (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

$$\left\{ \begin{array}{l} A = BQ + R \\ \text{et} \\ \text{Deg}(R) < \text{Deg}(B). \end{array} \right.$$

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

C6. 22. Exercice. — Effectuer la division euclidienne de $A := X^5 + X^4 + X^3 + X^2 + X + \alpha$ par $B := X^2 + X + 1$, où $\alpha \in \mathbf{K}$.

C6. 23. DÉFINITION (DIVISIBILITÉ). — Soit $(A, B) \in \mathbf{K}[X]^2$. On dit que A est divisible par B , ou que B divise A , s'il existe $Q \in \mathbf{K}[X]$ tel que $A = BQ$.

C6. 24. Exercice. — 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 . Quel relation existe-t-il entre A et B ?
4. On suppose que B est non nul. Démontrer :

$$A \text{ divise } B \implies \text{Deg}(A) \leq \text{Deg}(B) .$$

La réciproque est-elle vraie?

C6. 25. PROPOSITION (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.

C6. 26. Exercice. — 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 $B := X^2 + X + 1$.

C6. 27. Exercice. — 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 $\deg(A) < \deg(B)$.

C6. 28. Exercice. —

1. 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 $P(a)$.
2. 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 $P(b)$.

C6. 29. Exercice. — Soit $B \in \mathbf{K}[X]$ de degré $n \geq 1$. Soit

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

Démontrer que f est une application bien définie, qui est linéaire et surjective. Est-elle injective?

4 Polynôme dérivé

C6. 30. DÉFINITION (POLYNÔME DÉRIVÉ ET POLYNÔMES DÉRIVÉS ITÉRÉS). — Soit $P = \sum_{k=0}^n a_k X^k \in \mathbf{K}[X]$, où $n \in \mathbf{N}$.

1. Le polynôme dérivé P' de P est défini par

$$P' := \begin{cases} 0 & \text{si } n = 0 \\ \sum_{k=1}^n k a_k X^{k-1} & \text{si } n \geq 1. \end{cases}$$

2. On définit par récurrence les polynômes dérivés itérés (ou successifs) en posant

$$P^{(0)} = P \quad \text{et} \quad \forall k \in \mathbf{N}, P^{(k+1)} = (P^{(k)})'.$$

C6. 31. REMARQUE (DEGRÉ DU POLYNÔME DÉRIVÉ). — Soit $P \in \mathbf{K}[X]$. Alors

$$\deg(P') = \begin{cases} -\infty & \text{si } \deg P \leq 0 \\ \text{Deg}(P) - 1 & \text{si } \deg P \geq 1. \end{cases}$$

C6. 32. PROPOSITION (LINÉARITÉ DE LA DÉRIVATION DE POLYNÔMES). — L'application

$$D \quad \left| \begin{array}{ccc} \mathbf{K}[X] & \longrightarrow & \mathbf{K}[X] \\ P & \longmapsto & P' \end{array} \right.$$

est linéaire, surjective, de noyau $\mathbf{K}_0[X]$.

C6. 33. THÉORÈME (DÉRIVÉES DE PRODUITS DE POLYNÔMES ET FORMULE DE LEIBNIZ). —

1. Soient $P, Q \in \mathbf{K}[X]$. Alors :

$$(PQ)' = P'Q + PQ'$$

2. Soit n un nombre entier naturel supérieur ou égal à 2. Soient $P_1, P_2, \dots, P_n \in \mathbf{K}[X]$.

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

3. Soient $P, Q \in \mathbf{K}[X]$. Pour tout $n \in \mathbf{N}^*$:

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

Cette dernière identité est appelée **formule de Leibniz**.

Démonstration. 1. Les deux applications :

$$f \quad \left| \begin{array}{ccc} \mathbf{K}[X] \times \mathbf{K}[X] & \longrightarrow & \mathbf{K}[X] \\ (P, Q) & \longmapsto & (PQ)' \end{array} \right. \quad \text{et} \quad g \quad \left| \begin{array}{ccc} \mathbf{K}[X] \times \mathbf{K}[X] & \longrightarrow & \mathbf{K}[X] \\ (P, Q) & \longmapsto & P'Q + PQ' \end{array} \right.$$

sont bilinéaires (symétriques). Ainsi, pour tout $(P, Q) \in \mathbf{K}[X] \times \mathbf{K}[X]$:

$$f(P, Q) = f \left(\sum_{i=0}^{+\infty} [P]_i X^i, \sum_{j=0}^{+\infty} [Q]_j X^j \right) = \sum_{i=0}^{+\infty} \sum_{j=0}^{+\infty} [P]_i [Q]_j f(X^i, X^j)$$

et

$$g(P, Q) = g\left(\sum_{i=0}^{+\infty} [P]_i X^i, \sum_{j=0}^{+\infty} [Q]_j X^j\right) = \sum_{i=0}^{+\infty} \sum_{j=0}^{+\infty} [P]_i [Q]_j g(X^i, X^j) .$$

Pour démontrer que f et g coïncident pour tout $(P, Q) \in \mathbf{K}[X] \times \mathbf{K}[X]$, il suffit donc de prouver que, pour tout $(i, j) \in \mathbf{N}^2$, $f(X^i, X^j) = g(X^i, X^j)$. Nous calculons :

$$f(X^i, X^j) := (X^{i+j})' = (i+j) X^{i+j-1}$$

et

$$g(X^i, X^j) := (X^i)' X^j + X^i (X^j)' = i X^{i+j-1} + j X^{i+j-1} = (i+j) X^{i+j-1}$$

pour conclure.

2. Nous raisonnons par récurrence sur le nombre de polynômes en jeu.

Pour tout $n \in \mathbf{N}_{\geq 2}$, nous définissons le prédicat $\mathcal{P}(n)$ par :

$$\mathcal{P}(n) := \left| \text{Pour tout } (P_1, P_2, \dots, P_n) \in \mathbf{K}[X]^n, \left(\prod_{i=1}^n P_i\right)' = \sum_{j=1}^n P_j' \left(\prod_{\substack{i=1 \\ i \neq j}}^n P_i\right) \right.$$

Le prédicat $\mathcal{P}(2)$ est vrai, d'après la propriété 1.

Soit $n \in \mathbf{N}_{\geq 2}$ tel que $\mathcal{P}(n)$ est vrai. Soit $(P_1, P_2, \dots, P_n, P_{n+1}) \in \mathbf{K}[X]^{n+1}$. D'après la propriété 1 :

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

Grâce à l'hypothèse de récurrence, nous en déduisons :

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

En observant que le dernier terme égale $\sum_{j=1}^{n+1} P_j' \left(\prod_{\substack{i=1 \\ i \neq j}}^{n+1} P_i\right)$, nous pouvons conclure :

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

3. Nous raisonnons par récurrence sur l'ordre de dérivation, en mimant la démonstration par récurrence de la formule du binôme de Newton vue en classe.

Pour tout $n \in \mathbf{N}^*$, nous définissons le prédicat $\mathcal{P}(n)$ par :

$$\mathcal{P}(n) := \left| (PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)} \right.$$

Le prédicat $\mathcal{P}(1)$ est vrai, d'après la propriété 1.

Soit $n \in \mathbf{N}^*$ tel que $\mathcal{P}(n)$ est vrai. Par définition des dérivées itérées d'un polynôme, $(PQ)^{(n+1)} = ((PQ)^{(n)})'$. D'après l'hypothèse de récurrence, nous obtenons :

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

Grâce à la propriété 1 :

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

En remarquant que la première somme égale $\sum_{k=1}^{n+1} \binom{n}{k-1} P^{(k)} Q^{(n+1-k)}$, il vient :

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

Comme, pour tout $k \in \llbracket 1, n \rrbracket$, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ (relation de Pascal), $\binom{n}{n} = 1 = \binom{n+1}{n+1}$ et $\binom{n}{0} = 1 = \binom{n+1}{0}$, nous pouvons conclure :

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

Q.E.D.

C6. 34. *Lemme (Polynômes dérivés itérés de $(X - a)^k$).* — Soient $k \in \mathbf{N}^*$ et soit $\ell \in \mathbf{N}$. Soit $a \in \mathbf{K}$.

$$[(X - a)^k]^{(\ell)} = \begin{cases} \frac{k!}{(k - \ell)!} (X - a)^{k-\ell} & \text{si } \ell \leq k \\ 0 & \text{si } \ell > k . \end{cases}$$

Démonstration. • Pour tout $k \in \mathbf{N}^*$, on note $\mathcal{P}(k)$ le prédicat en la variable k suivant :

$$\forall \ell \in \mathbf{N}, \quad [(X - a)^k]^{(\ell)} = \begin{cases} \frac{k!}{(k - \ell)!} (X - a)^{k-\ell} & \text{si } \ell \leq k \\ 0 & \text{si } \ell > k . \end{cases}$$

- Initialisation à $k = 1$. Dans ce cas, $\mathcal{P}(k)$ s'écrit :

$$\forall \ell \in \mathbf{N}, \quad [X - a]^{(\ell)} = \begin{cases} X - a & \text{si } \ell = 0 \\ 1 & \text{si } \ell = 1 \\ 0 & \text{si } \ell > 0. \end{cases}$$

On a $[X - a]^{(0)} = X - a$ et $[X - a]' = 1$. Et comme $\deg(X - a) = 1$, pour tout $\ell > 1$, $[X - a]^{(\ell)} = 0$.
Donc $\mathcal{P}(1)$ est vraie.

- Hérédité. Supposons $\mathcal{P}(k)$ vraie pour un $k \in \mathbf{N}$ fixé et démontrons $\mathcal{P}(k + 1)$.
— Comme $\deg((X - a)^{k+1}) = k + 1$, pour tout $\ell > k + 1$:

$$[(X - a)^{k+1}]^{(\ell)} = 0.$$

— Soit $\ell \in \llbracket 0, k \rrbracket$. On remarque $(X - a)^{k+1} = (X - a)^k \times (X - a)$. D'après la formule de Leibniz :

$$(\star) \quad [(X - a)^{k+1}]^{(\ell)} = \sum_{i=0}^{\ell} \binom{\ell}{i} [(X - a)^k]^{(i)} [X - a]^{(\ell-i)}.$$

D'où

$$\begin{aligned} [(X - a)^{k+1}]^{(\ell)} &= \binom{\ell}{\ell} [(X - a)^k]^{(\ell)} (X - a) + \binom{\ell}{\ell-1} [(X - a)^k]^{(\ell-1)} \times 1 && \text{[initialisation]} \\ &= \frac{k!}{(k-\ell)!} (X - a)^{k-\ell} (X - a) + \ell \frac{k!}{(k+1-\ell)!} (X - a)^{k+1-\ell} && \text{[HR]} \\ &= \left(\frac{k!}{(k-\ell)!} + \ell \frac{k!}{(k+1-\ell)!} \right) (X - a)^{k+1-\ell} \\ &= \frac{(k+1)!}{(k+1-\ell)!} (X - a)^{k+1-\ell}. \end{aligned}$$

— Il reste le cas $\ell = k + 1$ à traiter. Dans ce cas (\star) se réécrit :

$$[(X - a)^{k+1}]^{(k+1)} = \sum_{i=0}^{k+1} \binom{k+1}{i} [(X - a)^k]^{(i)} [X - a]^{(k+1-i)}$$

et, grâce à l'initialisation et à l'hypothèse de récurrence, se simplifie :

$$\begin{aligned} [(X - a)^{k+1}]^{(k+1)} &= \binom{k+1}{k} [(X - a)^k]^{(k)} [X - a]^{(1)} \\ &= (k+1) k! \\ &= (k+1)! \\ &= \frac{(k+1)!}{(k+1-\ell)!} (X - a)^{k+1-\ell}. \end{aligned}$$

- Conclusion : d'après l'initialisation à $k = 1$, l'hérédité et l'axiome de récurrence, pour tout $k \in \mathbf{N}^*$, $\mathcal{P}(k)$ est vraie.

Q.E.D.

C6. 35. THÉORÈME (FORMULE DE TAYLOR EXACTE DANS $\mathbf{K}[X]$). — Soit $P \in \mathbf{K}[X]$ un polynôme de degré $n \in \mathbf{N}$. Soit $a \in \mathbf{K}$. Alors

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

Démonstration. La famille $((X - a)^k)_{k \in \llbracket 0, n \rrbracket}$ de polynômes de $\mathbf{K}_n[X]$ est libre car échelonnée en degré. Elle comporte $(n + 1) = \dim(\mathbf{K}_n[X])$ éléments. Elle forme donc une base de $\mathbf{K}_n[X]$. Ainsi existe-t-il $\lambda_0, \dots, \lambda_n \in \mathbf{K}$ tels que :

$$P = \sum_{k=0}^n \lambda_k (X - a)^k = \lambda_0 + \sum_{k=1}^n \lambda_k (X - a)^k .$$

- En évaluant en a , il vient :

$$\lambda_0 = P(a) = \frac{P^{(0)}(a)}{0!} .$$

- Soit $\ell \in \llbracket 1, n \rrbracket$. On dérive ℓ fois le polynôme P et on applique le lemme précédent pour obtenir :

$$\begin{aligned} P^{(\ell)} &= \sum_{k=0}^{\ell-1} \lambda_k [(X - a)^k]^{(\ell)} + \sum_{k=\ell}^n \lambda_k [(X - a)^k]^{(\ell)} \\ &= 0 + \sum_{k=\ell}^n \lambda_k \frac{k!}{(k - \ell)!} (X - a)^{k-\ell} \\ &= \lambda_\ell \ell! + \sum_{k=\ell+1}^n \lambda_k \frac{k!}{(k - \ell)!} (X - a)^{\overbrace{k-\ell}^{\geq 1}} . \end{aligned}$$

En évaluant en a , il vient :

$$P^{(\ell)}(a) = \lambda_\ell \ell!$$

et enfin $\lambda_\ell = \frac{P^{(\ell)}(a)}{\ell!}$.

Q.E.D.

C6. 36. Exercice. —

1. Trouver un endomorphisme $g \in \mathcal{L}(\mathbf{K}[X])$ tel que $D \circ g = \text{id}_{\mathbf{K}[X]}$.
2. Existe-t-il un endomorphisme $h \in \mathcal{L}(\mathbf{K}[X])$ tel que $h \circ D = \text{id}_{\mathbf{K}[X]}$?

C6. 37. Exercice. — Soit $n \in \mathbf{N}$. Soit $a \in \mathbf{K}$.

1. Justifier que la famille $\mathcal{B}_a := (1, X - a, (X - a)^2, \dots, (X - a)^n)$ est une base de $\mathbf{K}_n[X]$.
2. Soit $P \in \mathbf{K}_n[X]$. Quelles sont les coordonnées de P dans la base \mathcal{B}_a ?

5 Racines d'un polynômes

C6. 38. DÉFINITION (RACINE D'UN POLYNÔME). — Soit $P \in \mathbf{K}[X]$. Soit $\alpha \in \mathbf{K}$. On dit que α est une racine de P si $P(\alpha) = 0$.

C6. 39. DÉFINITION (SPECTRE D'UN POLYNÔME). — Soit $P \in \mathbf{K}[X]$. On note $\text{Spec}_{\mathbf{K}}(P)$ l'ensemble des racines de P dans \mathbf{K} , i.e. :

$$\text{Spec}_{\mathbf{K}}(P) := \{\alpha \in \mathbf{K} : P(\alpha) = 0\} .$$

C6. 40. Remarque (Spectre et extension de corps). — Soit $P \in \mathbf{K}[X]$. Soit \mathbf{L} un sur-corps de \mathbf{K} qui est un sous-corps de $\mathbf{C} : \mathbf{K} \subset \mathbf{L} \subset \mathbf{C}$. On note $\text{Spec}_{\mathbf{L}}(P)$ l'ensemble des racines de P (considéré comme polynôme à coefficients dans \mathbf{L}) dans \mathbf{L} :

$$\text{Spec}_{\mathbf{L}}(P) := \{\alpha \in \mathbf{L} : P(\alpha) = 0\} .$$

On a naturellement l'inclusion :

$$\text{Spec}_{\mathbf{K}}(P) \subset \text{Spec}_{\mathbf{L}}(P)$$

mais cette inclusion peut être stricte (cf. exercice ci-dessous).

C6. 41. Attention. — Le spectre d'un polynôme dépendant du corps dans lequel on s'autorise à considérer les racines, on prendra toujours garde à bien indiquer le corps en indice. On évitera en particulier la notation $\text{Spec}(P)$.

C6. 42. Exercice (Spectre réel et complexe de $X^n + X^{n-1} + \dots + X + 1$). — Soient $n \in \mathbf{N}^*$ et $P = \sum_{k=0}^n X^k$.

Déterminer $\text{Spec}_{\mathbf{R}}(P)$ et $\text{Spec}_{\mathbf{C}}(P)$.

C6. 43. PROPOSITION (CRITÈRE POUR ÊTRE UNE RACINE VIA LA DIVISIBILITÉ). — Soit $P \in \mathbf{K}[X]$. Soit $\alpha \in \mathbf{K}$. Alors

$$\alpha \text{ est racine de } P \text{ dans } \mathbf{K} \iff (X - \alpha) \text{ divise } P \text{ dans } \mathbf{K}[X].$$

C6. 44. PROPOSITION (FACTORISATION D'UN POLYNÔME POSSÉDANT n RACINES DEUX-À-DEUX DISTINCTES). — Soit $P \in \mathbf{K}[X]$. Soient $\alpha_1, \dots, \alpha_n$ des éléments de \mathbf{K} deux-à-deux distincts. Alors

$$\alpha_1, \dots, \alpha_n \text{ sont racines de } P \text{ dans } \mathbf{K} \iff \prod_{k=1}^n (X - \alpha_k) \text{ divise } P \text{ dans } \mathbf{K}[X].$$

C6. 45. COROLLAIRE (NOMBRE MAXIMAL DE RACINES D'UN POLYNÔME NON NUL). — Soit $P \in \mathbf{K}[X]$. Si $P \neq 0$ alors P possède au plus $\text{Deg}(P)$ racines dans \mathbf{K} .

Démonstration. Supposons P non nul et notons $n := \text{Deg}(P) \in \mathbf{N}$. Raisonnons par l'absurde et supposons que P possède au moins $(n + 1)$ racines deux-à-deux distinctes $\alpha_1, \dots, \alpha_{n+1}$ dans \mathbf{K} . D'après la proposition précédente, il existe $Q \in \mathbf{K}[X]$ tel que

$$P = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n)(X - \alpha_{n+1})Q.$$

Le polynôme P étant non nul, Q l'est également. Donc $\text{Deg}(P) = n + 1 + \text{deg}(Q)$ et $\text{deg}(Q) \geq 0$. Ainsi $\text{Deg}(P) \geq n + 1$. Contradiction. Q.E.D.

C6. 46. COROLLAIRE (CRITÈRE DE NULLITÉ POUR UN POLYNÔME). — Soit n un nombre entier naturel. Soit P un polynôme de degré inférieur ou égal à n . Si P possède au moins $n + 1$ racines deux-à-deux distinctes, alors $P = 0$.

C6. 47. PROPOSITION (POLYNÔME VERSUS FONCTION POLYNOMIALE). — Si $P \in \mathbf{K}[X]$, on lui associe la fonction

$$\tilde{P} \quad \left| \begin{array}{l} \mathbf{K} \longrightarrow \mathbf{K} \\ x \longmapsto P(x) \end{array} \right.$$

L'application

$$\varphi \quad \left| \begin{array}{l} \mathbf{K}[X] \longrightarrow \mathcal{F}(\mathbf{K}, \mathbf{K}) \\ P \longmapsto \tilde{P} \end{array} \right.$$

est injective.

Démonstration. L'application φ est clairement linéaire. Montrons que son noyau est réduit au polynôme nul.

Soit $P \in \mathbf{K}[X]$ tel que $\tilde{P} = 0$. Alors tout élément de \mathbf{K} est racine de P . Comme \mathbf{K} est un sous-corps de \mathbf{C} , il contient \mathbf{Q} et est donc infini. Comme P a une infinité de racines, il est nul (cf. Corollaire précédent). Q.E.D.

C6. 48. Remarque (Identification entre polynôme et fonction polynomiale). — Une fonction de \mathbf{K} dans \mathbf{K} est dite polynomiale si elle est égale à \tilde{P} , pour un $P \in \mathbf{K}[X]$. En d'autres termes les fonctions polynomiales sont celles qui sont dans l'image de l'application φ de la proposition précédente. L'application φ étant injective, on confondra parfois/souvent un polynôme $P \in \mathbf{K}[X]$ et la fonction polynomiale correspondante \tilde{P} .

C6. 49. Exercice (Quid des fonctions polynomiales sur les corps finis?). — Soit p un nombre premier. Les constructions élaborées jusqu'ici pour un sous-corps \mathbf{K} de \mathbf{C} s'appliquent *mutatis mutandis* au corps $\mathbf{Z}/p\mathbf{Z}$, que l'on note également \mathbf{F}_p . On peut donc considérer la \mathbf{F}_p -algèbre $\mathbf{F}_p[X]$ des polynômes à coefficients dans \mathbf{F}_p . Soit $P = X \in \mathbf{F}_p[X]$ et $Q = X^p \in \mathbf{F}_p[X]$. Comparer les deux applications

$$\hat{P} \quad \left| \begin{array}{l} \mathbf{F}_p \rightarrow \mathbf{F}_p \\ x \mapsto P(x) \end{array} \right. \quad \text{et} \quad \hat{Q} \quad \left| \begin{array}{l} \mathbf{F}_p \rightarrow \mathbf{F}_p \\ x \mapsto Q(x) \end{array} \right.$$

et commenter.

C6. 50. Exercice (Déterminant de Vandermonde). — Si $n \in \mathbf{N}_{\geq 2}$ et si $(\alpha_1, \dots, \alpha_n) \in \mathbf{K}^n$, on pose :

$$V(\alpha_1, \dots, \alpha_n) := \det \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \alpha_n \\ (\alpha_1)^2 & (\alpha_2)^2 & \dots & (\alpha_{n-1})^2 & (\alpha_n)^2 \\ \vdots & \vdots & & \vdots & \vdots \\ (\alpha_1)^{n-2} & (\alpha_2)^{n-2} & \dots & (\alpha_{n-1})^{n-2} & (\alpha_n)^{n-2} \\ (\alpha_1)^{n-1} & (\alpha_2)^{n-1} & \dots & (\alpha_{n-1})^{n-1} & (\alpha_n)^{n-1} \end{pmatrix} .$$

Le scalaire $V(\alpha_1, \dots, \alpha_n)$ désigne donc le déterminant de la matrice $\left((\alpha_j)^{i-1} \right)_{1 \leq i, j \leq n}$.

1. Soient $\alpha_1, \dots, \alpha_n$ des scalaires deux-à-deux distincts.

(a) Justifier que la fonction

$$P \quad \left| \begin{array}{l} \mathbf{K} \longrightarrow \mathbf{K} \\ x \longmapsto V(\alpha_1, \dots, \alpha_n, x) \end{array} \right.$$

est polynomiale et déterminer son coefficient devant x^n .

(b) En déduire que :

$$P = V(\alpha_1, \dots, \alpha_n) \prod_{k=1}^n (X - \alpha_k) .$$

2. Démontrer que pour tout $(\alpha_1, \dots, \alpha_n) \in \mathbf{K}^n$:

$$V(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) .$$

UN CORRIGÉ DE L'EXERCICE PRÉCÉDENT SUR LES DÉTERMINANTS DE VANDERMONDE. —

1. (a) Soit $x \in \mathbf{R}$.

$$V(\alpha_1, \dots, \alpha_n, x) := \det \underbrace{\begin{pmatrix} 1 & 1 & \dots & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} & \alpha_n & x \\ (\alpha_1)^2 & (\alpha_2)^2 & \dots & (\alpha_{n-1})^2 & (\alpha_n)^2 & x^2 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ (\alpha_1)^{n-2} & (\alpha_2)^{n-2} & \dots & (\alpha_{n-1})^{n-2} & (\alpha_n)^{n-2} & x^{n-2} \\ (\alpha_1)^{n-1} & (\alpha_2)^{n-1} & \dots & (\alpha_{n-1})^{n-1} & (\alpha_n)^{n-1} & x^{n-1} \\ (\alpha_1)^n & (\alpha_2)^n & \dots & (\alpha_{n-1})^n & (\alpha_n)^n & x^n \end{pmatrix}}_{M(\alpha_1, \dots, \alpha_n, x)}.$$

En développant ce déterminant par rapport à la dernière colonne, il vient :

$$V(\alpha_1, \dots, \alpha_n, x) = \sum_{i=1}^{n+1} (-1)^{i+n+1} x^{i-1} \det \left(M(\alpha_1, \dots, \alpha_n, x)_{i, n+1} \right)$$

où $M(\alpha_1, \dots, \alpha_n, x)_{i, n+1}$ est la matrice $n \times n$ obtenue en supprimant la i -ième ligne et la $(n+1)$ -ième colonne de la matrice $M(\alpha_1, \dots, \alpha_n, x)$. Comme seule la $(n+1)$ -ième colonne contient des x^k pour $1 \leq k \leq n$, la fonction P est polynomiale de degré inférieur ou égal à n et son coefficient devant x^n est :

$$(-1)^{n+1+n+1} \det \left(M(\alpha_1, \dots, \alpha_n, x)_{n+1, n+1} \right) = V(\alpha_1, \dots, \alpha_n).$$

(b) Soit $k \in \llbracket 1, n \rrbracket$. Si $x = \alpha_k$ alors la matrice $M(\alpha_1, \dots, \alpha_n, x)$ possède deux colonnes identiques. Par suite

$$P(\alpha_k) = \det \left(M(\alpha_1, \dots, \alpha_n, \alpha_k) \right) = 0.$$

Comme $\alpha_1, \dots, \alpha_n$ sont des racines deux-à-deux distinctes de P , qui est de degré inférieur ou égal à n , il existe $\lambda \in \mathbf{K}$ tel que :

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

Comme λ est le coefficient de P devant X^n , nous savons que

$$\lambda = V(\alpha_1, \dots, \alpha_n)$$

par la question 1.(a). Ainsi :

$$P = V(\alpha_1, \dots, \alpha_n, X) = V(\alpha_1, \dots, \alpha_n) \prod_{k=1}^n (X - \alpha_k).$$

2. Si deux des scalaires $\alpha_1, \dots, \alpha_n$ sont égaux, alors

$$V(\alpha_1, \dots, \alpha_n) = 0 = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) .$$

Nous démontrons, par récurrence que pour tout $n \in \mathbf{N}_{\geq 2}$:

$$\mathcal{P}(n) : \text{ pour tout } \alpha_1, \dots, \alpha_n \in \mathbf{K} \text{ deux-à-deux distincts, } V(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

- Initialisation à $n = 2$.

$$V(\alpha_1, \alpha_2) = \alpha_2 - \alpha_1 = \prod_{1 \leq i < j \leq 2} (\alpha_j - \alpha_i) .$$

- Hérité.

Soit $n \in \mathbf{N}_{\geq 2}$ tel que $\mathcal{P}(n)$ est vraie. Soient $\alpha_1, \dots, \alpha_n, \alpha_{n+1} \in \mathbf{K}$ deux-à-deux distincts. Alors :

$$\begin{aligned} V(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) &= V(\alpha_1, \dots, \alpha_n) \prod_{k=1}^n (\alpha_{n+1} - \alpha_k) \quad [\text{cf. question 1.(b)}] \\ &= \left[\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) \right] \left[\prod_{k=1}^n (\alpha_{n+1} - \alpha_k) \right] \quad [\text{hypothèse de récurrence}] \\ &= \prod_{1 \leq i < j \leq n+1} (\alpha_j - \alpha_i) . \end{aligned}$$

- Conclusion.

D'après l'initialisation à $n = 2$, l'hérité et l'axiome de récurrence, pour tout $n \in \mathbf{N}_{\geq 2}$, pour tout $\alpha_1, \dots, \alpha_n \in \mathbf{K}$ deux-à-deux distincts :

$$V(\alpha_1, \dots, \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

C6. 51. DÉFINITION (POLYNÔME DE $\mathbf{K}[X]$ SCINDÉ SUR \mathbf{K}). — Soit $P \in \mathbf{K}[X]$ tel que $\text{Deg}(P) \geq 1$. On dit que P est scindé sur \mathbf{K} s'il existe $\alpha_1, \dots, \alpha_n \in \mathbf{K}$ tels que

$$P = \text{Dom}(P) \prod_{k=1}^n (X - \alpha_k).$$

C6. 52. REMARQUE (SCINDAGE ET EXTENSION DE CORPS). — Soit $P \in \mathbf{K}[X]$. Soit \mathbf{L} un sur-corps de \mathbf{K} qui est un sous-corps de $\mathbf{C} : \mathbf{K} \subset \mathbf{L} \subset \mathbf{C}$. Le polynôme P (considéré comme polynôme à coefficients dans \mathbf{L}) peut être scindé sur \mathbf{L} , sans pour autant être scindé sur \mathbf{K} (cf. exemple ci-dessous).

C6. 53. Exemple. —

1. Le polynôme $X^2 - 2$ n'est pas scindé sur \mathbf{Q} , mais il est scindé sur \mathbf{R} .
2. Le polynôme $X^2 + 1$ n'est pas scindé sur \mathbf{R} , mais il est scindé sur \mathbf{C} .

C6. 54. Exercice. — Soit $a, b, c \in \mathbf{K}$, avec $a \neq 0$. Posons $P = aX^2 + bX + c \in \mathbf{K}[X]$.

1. Démontrer que si $\Delta := b^2 - 4ac$ est un carré dans \mathbf{K} , i.e. s'il existe $\delta \in \mathbf{K}$ tel que $\delta^2 = \Delta$, alors P est scindé sur \mathbf{K} .
2. Étudier la réciproque.

C6. 55. THÉORÈME (THÉORÈME DE D'ALEMBERT-GAUSS). — Tout polynôme de $\mathbf{C}[X]$ de degré supérieur ou égal à 1 possède au moins une racine dans \mathbf{C} .

C6. 56. COROLLAIRE (TOUT POLYNÔME DE $\mathbf{C}[X]$ EST SCINDÉ SUR \mathbf{C}). — Soit $P \in \mathbf{C}[X]$ tel que $\text{Deg}(P) \geq 1$. Alors P est scindé sur \mathbf{C} , i.e. il existe et $\alpha_1, \dots, \alpha_n \in \mathbf{C}$ tels que

$$P = \text{Dom}(P) \prod_{k=1}^n (X - \alpha_k).$$

Quitte à regrouper les α_k qui sont égaux et à ré-indexer les α_k , on peut écrire P sous la forme

$$P = \text{Dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

où

- $\alpha_1, \alpha_2, \dots, \alpha_r$ sont des racines complexes deux-à-deux distinctes de P
- n_1, n_2, \dots, n_r sont des entiers naturels non nuls.

C6. 57. DÉFINITION (ORDRE DE MULTIPLICITÉ D'UNE RACINE). — Soit $P \in \mathbf{K}[X]$ tel que $\text{Deg}(P) \geq 1$. Soit $\alpha \in \mathbf{K}$ une racine de P . L'ensemble

$$\{k \in \mathbf{N}^* : (X - \alpha)^k \text{ divise } P\}$$

est une partie de \mathbf{N} , non vide (α est racine de P donc $X - \alpha$ divise P) et majorée par $\text{Deg}(P)$ (un diviseur de P a un degré inférieur ou égal à $\text{Deg}(P)$). Il admet donc un maximum que l'on appelle ordre de multiplicité de α dans P et que l'on note $\text{Mult}(\alpha, P)$. On a donc

$$\text{Mult}(\alpha, P) := \max(\{k \in \mathbf{N}^* : (X - \alpha)^k \text{ divise } P\}).$$

La multiplicité de α dans P est donc le plus grand exposant $k \geq 1$ tel que $(X - \alpha)^k$ divise P .

C6. 58. Remarque. — Soit $P \in \mathbf{K}[X]$ tel que $\text{Deg}(P) \geq 1$, soit $\alpha \in \mathbf{K}$ une racine de P . Alors $1 \leq \text{Mult}(\alpha, P) \leq \text{Deg}(P)$.

C6. 59. THÉORÈME (CARACTÉRISATION DE L'ORDRE DE MULTIPLICITÉ D'UNE RACINE). — Soit $P \in \mathbf{K}[X]$ tel que $\text{Deg}(P) \geq 1$. Soit $\alpha \in \mathbf{K}$ une racine de P . Soit $n \in \llbracket 1, \text{Deg}(P) \rrbracket$. Les assertions suivantes sont équivalentes.

1. $n = \text{Mult}(\alpha, P)$
2. $(X - \alpha)^n$ divise P et $(X - \alpha)^{n+1}$ ne divise pas P .
3. Pour tout $k \in \llbracket 0, n - 1 \rrbracket$, $P^{(k)}(\alpha) = 0$ et $P^{(n)}(\alpha) \neq 0$.

Démonstration. Soit $\mathcal{E} := \{k \in \mathbf{N}^* : (X - \alpha)^k \text{ divise } P\}$. Ainsi, $\text{Mult}(\alpha, P) = \max(\mathcal{E})$.

$\boxed{1 \Rightarrow 2}$ Supposons $n = \text{Mult}(\alpha, P)$. Comme $n \in \mathcal{E}$, $(X - \alpha)^n$ divise P . Comme n est le plus grand élément de \mathcal{E} , $n + 1 \notin \mathcal{E}$, donc $(X - \alpha)^{n+1}$ ne divise pas P .

$\boxed{2 \Rightarrow 1}$ Supposons que $(X - \alpha)^n$ divise P et que $(X - \alpha)^{n+1}$ ne divise pas P . Comme $(X - \alpha)^n$ divise P , $n \in \mathcal{E}$, donc $n \leq \text{Mult}(\alpha, P)$. Montrons que $n \geq \text{Mult}(\alpha, P)$, ce qui livrera $n = \text{Mult}(\alpha, P)$, grâce à la précédente inégalité. Raisonnons par l'absurde. Si $n < \text{Mult}(\alpha, P)$, alors $n + 1 \leq \text{Mult}(\alpha, P)$. De $(X - \alpha)^{n+1}$ divise $(X - \alpha)^{\text{Mult}(\alpha, P)}$ et $(X - \alpha)^{\text{Mult}(\alpha, P)}$ divise P , nous déduisons $(X - \alpha)^{n+1}$ divise P . Contradiction.

$\boxed{2 \Rightarrow 3}$ Supposons $(X - \alpha)^n$ divise P et $(X - \alpha)^{n+1}$ ne divise pas P . D'après la formule de Taylor pour P en a , il vient

$$\begin{aligned} P &= \sum_{k=0}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^k = \underbrace{\sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!} (X - a)^k}_{\text{degré} < n} + \sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^k \\ &\stackrel{(*)}{=} (X - a)^n \underbrace{\left(\sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^{\overbrace{k-n}^{\geq 0}} \right)}_{\text{quotient}} + \underbrace{\sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!} (X - a)^k}_{\text{reste}} \end{aligned}$$

Comme $(X - a)^n$ divise P , le reste dans la division euclidienne de P par $(X - a)^n$ est nul. Donc

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

Comme $((X - a)^k)_{k \in \llbracket 0, n-1 \rrbracket}$ est une famille libre de polynômes (théorème des degrés échelonnés), $P^{(k)}(a) = 0$ pour tout $k \in \llbracket 0, n-1 \rrbracket$.

Il reste à voir que $P^{(n)}(a) \neq 0$. Pour cela, raisonnons par l'absurde et supposons $P^{(n)}(a) = 0$. Alors d'après l'identité (\star) , on ne peut avoir $n = \text{Deg}(P)$ (dans ce cas l'identité (\star) livrerait $P = 0$) donc $\text{Deg}(P) \geq n + 1$ et

$$P = \sum_{k=n+1}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^k = (X - a)^{n+1} \left(\sum_{k=n+1}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^{\overbrace{k-n-1}^{\geq 0}} \right)$$

Ainsi $(X - a)^{n+1}$ divise P . Contradiction.

$\boxed{3 \Rightarrow 2}$ Supposons que pour tout $k \in \llbracket 0, n-1 \rrbracket$, $P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$. Alors $\text{Deg}(P) \geq n$ (un polynôme de degré strictement inférieur à n a un polynôme dérivé n -ième nul) et la formule de Taylor pour P en a s'écrit

$$P = \sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^k \stackrel{(\star\star)}{=} (X - a)^n \left(\sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^{\overbrace{k-n}^{\geq 0}} \right).$$

Donc $(X - a)^n$ divise P . Il reste à voir que $(X - a)^{n+1}$ ne divise pas P . Pour cela, raisonnons par l'absurde et supposons $(X - a)^{n+1}$ divise P . Il existe donc $Q \in \mathbf{K}[X]$ tel que $P = (X - a)^n (X - a)Q$. De cette identité et de $(\star\star)$, nous déduisons

$$(X - a)^n \sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^{\overbrace{k-n}^{\geq 0}} = (X - a)^n (X - a)Q.$$

Comme $\mathbf{K}[X]$ est intègre, donc régulier, il vient

$$\sum_{k=n}^{\text{Deg}(P)} \frac{P^{(k)}(a)}{k!} (X - a)^{\overbrace{k-n}^{\geq 0}} = (X - a)Q.$$

En évaluant en a , nous obtenons $\frac{P^{(n)}(a)}{n!} = 0$, soit $P^{(n)}(a) = 0$. Contradiction.

Q.E.D.

C6. 60. Exercice (Ordre de multiplicité d'une racine d'un polynôme scindé). — Soit $P \in \mathbf{K}[X]$ un polynôme scindé sur \mathbf{K} , que l'on écrit

$$P = \text{Dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

où

- $\alpha_1, \alpha_2, \dots, \alpha_r$ sont des racines deux-à-deux distinctes de P dans \mathbf{K}

- n_1, n_2, \dots, n_r sont des entiers naturels non nuls.

Préciser l'ordre de multiplicité de la racine α_k de P , pour tout $k \in \llbracket 1, r \rrbracket$.

C6. 61. *Exercice (Racine complexe d'un polynôme à coefficients réels).* — Soit $P \in \mathbf{R}[X]$ et soit $\alpha \in \mathbf{C}$ une racine de P .

1. Démontrer que son conjugué $\bar{\alpha}$ est également racine de P .
2. Démontrer $\text{Mult}(\alpha, P) = \text{Mult}(\bar{\alpha}, P)$.

C6. 62. *Exercice (Relations coefficients racines pour un polynôme scindé).* — Soit $P = \sum_{k=0}^n a_k X^k \in \mathbf{K}[X]$ scindé sur \mathbf{K} . Notons $\alpha_1, \dots, \alpha_n$ les racines de P dans \mathbf{K} , comptées avec leurs ordres de multiplicité.

1. Que vaut la somme des racines?
2. Que vaut le produit des racines?

C6. 63. *Exercice.* — Démontrer qu'il n'existe pas de triplet (a, b, c) de nombres réels tels que

$$a + b + c = 6 \quad \text{et} \quad ab + ac + bc = 15.$$

C6. 64. *Exercice (Autour des racines de l'unité).* — Soit $n \in \mathbf{N}^*$. Déterminer les racines du polynôme $\sum_{k=1}^n X^k$ dans \mathbf{C} et en déduire la valeur de $\prod_{k=1}^n \sin\left(\frac{k\pi}{n+1}\right)$.

C6. 65. *Question.* — Que dire d'un polynôme $P \in \mathbf{C}[X]$ tel que $P(\mathbf{C}) \subset \mathbf{R}$?

6 Idéaux de $\mathbf{K}[X]$

6.1 Idéal d'un anneau commutatif

Soit $(A, +, \times)$ un anneau commutatif.

C6. 66. DÉFINITION (IDÉAL). — *Un idéal de A est une partie I de A , qui est un sous-groupe du groupe abélien $(A, +)$ i.e. :*

- (a) $0_A \in I$;
- (b) $\forall (x, y) \in I^2, \quad x + y \in I$;
- (c) $\forall x \in I, \quad -x \in I$;

et qui est absorbant, i.e. :

- (d) $\forall a \in A, \forall x \in I, \quad ax \in I$.

C6. 67. PROPOSITION (CARACTÉRISATION D'UN IDÉAL). — *Soit I une partie de A . Alors I est un idéal de A si et seulement si les trois propriétés suivantes sont vérifiées :*

- (A) I est non vide;
- (B) I est stable par somme tordue : $\forall (x, y) \in I^2, \quad x - y \in I$;
- (C) I est absorbant : $\forall a \in A, \forall x \in I, \quad ax \in I$.

C6. 68. PROPOSITION (OPÉRATIONS SUR LES IDÉAUX). — *Soit I_1, I_2, \dots, I_n des idéaux de A .*

1. $I_1 \cap I_2 \cap \dots \cap I_n$ est un idéal de A .
2. $I_1 + I_2 + \dots + I_n := \{x_1 + x_2 + \dots + x_n : (x_1, x_2, \dots, x_n) \in I_1 \times I_2 \times \dots \times I_n\}$ est un idéal de A .

6.2 Exemples d'idéaux de $\mathbf{K}[X]$

C6. 69. Exemple (Idéaux triviaux de $\mathbf{K}[X]$). — Les parties $\{0\}$ et $\mathbf{K}[X]$ sont des idéaux de $\mathbf{K}[X]$, appelés idéaux triviaux.

C6. 70. Exercice (Exemple fondamental d'idéal de $\mathbf{K}[X]$). —

1. Soit $A \in \mathbf{K}[X]$. Démontrer que l'ensemble des multiples de A

$$A\mathbf{K}[X] := \{PA : P \in \mathbf{K}[X]\}$$

est un idéal de $\mathbf{K}[X]$.

2. Soient A et B des polynômes de $\mathbf{K}[X]$. Donner une condition nécessaire et suffisante sur A et B pour que $A\mathbf{K}[X]$ soit inclus dans $B\mathbf{K}[X]$.

C6. 71. Exercice (Polynômes associés). — Soient $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. On dit que A et B sont associés s'il existe $\lambda \in \mathbf{K}^*$ tel que $A = \lambda B$. Démontrer :

$$A \text{ et } B \text{ sont associés} \iff A\mathbf{K}[X] = B\mathbf{K}[X].$$

C6. 72. Exercice. — Pour tout $a \in \mathbf{K}$, on note $Z(a)$ l'ensemble des polynômes s'annulant en a :

$$Z(a) := \{P \in \mathbf{K}[X] : P(a) = 0\}.$$

1. Démontrer que $Z(a)$ est un idéal de $\mathbf{K}[X]$.
2. Soient a et b des éléments distincts de \mathbf{K} . Démontrer que $Z(a) + Z(b) = \mathbf{K}[X]$.

C6. 73. Question. — Que dire d'un idéal I de $\mathbf{K}[X]$ qui contient un polynôme constant non nul ?

C6. 74. Exercice. — Justifier que $I := \{P \in \mathbf{K}[X] : P(0) = P(1) = 0\}$ est un idéal de $\mathbf{K}[X]$.

6.3 Description des idéaux de $\mathbf{K}[X]$

C6. 75. THÉORÈME (DESCRIPTION DES IDÉAUX DE $\mathbf{K}[X]$). — Soit I un idéal de $\mathbf{K}[X]$. Alors

$$\exists A \in \mathbf{K}[X] \quad I = A\mathbf{K}[X] := \{PA : P \in \mathbf{K}[X]\}.$$

Un tel polynôme A est appelé *générateur de l'idéal I* .

C6. 76. Remarque (Raffinement du précédent théorème). —

1. D'après l'Exercice **C6.70** et le Théorème **C6.75**, nous savons que les idéaux de $\mathbf{K}[X]$ sont précisément les parties de $\mathbf{K}[X]$ de la forme $A\mathbf{K}[X]$, où $A \in \mathbf{K}[X]$.
2. De la démonstration donnée du Théorème **C6.75**, il ressort que si I est un idéal de $\mathbf{K}[X]$ alors un générateur A de I est donné par

$$A = \begin{cases} 0 & \text{si } I = \{0\} \\ \text{un polynôme de degré minimal dans } I \setminus \{0\} & \text{si } I \neq \{0\}. \end{cases}$$

3. De l'Exercice **C6.71**, nous déduisons que si A est générateur d'un idéal I non nul de $\mathbf{K}[X]$, alors les autres générateurs sont de la forme λA , où $\lambda \in \mathbf{K}^*$. Par conséquent, un idéal non nul de $\mathbf{K}[X]$ possède un unique générateur unitaire.

C6. 77. Exercice. — Donner l'unique générateur unitaire de l'idéal $I := \{P \in \mathbf{K}[X] : P(0) = P(1) = 0\}$ de $\mathbf{K}[X]$.

7 PGCD et PPCM

7.1 Notions de PGCD et de PPCM

C6. 78. DÉFINITION (PGCD ET PPCM DE DEUX POLYNÔMES NON NULS). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$.

1. L'idéal $A\mathbf{K}[X] + B\mathbf{K}[X]$ est non nul (il contient $A \neq 0$ par exemple). Son unique générateur unitaire est appelé Plus Grand Commun Diviseur de A et B , et est noté $A \wedge B$. On a donc

$$A\mathbf{K}[X] + B\mathbf{K}[X] = (A \wedge B)\mathbf{K}[X].$$

2. L'idéal $A\mathbf{K}[X] \cap B\mathbf{K}[X]$ est non nul (il contient $AB \neq 0$). Son unique générateur unitaire est appelé Plus Petit Commun Multiple de A et B , et est noté $A \vee B$. On a donc

$$A\mathbf{K}[X] \cap B\mathbf{K}[X] = (A \vee B)\mathbf{K}[X].$$

C6. 79. PROPOSITION (CARACTÉRISATION DU PGCD (RESP. PPCM) OU JUSTIFICATION DE LA TERMINOLOGIE). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$.

1. $A \wedge B$ est le polynôme unitaire de degré maximal divisant à la fois A et B .
2. $A \vee B$ est le polynôme unitaire de degré minimal divisible à la fois A et B .

C6. 80. Exemple (Calculs de quelques PGCD et PPCM dans des cas triviaux). — Soient $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$.

1. Si $\deg(B) = 0$, i.e. si B est un polynôme constant non nul, alors $A \wedge B = 1$ et $A \vee B = \widehat{A}$.
2. Si B divise A , alors $A \wedge B = \widehat{B}$ et $A \vee B = \widehat{A}$.

C6. 81. Exercice (Remplacer des polynômes par leurs normalisés ne modifie ni le PGCD, ni le PPCM). — Soient $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. Alors $A \wedge B = \widehat{A} \wedge \widehat{B}$ et $A \vee B = \widehat{A} \vee \widehat{B}$.

C6. 82. DÉFINITION (PGCD ET PPCM D'UN NOMBRE FINI DE POLYNÔMES NON NULS). — Soit $(A_1, A_2, \dots, A_n) \in (\mathbf{K}[X] \setminus \{0\})^n$.

1. L'idéal $A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_n\mathbf{K}[X]$ est non nul (il contient $A_1 \neq 0$ par exemple). Son unique générateur unitaire est appelé Plus Grand Commun Diviseur de A_1, A_2, \dots, A_n , et est noté $A_1 \wedge A_2 \wedge \dots \wedge A_n$. On a donc

$$A_1\mathbf{K}[X] + A_2\mathbf{K}[X] + \dots + A_n\mathbf{K}[X] = (A_1 \wedge A_2 \wedge \dots \wedge A_n)\mathbf{K}[X].$$

2. L'idéal $A_1\mathbf{K}[X] \cap A_2\mathbf{K}[X] \cap \dots \cap A_n\mathbf{K}[X]$ est non nul (il contient $A_1 A_2 \dots A_n \neq 0$). Son unique générateur unitaire est appelé Plus Petit Commun Multiple de A_1, A_2, \dots, A_n , et est noté $A_1 \vee A_2 \vee \dots \vee A_n$. On a donc

$$A_1\mathbf{K}[X] \cap A_2\mathbf{K}[X] \cap \dots \cap A_n\mathbf{K}[X] = (A_1 \vee A_2 \vee \dots \vee A_n)\mathbf{K}[X].$$

7.2 Primalité relative

C6. 83. DÉFINITION (POLYNÔMES PREMIERS ENTRE EUX). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. On dit que A et B sont premiers entre eux si $A \wedge B = 1$.

C6. 84. THÉORÈME (THÉORÈME DE BÉZOUT). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. Alors A et B sont premiers entre eux si et seulement si

$$\exists (U, V) \in \mathbf{K}[X]^2, \quad AU + BV = 1.$$

Une telle identité est parfois appelée identité de Bézout.

C6. 85. Exemple (Primalité relative et identité de Bézout dans un cas trivial). — Soient $a \in \mathbf{K}$ et $b \in \mathbf{K}$ distincts. Alors les polynômes $X - a$ et $X - b$ sont premiers entre eux, comme le prouve l'identité

$$\frac{1}{b-a} (X - a) - \frac{1}{b-a} (X - b) = 1$$

qui est donc une identité de Bézout.

C6. 86. Exercice. — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$.

1. Pourquoi existe-t-il $(U, V) \in \mathbf{K}[X]^2$ tel que $AU + BV = A \wedge B$?
2. Si $AU + BV = C$, avec $(U, V, C) \in \mathbf{K}[X]^3$, a-t-on nécessairement $C = A \wedge B$?

C6. 87. Lemme (Primalité relative et produit). — Soit $(A, B, C) \in (\mathbf{K}[X] \setminus \{0\})^2$. Si A est premier avec B et C , alors A est premier avec le polynôme BC .

C6. 88. Lemme (Primalité relative et puissances). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. Si A et B sont premiers entre eux, alors il en est de même de A^n et B^m , pour tout $(n, m) \in \mathbf{N}^* \times \mathbf{N}^*$.

C6. 89. Exercice (D'un PGCD quelconque à un PGCD égal à 1). — Soit $(A, B) \in (\mathbf{K}[X] \setminus \{0\})^2$. Alors comme $D := A \wedge B$ divise A et B , il existe $(A_0, B_0) \in (\mathbf{K}[X] \setminus \{0\})^2$ tel que $A = A_0D$ et $B = B_0D$. Démontrer : $A_0 \wedge B_0 = 1$.

C6. 90. THÉORÈME (THÉORÈME DE GAUSS). — Soit $(A, B, C) \in (\mathbf{K}[X] \setminus \{0\})^3$. Alors

$$\left(\begin{array}{l} A \text{ divise } BC \\ A \wedge B = 1 \end{array} \right) \implies A \text{ divise } C.$$

C6. 91. PROPOSITION (PRODUIT DU PGCD ET DU PPCM). — Soient $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X]$ des polynômes unitaires. Alors

$$(A \wedge B)(A \vee B) = AB.$$

7.3 Une méthode de calcul du PGCD et du PPCM

C6. 92. REMARQUE (LA CONNAISSANCE DU PGCD LIVRE CELLE DU PPCM). — D'après la précédente proposition, nous déduisons le PPCM du PGCD, à l'aide d'une division euclidienne par exemple. Un Algorithme existe pour calculer le PGCD : l'Algorithme d'Euclide, que nous présentons ci-dessous.

C6. 93. Lemme (Lemme clé pour l'Algorithme d'Euclide). — Soit $(A, B) \in \mathbf{K}[X]^2$ tel que $A \neq 0$ et $\deg(B) \geq 1$. Considérons la division euclidienne de A par B : $A = BQ + R$, où $(Q, R) \in \mathbf{K}[X]^2$ et $\deg(R) < \deg(B)$. Alors

$$A \wedge B = \begin{cases} B \wedge R & \text{si } R \neq 0 \\ \widehat{B} & \text{si } R = 0. \end{cases}$$

C6. 94. Algorithme d'Euclide pour le calcul du PGCD. — Soit $A \in \mathbf{K}[X] \setminus \{0\}$ et $B \in \mathbf{K}[X]$ tel que $\deg(B) \geq 1$. Nous présentons un Algorithme, appelé Algorithme d'Euclide, qui permet le calcul de $A \wedge B$, à l'aide de divisions euclidiennes successives. Il repose, de manière essentielle, sur le lemme précédent.

- **Étape 1.** On effectue la division euclidienne de A par B :

$$A = BQ_1 + R_1, \text{ où } (Q_1, R_1) \in \mathbf{K}[X]^2 \text{ et } \text{Deg}(R_1) < \text{Deg}(B).$$

→ Si $R_1 = 0$, alors $A \wedge B = \widehat{B}$ et on s'arrête.

→ Si $\text{Deg}(R_1) = 0$, i.e. si R_1 est un polynôme constant non nul, alors $A \wedge B = 1$ et on s'arrête.

→ Si $\text{Deg}(R_1) \geq 1$, alors $A \wedge B = B \wedge R_1$ et on continue.

- **Étape 2.** On effectue la division euclidienne de B par R_1

$$B = R_1Q_2 + R_2, \text{ où } (Q_2, R_2) \in \mathbf{K}[X]^2 \text{ et } \text{Deg}(R_2) < \text{Deg}(R_1).$$

→ Si $R_2 = 0$, alors $A \wedge B = B \wedge R_1 = \widehat{R_1}$ et on s'arrête.

→ Si $\text{Deg}(R_2) = 0$, i.e. si R_2 est un polynôme constant non nul, alors $A \wedge B = B \wedge R_1 = R_1 \wedge R_2 = 1$ et on s'arrête.

→ Si $R_2 \neq 0$, alors $A \wedge B = B \wedge R_1 = R_1 \wedge R_2$ et on continue.

- **Étape $n + 1$, où n est un nombre entier supérieur ou égal à 2.**

Supposons construits des polynômes R_{n-1} et R_n tels que

$$A \wedge B = R_{n-1} \wedge R_n \text{ et } 1 \leq \text{Deg}(R_n) < \text{deg } R_{n-1}.$$

On effectue la division euclidienne de R_{n-1} par R_n :

$$R_{n-1} = R_nQ_{n+1} + R_{n+1}, \text{ où } (Q_{n+1}, R_{n+1}) \in \mathbf{K}[X]^2 \text{ et } \text{Deg}(R_{n+1}) < \text{deg } R_n.$$

→ Si $R_{n+1} = 0$, alors $A \wedge B = R_{n-1} \wedge R_n = \widehat{R_n}$ et on s'arrête.

→ Si $\text{Deg}(R_{n+1}) = 0$, i.e. si R_{n+1} est un polynôme constant non nul, alors $A \wedge B = R_{n-1} \wedge R_n = R_n \wedge R_{n+1} = 1$ et on s'arrête.

→ Si $R_{n+1} \neq 0$, alors $A \wedge B = R_{n-1} \wedge R_n = R_n \wedge R_{n+1}$ et on continue.

C6. 95. PROPOSITION (TERMINAISON DE L'ALGORITHME D'EUCLIDE). — *L'Algorithme d'Euclide se termine au bout d'un nombre fini d'étapes.*

Démonstration. Si la construction ne s'arrêtait pas, nous construirions une suite d'entiers naturels strictement décroissante

$$\text{Deg}(B) > \text{Deg}(R_1) > \text{Deg}(R_2) > \dots > \text{Deg}(R_n) > \text{Deg}(R_{n+1}) > \dots$$

ce qui n'est pas possible.

Q.E.D.

C6. 96. PROPOSITION (CORRECTION DE L'ALGORITHME D'EUCLIDE). — *L'Algorithme d'Euclide livre le PGCD de A et B.*

Démonstration. Soit n_0 le nombre d'étapes effectuées, avant l'arrêt.

C'est lors de cette dernière étape que nous obtenons pour la première fois, un reste qui est un polynôme constant (nul ou non) dans la division euclidienne considérée. Ainsi a-t-on

$$\text{Deg}(R_{n_0}) = 0 \quad \text{et} \quad \text{Deg}(R_k) \neq 0, \text{ pour tout } k \in \llbracket 1, n_0 - 1 \rrbracket.$$

On a

$$A \wedge B = B \wedge R_1 = R_1 \wedge R_2 = \dots = R_{n_0-2} \wedge R_{n_0-1} = \begin{cases} \widehat{R_{n_0-1}} & \text{si } R_{n_0} = 0 \\ 1 & \text{si } R_{n_0} \text{ est un polynôme constant non nul.} \end{cases}$$

Le PGCD de A et B est donc calculé.

Q.E.D.

C6. 97. Une méthode pour obtenir une relation de Bézout. — On considère de nouveau l'Algorithme d'Euclide **C6.94**. À partir des divisions euclidiennes encadrées, nous pouvons former une relation de Bézout en « remontant » l'Algorithme.

C6. 98. Exercice (Complexité de l'Algorithme d'Euclide). — Majorer le nombre de divisions euclidiennes effectuées lors de la mise en œuvre de l'Algorithme d'Euclide.

C6. 99. Exercice. — Calculer le PGCD et le PPCM de $A = X^5 + 3X^4 + X^3 + 2X^2 + X + 1$ et $B = X^4 + 2X^3 + 3X^2 + 1$.

C6. 100. Exercice. — Soient $(a, b) \in \mathbf{K}[X]^2$ et $(n, m) \in (\mathbf{N}^*)^2$. Déterminer $(X - a)^n \wedge (X - b)^m$.

C6. 101. *Exercice (Droite affine dans $\mathbf{K}[X]^2$).* — Résoudre l'équation

$$U(X^4 + X + 1) + V(X^3 + 3) = 1$$

d'inconnue $(U, V) \in \mathbf{K}[X]^2$.

8 Décomposition d'un polynôme en produit d'irréductibles

8.1 Notion de polynôme irréductible sur un corps

C6. 102. DÉFINITION (POLYNÔME IRREDUCTIBLE SUR UN CORPS). — Soit $P \in \mathbf{K}[X]$. P est dit irréductible sur \mathbf{K} si

$$\left\{ \begin{array}{l} \text{Deg}(P) \geq 1 \\ \text{et} \\ \forall (P_1, P_2) \in \mathbf{K}[X]^2 \quad P = P_1 P_2 \implies (P_1 \in \mathbf{K}_0[X] \text{ ou } P_2 \in \mathbf{K}_0[X]). \end{array} \right.$$

Le polynôme P est dit réductible sur \mathbf{K} , s'il n'est pas irréductible sur \mathbf{K} .

C6. 103. Remarque. — On peut donc penser à un polynôme de $\mathbf{K}[X]$, irréductible sur \mathbf{K} , comme à un polynôme non constant, qui n'admet pas de factorisation non triviale dans $\mathbf{K}[X]$.

C6. 104. REMARQUE (IRRÉDUCTIBILITÉ ET EXTENSION DE CORPS). — Soit $P \in \mathbf{K}[X]$. Soit \mathbf{L} un sur-corps de \mathbf{K} qui est un sous-corps de $\mathbf{C} : \mathbf{K} \subset \mathbf{L} \subset \mathbf{C}$. Le polynôme P peut être irréductible sur \mathbf{K} , mais réductible sur \mathbf{L} (cf. Exemple suivant).

C6. 105. Attention. — Le caractère irréductible d'un polynôme dépendant du corps sur lequel on se place, on évitera de parler de polynôme irréductible sans préciser de corps, pour préférer l'expression : le polynôme est irréductible sur tel corps.

C6. 106. Exemple. — Le polynôme $X^2 + 1$ est irréductible sur \mathbf{R} , mais réductible sur \mathbf{C} .

C6. 107. Exercice (Être irréductible sur \mathbf{K} versus avoir des racines dans \mathbf{K}). —

1. Démontrer que tout polynôme de $\mathbf{K}[X]$ de degré 1 est irréductible sur \mathbf{K} .
2. Soit P un polynôme de $\mathbf{K}[X]$ tel que $\text{Deg}(P) \in \{2, 3\}$. Démontrer que P est irréductible sur \mathbf{K} si et seulement si il ne possède pas de racine dans \mathbf{K} .
3. Démontrer qu'un polynôme de $\mathbf{R}[X]$, de degré impair supérieur ou égal à 3, n'est pas irréductible sur \mathbf{R} .
4. Donner un exemple de polynôme P dans $\mathbf{R}[X]$ qui n'admet pas de racine dans \mathbf{R} , et qui n'est pas irréductible sur \mathbf{R} .

C6. 108. Lemme (PGCD de deux polynômes irréductibles sur \mathbf{K} , unitaires, distincts). — Soient A et B des polynômes irréductibles sur \mathbf{K} , unitaires, distincts. Alors $A \wedge B = 1$.

Démonstration. On raisonne par l'absurde. Supposons donc que $D := A \wedge B \neq 1$. Alors $\deg(D) \geq 1$. Comme D divise A , il existe $Q \in \mathbf{K}[X]$ tel que $A = DQ$. Comme A est irréductible et $\deg(D) \geq 1$, il vient $Q \in \mathbf{K}_0[X]$. Comme A et D sont unitaires, nous avons $Q = 1$, soit $D = A$. De même, nous établissons $D = B$. Ainsi $A = B$, ce qui contredit une des hypothèses. Q.E.D.

8.2 Décomposition d'un polynôme en produit de polynômes irréductibles

C6. 109. THÉORÈME (DÉCOMPOSITION D'UN POLYNÔME EN PRODUIT DE POLYNÔMES IRRÉDUCTIBLES).

— Soit $P \in \mathbf{K}[X]$ tel que $\text{Deg}(P) \geq 1$.

1. Il existe $r \in \mathbf{N}^*$, des polynômes $P_1, \dots, P_r \in \mathbf{K}[X]$ irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, des entiers naturels non nuls n_1, \dots, n_r tels que :

$$P = \text{Dom}(P) P_1^{n_1} \dots P_r^{n_r}.$$

2. Cette décomposition de P en produit de facteurs irréductibles est unique à l'ordre près, i.e. étant donné $s \in \mathbf{N}^*$, des polynômes $Q_1, \dots, Q_s \in \mathbf{K}[X]$ irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, des entiers naturels non nuls m_1, \dots, m_s tels que :

$$P = \text{Dom}(P) Q_1^{m_1} \dots Q_s^{m_s}$$

alors

- $r = s$
- il existe une bijection $\sigma: \llbracket 1, r \rrbracket \rightarrow \llbracket 1, r \rrbracket$ telle que

$$\forall i \in \llbracket 1, r \rrbracket \quad Q_i = P_{\sigma(i)} \quad \text{et} \quad m_i = n_{\sigma(i)}.$$

Démonstration. Quitte à remplacer P par son normalisé, on peut supposer que $\text{Dom}(P) = 1$.

- **Existence.** On raisonne par récurrence forte sur le degré de P . Pour tout $d \in \mathbf{N}^*$, notons $\mathcal{P}(d)$ le prédicat en la variable d : tout polynôme unitaire de $\mathbf{K}[X]$ de degré d admet une décomposition en produit d'irréductibles, comme dans l'assertion 1 du Théorème.

— *Initialisation à $d = 1$*

Soit $P \in \mathbf{K}[X]$ un polynôme unitaire, tel que $\text{Deg}(P) = 1$. Alors P est irréductible sur \mathbf{K} . On peut donc l'écrire sous la forme introduite dans l'assertion 1 du théorème, en posant

$$r = 1 \quad , \quad P_1 = P \quad , \quad n_1 = 1.$$

— *Hérédité*

Soit $d \in \mathbf{N}^*$ fixé. Supposons $\mathcal{P}(k)$ vraie pour tout $k \in \llbracket 1, d \rrbracket$. Soit P un polynôme unitaire de degré $d + 1$.

- Si P est irréductible sur \mathbf{K} , alors on peut l'écrire sous la forme introduite dans l'assertion 1 du théorème, en posant

$$r = 1 \quad , \quad P_1 = P \quad , \quad n_1 = 1.$$

- Si P n'est pas irréductible sur \mathbf{K} alors il existe $A, B \in \mathbf{K}[X]$ des polynômes unitaires tels que $P = AB$, $\deg(A) \geq 1$ et $\deg(B) \geq 1$. Puisque

$$\deg(A) + \deg(B) = \deg(AB) = \text{Deg}(P) = d + 1$$

nous en déduisons $\deg(A) \in \llbracket 1, d \rrbracket$ et $\deg(B) \in \llbracket 1, d \rrbracket$. Nous appliquons l'hypothèse de récurrence à A et à B pour obtenir l'existence de $r, s \in \mathbf{N}^*$, de polynômes A_1, \dots, A_r irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, de polynômes B_1, \dots, B_s irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, d'entiers naturels non nuls $n_1, \dots, n_r, m_1, \dots, m_s$ tels que

$$A = P_1^{n_1} \dots P_r^{n_r} \quad \text{et} \quad B = Q_1^{m_1} \dots Q_s^{m_s}.$$

D'où

$$P = P_1^{n_1} \dots P_r^{n_r} Q_1^{m_1} \dots Q_s^{m_s}.$$

En regroupant éventuellement les polynômes P_i et Q_j égaux ($i \in \llbracket 1, r \rrbracket, j \in \llbracket 1, s \rrbracket$), nous obtenons une écriture de P comme dans l'assertion 1 du théorème.

- **Unicité.** On présente uniquement une esquisse de preuve, en étant moins formel que pour l'existence, en raisonnant par itérations successives. Soient deux décompositions en produits d'irréductibles de P , comme dans l'assertion 2 du Théorème :

$$P_1^{n_1} \dots P_r^{n_r} = P = Q_1^{m_1} \dots Q_s^{m_s}.$$

- Le polynôme P_1 divise le polynôme P (car $n_1 \geq 1$), donc le polynôme $Q_1^{m_1} \dots Q_s^{m_s}$. Le polynôme P_1 ne peut pas être premier avec tous les polynômes Q_1, \dots, Q_s , sinon le Théorème de Gauß serait mis en défaut. Par conséquent, quitte à ré-indexer les polynômes Q_1, \dots, Q_s , on peut supposer $P_1 \wedge Q_1 \neq 1$. Alors, d'après le Lemme **C6.108**, $P_1 = Q_1$. D'après le Lemme **C6.108** et le Lemme **C6.88**, $P_1^{n_1}$ est premier avec les polynômes $Q_2^{m_2}, \dots, Q_s^{m_s}$. Grâce au Lemme **C6.87**, nous en déduisons que $P_1^{n_1}$ est premier avec le polynôme $Q_2^{m_2} \dots Q_s^{m_s}$. D'après le Théorème de Gauß, $P_1^{n_1}$ divise $Q_1^{m_1} = P_1^{m_1}$ et donc $n_1 \leq m_1$. Alors

$$P_2^{n_2} \dots P_r^{n_r} = Q_1^{m_1 - n_1} \dots Q_s^{m_s}.$$

Si $m_1 > n_1$, alors le polynôme $Q_1 = P_1$ divise le polynôme $P_2^{n_2} \dots P_r^{n_r}$, ce qui n'est pas possible, puisque P_1 est premier avec les polynômes P_2, \dots, P_r (adapter le raisonnement précédent). Ainsi, $n_1 = m_1$ et

$$P_2^{n_2} \dots P_r^{n_r} = Q_2^{m_2} \dots Q_s^{m_s}.$$

- En itérant ce procédé, on démontre le résultat souhaité. La bijection σ qui figure dans l'assertion 2 du Théorème est « cachée » dans les ré-indexations éventuelles des polynômes Q_j , $j \in \llbracket 1, s \rrbracket$.

Q.E.D.

C6.110. Exercice. — Soit $P \in \mathbf{K}[X]$ un polynôme unitaire, de degré supérieur ou égal à 1. On considère la décomposition de P en produit de polynômes irréductibles :

$$P = P_1^{n_1} \dots P_r^{n_r}$$

où $r \in \mathbf{N}^*$, $P_1, \dots, P_r \in \mathbf{K}[X]$ sont des polynômes irréductibles sur \mathbf{K} , unitaires et deux-à-deux distincts, n_1, \dots, n_r sont des entiers naturels non nuls. Quels sont les diviseurs unitaires de P ?

8.3 Irréductibles de $\mathbf{C}[X]$ et irréductibles de $\mathbf{R}[X]$

C6. 111. THÉORÈME (DESCRIPTION DES IRRÉDUCTIBLES DE $\mathbf{C}[X]$ (RESP. $\mathbf{R}[X]$)). —

1. Soit $P \in \mathbf{C}[X]$.

$$P \text{ est irréductible sur } \mathbf{C} \iff \text{Deg}(P) = 1.$$

2. Soit $P \in \mathbf{R}[X]$.

$$P \text{ est irréductible sur } \mathbf{R} \iff \left\{ \begin{array}{l} \text{Deg}(P) = 1 \\ \text{ou} \\ P \text{ est de degré 2 et de discriminant strictement négatif.} \end{array} \right.$$

8.4 Décomposition en produit d'irréductibles dans $\mathbf{C}[X]$

C6. 112. COROLLAIRE (DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{C}[X]$). — Soit $P \in \mathbf{C}[X]$ tel que $\text{Deg}(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{C}[X]$ est « de la forme »

$$P = \text{Dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

où

- r est un entier naturel non nul
- $\alpha_1, \dots, \alpha_r$ sont des complexes deux-à-deux distincts
- n_1, \dots, n_r sont des entiers naturels non nuls.

Démonstration. Il s'agit d'une conséquence des Théorèmes **C6.109** et **C6.111**.

Q.E.D.

C6. 113. Remarque. — L'entier r est le nombre de racines complexes deux-à-deux distinctes de P , les complexes $\alpha_1, \dots, \alpha_r$ sont les racines complexes deux-à-deux distinctes de P et pour tout $k \in \llbracket 1, r \rrbracket$, n_k est l'ordre de multiplicité de la racine α_k de P .

C6. 114. Remarque. — Soit $P \in \mathbf{C}[X]$ de degré supérieur ou égale à 1. Soient $\alpha_1, \dots, \alpha_r$ les racines complexes deux-à-deux distinctes de P et n_1, \dots, n_r leurs multiplicités respectives. Alors, dans le corps des fractions rationnelles $\mathbf{C}(X)$:

$$\frac{P'}{P} = \sum_{k=1}^r \frac{n_k}{X - \alpha_k}.$$

8.5 Décomposition en produit d'irréductibles dans $\mathbf{R}[X]$

C6.115. COROLLAIRE (DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{R}[X]$). — Soit $P \in \mathbf{R}[X]$ tel que $\text{Deg}(P) \geq 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$ est « d'une des formes suivantes »

1. Cas où P n'a aucune racine dans \mathbf{R}

$$P = \text{Dom}(P) \prod_{\ell=1}^s (X^2 + a_\ell X + b_\ell)^{m_\ell}$$

2. Cas où P n'a aucune racine dans $\mathbf{C} \setminus \mathbf{R}$ (i.e. est scindé sur \mathbf{R})

$$P = \text{Dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k}$$

3. Cas où P a une racine dans \mathbf{R} et une racine dans $\mathbf{C} \setminus \mathbf{R}$

$$P = \text{Dom}(P) \prod_{k=1}^r (X - \alpha_k)^{n_k} \prod_{\ell=1}^s (X^2 + a_\ell X + b_\ell)^{m_\ell}$$

où

- r et s sont des entiers non nuls
- $n_1, \dots, n_r, m_1, \dots, m_r$ sont des entiers non nuls
- $\alpha_1, \dots, \alpha_r$ sont des réels deux-à-deux distincts
- $(a_1, b_1), \dots, (a_s, b_s)$ sont des couples deux-à-deux distincts de réels tels que pour tout $k \in \llbracket 1, s \rrbracket$, $a_k^2 < 4b_k$.

Démonstration. Il s'agit d'une conséquence des Théorèmes **C6.109** et **C6.111**.

Q.E.D.

C6.116. Exercice. — Décomposer le polynôme $P = X^4 + 16$ en produit d'irréductibles dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$.

C6.117. Exercice. — Soit $n \in \mathbf{N}_{\geq 2}$. Nous posons $P := X^n - 1$.

1. Décomposer P en produit de facteurs irréductibles dans $\mathbf{C}[X]$.
2. En déduire la décomposition de P en produit de facteurs irréductibles dans $\mathbf{R}[X]$.

9 Une sélection d'exercices

C6. 118. Exercice (CCINP). — On considère les polynômes $P(X) = 2X^4 - 3X^2 + 1$ et $Q(X) = X^3 + 3X^2 + 3X + 2$.

1. Décomposer P en produit de facteurs premiers dans $\mathbf{C}[X]$ (on pourra calculer $P(1)$ et $P(-1)$).
2. Décomposer Q en produit de facteurs premiers dans $\mathbf{C}[X]$ (on pourra calculer $Q(-2)$).
 - (a) Dédurre des questions précédentes l'existence de polynômes U, V tels que $PU + QV = 1$.
 - (b) Indiquer une méthode pour déterminer les polynômes U, V à l'aide de l'algorithme d'Euclide.

C6. 119. Exercice (CCINP). — On considère les polynômes $P(X) = 3X^4 - 9X^3 + 7X^2 - 3X + 2$ et $Q(X) = X^4 - 3X^3 + 3X^2 - 3X + 2$.

1. Décomposer P et Q en produits de facteurs premiers dans $\mathbf{R}[X]$ puis dans $\mathbf{C}[X]$ (on pourra calculer les valeurs de P et Q en 1 et en 2).
2. Déterminer le PGCD et le PPCM de P et de Q .

C6. 120. Exercice (CCINP). — Notons f l'endomorphisme de $\mathbf{K}_n[X]$ défini par

$$f \quad \left| \begin{array}{l} \mathbf{K}_n[X] \longrightarrow \mathbf{K}_n[X] \\ P \longmapsto P - P' \end{array} \right.$$

1. Démontrer que f est injectif de deux façons différentes.
 - (a) En utilisant la matrice de f dans la base canonique.
 - (b) Sans utiliser la matrice de f dans la base canonique.
2. Soit $Q \in \mathbf{K}_n[X]$. Trouver P tel que $f(P) = Q$.
Indication : si $P \in \mathbf{K}_n[X]$, que vaut $P^{(n+1)}$?

C6. 121. Exercice. —

1. Soit $(\lambda, \mu) \in \mathbf{R}^2$. Effectuer la division euclidienne de $X^4 + X^3 + \lambda X^2 + \mu X + 2$ par $X^2 + 2$.
2. Déterminer les valeurs de (λ, μ) pour lesquelles $X^2 + 2$ divise de $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

C6. 122. Exercice (CCINP). — Notons Φ l'endomorphisme de $\mathbf{R}_n[X]$ défini par

$$\Phi \quad \left| \begin{array}{l} \mathbf{R}_n[X] \longrightarrow \mathbf{R}_n[X] \\ P \longmapsto P(X) - P(X-1) \end{array} \right.$$

déterminer la matrice de Φ dans la base canonique de $\mathbf{R}_n[X]$ et en Dédurre $\text{Ker}(\Phi)$ et $\text{Im}(\Phi)$.

C6. 123. Exercice. — Soit $P \in \mathbf{R}[X]$, soit $z \in \mathbf{C}$ une racine de P .

1. Démontrer que \bar{z} est une racine de P .
2. Supposons que $z \in \mathbf{C} \setminus \mathbf{R}$. Démontrer que $X^2 - 2\operatorname{Re}(z)X + |z|^2$ divise P .
3. Supposons encore que $z \in \mathbf{C} \setminus \mathbf{R}$. Démontrer par récurrence sur le degré de P que si z est racine de P d'ordre $n \in \mathbf{N}^*$, alors \bar{z} est racine de P d'ordre n .

C6. 124. Exercice. — Soit $P \in \mathbf{C}[X]$.

1. Démontrer que $P(X) - X$ divise $P(P(X)) - P(X)$.
2. En déduire que $P(X) - X$ divise $P(P(X)) - X$.
3. Pour tout $n \in \mathbf{N}$, montrer que $P(X) - X$ divise $P^n(X) - X$, où P^n désigne le polynôme obtenu en composant P n fois avec lui-même.

C6. 125. Exercice. — Soient $(A, B) \in \mathbf{C}[X]^2$ tels que $A \wedge B = 1$. Démontrer qu'il existe un unique couple $(U, V) \in \mathbf{C}[X]^2$ tel que $AU + BV = 1$ et $\deg U < \deg B$ et $\deg V < \deg A$.

C6. 126. Exercice. — Soient $(p, q) \in \mathbf{N}^* \times \mathbf{N}^*$. Démontrer que $(X^p - 1) \wedge (X^q - 1) = X^{p \wedge q} - 1$.

C6. 127. Exercice. — Soient $(A, B) \in \mathbf{C}[X]^2$. Démontrer que $(A + B) \wedge AB = 1$ si et seulement si $A \wedge B = 1$.

C6. 128. Exercice. — Résoudre l'équation

$$x^3 - 8x^2 + 23x - 28 = 0$$

d'inconnue $x \in \mathbf{C}$, sachant que la somme de deux racines est égale à la troisième.

C6. 129. Exercice. — Déterminer tous les polynômes $P \in \mathbf{R}[X]$ tels que $P(X^2) = P(X)^2$.

C6. 130. Exercice. — Déterminer les polynômes $P \in \mathbf{R}[X]$ tels que P' divise P .

C6. 131. Exercice (CCINP). — Déterminer les complexes a, b, c vérifiant les trois conditions

1. $|a| = |b| = |c| = 1$;
2. $a + b + c = 1$;
3. $abc = 1$.

C6. 132. Exercice (CCINP). — Déterminer tous les polynômes $P \in \mathbf{C}_3[X]$ tels que $P(j) = P'(j^2) = j^2$ et $P(j^2) = P'(j) = j$.

C6. 133. Exercice (CCINP). — Déterminer tous les polynômes $P \in \mathbf{R}[X]$ vérifiant $P(X^2) = (X^2 + 1)P(X)$.

C6. 134. Exercice (CCINP). — Soient $a \in]0, \pi[$ et $n \in \mathbf{N}^*$. Factoriser dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$ le polynôme

$$X^{2n} - 2 \cos(na)X^n + 1.$$

C6. 135. Exercice (CCINP). — Soit $P \in \mathbf{C}[X]$ non nul tel que $P(X^2) = P(X)P(X-1)$.

1. Soit $a \in \mathbf{C}$ une racine de P . Démontrer que pour tout $n \in \mathbf{N}$, a^{2^n} est racine de P .
2. En déduire que $a = 0$ ou $|a| = 1$.
3. Démontrer qu'en outre, $a = -1$ ou $|a + 1| = 1$.
4. En déduire tous les polynômes $P \in \mathbf{C}[X]$ tels que $P(X^2) = P(X)P(X-1)$.

C6. 136. Exercice (CCINP). — Soit $P \in \mathbf{R}[X]$ de degré 7. On suppose que $P + i$ est multiple de $(X - i)^4$. Déterminer P' et en déduire P .

C6. 137. Exercice (CCINP). — Pour tout $n \in \mathbf{N}^*$, posons $P_n(X) = \frac{1}{2^n n!} \frac{d^n}{dX^n} ((X^2 - 1)^n)$.

1. Étudier le degré de P_n ainsi que sa parité.
2. Démontrer que $P_n(1) = 1$. En déduire $P_n(-1)$.
3. Démontrer que P_n possède n racines distinctes dans $] -1, 1[$.

C6. 138. Exercice (CCINP). — Soit f l'application définie par

$$f \left| \begin{array}{l} \mathbf{R}[X] \longrightarrow \mathbf{R}[X] \\ P \longmapsto P(X+1) - P(X) \end{array} \right.$$

1. Démontrer que f est linéaire, déterminer son noyau et son image.
2. Soit $Q \in \mathbf{R}[X]$. Démontrer qu'il existe un unique $P \in \mathbf{R}[X]$ tel que $P(0) = 0$ et $Q = f(P)$.

Simplifier alors $\sum_{k=0}^n Q(k)$.

3. Calculer $\sum_{k=0}^n k^2$. Généraliser.

C6. 139. Exercice (CCINP). — Soit $n \geq 2$. Pour tout $k \in \llbracket 0, n \rrbracket$, posons $P_k(X) = X^k(1 - X)^{n-k}$.

1. Démontrer que (P_0, \dots, P_n) est une base de $\mathbf{R}_n[X]$.
2. Exprimer $1, X, \dots, X^n$ dans la base précédente.

C6. 140. Exercice. — Soient $P, Q \in \mathbf{R}[X]^2$. Notons D_1 leur PGCD dans $\mathbf{R}[X]$ et D_2 leur PGCD dans $\mathbf{C}[X]$. Démontrer que $D_1 = D_2$.

C6. 141. Exercice (Mines). — Soit $n \in \mathbf{N}$.

1. Exprimer

$$\frac{\sin((2n+1)x)}{\sin(x)}$$

à l'aide d'un polynôme en $\cotan^2(x)$.

2. En déduire les racines du polynôme $\sum_{k=0}^n (-1)^k \binom{2n+1}{2k+1} X^{n-k}$.

C6. 142. Exercice (Mines). — Soit $Q \in \mathbf{R}_n[X]$.

1. Démontrer qu'il existe un unique $P \in \mathbf{R}_n[X]$ tel que $P - P' = Q$.
2. Supposons que, pour tout $x \in \mathbf{R}$, $Q(x) \geq 0$. Démontrer que, pour tout $x \in \mathbf{R}$, $P(x) \geq 0$.

C6. 143. Exercice (Mines). — Soit $n \in \mathbf{N}^*$. Déterminer le noyau, le rang et l'image de

$$f \quad \left| \begin{array}{l} \mathbf{R}_n[X] \longrightarrow \mathbf{R}_n[X] \\ P \longmapsto P(X+1) + P(X-1) - 2P(X) \end{array} \right.$$

C6. 144. Exercice (Centrale). — Soient $P, Q \in \mathbf{C}[X]$ de degrés respectifs n et m .

1. Démontrer qu'il existe un unique endomorphisme $u_{P,Q}$ de $\mathbf{C}_{n+m-1}[X]$ tel que

$$\forall (A, B) \in \mathbf{C}_{m-1}[X] \times \mathbf{C}_{n-1}[X] \quad u_{P,Q}(X^n A + B) = PA + QB.$$

2. Donner la matrice de $u_{P,Q}$ dans la base canonique.
3. Donner une condition nécessaire et suffisante pour que $u_{P,Q}$ soit un automorphisme.

4. On suppose désormais que P et Q sont à coefficients rationnels. Pour tout $y \in \mathbf{C}$, notons $Q_y(X) = Q(y - X)$ (il s'agit d'une composition et non d'une multiplication) et $T(y) = \det u_{P, Q_y}$. Démontrer que T est une fonction polynomiale à coefficients rationnels.
5. Soient $(\alpha, \beta) \in \mathbf{C}^2$ tels que $P(\alpha) = Q(\beta) = 0$. Déterminer deux polynômes $R, S \in \mathbb{Q}[X]$ tels que $R(\alpha + \beta) = S(\alpha\beta) = 0$.

C6. 145. Exercice (Centrale). — On dit qu'une suite $(P_n)_{n \in \mathbf{N}} \in \mathbf{R}[X]^{\mathbf{N}}$ de polynômes vérifie la propriété (C) si :

(a) $P_0 = 1$

(b) $P_1 \neq 0$

(c) $\forall (n, x, y) \in \mathbf{N} \times \mathbf{R}^2, P_n(x + y) = \sum_{k=0}^n P_k(x)P_{n-k}(y)$.

1. Démontrer que la suite $\left(\frac{X^n}{n!}\right)_{n \in \mathbf{N}}$ vérifie la propriété (C).

2. Notons $(P_n)_{n \in \mathbf{N}}$ la suite définie par $P_0 = 1$ et $\forall n \in \mathbf{N}^*, P_n(X) = \frac{X}{n!}(n + X)^{n-1}$.

(a) Démontrer que pour tout $n \in \mathbf{N}^*, P'_n(X) = P_{n-1}(X + 1)$.

(b) En déduire que $(P_n)_{n \in \mathbf{N}}$ vérifie la propriété (C).

3. Soit $(P_n)_{n \in \mathbf{N}}$ vérifiant la propriété (C).

(a) Démontrer que pour tout $n \in \mathbf{N}^*, P_n(0) = 0$.

(b) Démontrer que $\deg P_1 = 1$.

(c) Démontrer que pour tout $n \in \mathbf{N}, P_n$ est de degré n et calculer son coefficient dominant.

(d) Pour tout $n \in \mathbf{N}$, posons $a_n = P'_n(0)$. Démontrer que pour tout $n \in \mathbf{N}^*, P'_n = \sum_{k=0}^n a_{n-k}P_k$.

4. Soit $(a_n)_{n \in \mathbf{N}}$ une suite réelle. Existe-t-il toujours une suite (P_n) vérifiant la propriété (C) telle que pour tout $n \in \mathbf{N}, P'_n(0) = a_n$?

C6. 146. Exercice (Centrale). — Soit $n \in \mathbf{N}^*$.

1. Notons \mathbb{U}_n l'ensemble des racines n -ièmes de l'unité. Soit $p \in \mathbf{N}$. Calculer $\sum_{\xi \in \mathbb{U}_n} \xi^p$.

2. Soit $P = \sum_{k=0}^n a_k X^k$. Démontrer que $\sup_{|z|=1} |P(z)| \geq \max_{0 \leq k \leq n} |a_k|$.

C6. 147. Exercice (X). — Soit $P \in \mathbf{R}[X]$ tel que, pour tout $x \in \mathbf{R}, P(x) \geq 0$. Démontrer qu'il existe $(A, B) \in \mathbf{R}[X]^2$ tel que $P = A^2 + B^2$.

C6. 148. Exercice (X). — Soit $P \in \mathbf{C}[X]$, soit $a \in \mathbf{C}$ tel que $P(a) \neq 0$. Supposons a racine d'ordre $k \in \mathbf{N}^*$ de $P - P(a)$. Démontrer que pour tout $\rho > 0$ assez petit, il existe $2k$ points z_1, \dots, z_{2k} sur le cercle de centre a et de rayon ρ tels que $|P(z_1)| = \dots = |P(z_{2k})| = |P(a)|$.

C6. 149. Exercice (X-ENS). — Soit $P \in \mathbf{R}[X]$ un polynôme de degré $n \in \mathbf{N}$.

1. On suppose que, pour tout $k \in \llbracket 0, n \rrbracket$, $P(k) \in \mathbf{Z}$. Démontrer que, pour tout $k \in \mathbf{Z}$, $P(k) \in \mathbf{Z}$.
2. Notons d le pgcd de $P(0), \dots, P(n)$. Démontrer que pour tout $k \in \mathbf{Z}$, d divise $P(k)$.

C6. 150. Exercice (ENS). — Soient z_0, \dots, z_n des complexes distincts deux-à-deux. On suppose que pour tout polynôme $P \in \mathbf{C}_{n-1}[X]$, $P(z_0) = \sum_{k=1}^n P(z_k)$. Démontrer que z_1, \dots, z_n sont les sommets d'un polygone régulier centré en z_0 .

C6. 151. Exercice (X-ENS). — Soient $P, Q, R \in \mathbf{C}[X]$, soit $n \geq 3$. Supposons que $P^n + Q^n + R^n = 0$. Démontrer que les polynômes P, Q, R sont égaux à une constante multiplicative près.