Révisions sur les polynômes

par David Blottière, le 14 septembre 2023 à 17h26

Chapitre 2

Sommaire

§ 1. RAPPELS SUR LA CONSTRUCTION DE $\mathbf{K}[X]$

NOTATION. — La lettre $\mathbf{K}$ désigne un corps. 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. :

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

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 :

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

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

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

2. LA 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 $(\lambda\, a_n)_{n\in\mathbf{N}}$ 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 :

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

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

3. LA MULTIPLICATION INTERNE × 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 :

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

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

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

Comme on vérifie de plus :

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

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

4. L'ÉLÉMENT X DE $\mathbf{K}^{(N)}$

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. :

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

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

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

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 $i \in \mathbf{N}$.

5. LA BASE CANONIQUE DE $\mathbf{K}^{(\mathbf{N})}$

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

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

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

6. NOTION DE POLYNÔME ET L'ENSEMBLE $\mathbf{K}[X]$

L'ensemble $\mathbf{K}^{(\mathbf{N})}$ 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 $\mathbf{K}$.

7. ÉCRITURE D'UN POLYNÔME COMME COMBINAISON LINÉAIRE DE PUISSANCES DE X

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

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

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

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

Remarque 1. — Dans la suite, nous écrirons les polynômes sous l'une des formes $(\star)$ ou $(\star\star)$, et plus comme des suites presque nulles d'éléments de $\mathbf{K}$. ■

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 :

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

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

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

9. NOUVELLES EXPRESSIONS DES OPÉRATIONS SUR LES POLYNÔMES

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

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

MULTIPLICATION PAR UN SCALAIRE ·. — Pour tout $\lambda\in\mathbf{K}$, pour tout $P\in\mathbf{K}[X]$

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

On a donc

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

MULTIPLICATION INTERNE ×. — 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

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

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

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

10. STRUCTURE DE L'ENSEMBLE DES POLYNÔMES À COEFFICIENTS DANS K

THÉORÈME 2 (STRUCTURE SUR L'ENSEMBLE DES POLYNÔMES À COEFFICIENTS DANS 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* $\left(X^i\right)_{i\in\mathbf{N}}$ *est une base.*
2. $(\mathbf{K}[X],+,\times)$ *est un anneau commutatif.*
3. $(\mathbf{K}[X],+,\times,\cdot)$ *est une* $\mathbf{K}$*-algèbre.*

Remarque 3 (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. ■

EXERCICE 4. —

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

□

EXERCICE 5 (FORMULE DES COMITÉS). — 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 à l'aide de la formule du binôme de Newton. En proposer une généralisation. □

§ 2. DEGRÉ

DÉFINITION 6 (DEGRÉ). — *Soit*

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

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

$$\deg(0) = -\infty.$$

2. *Si dans* $(\star)$ *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*

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

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

Remarque 7. — Le degré d'un polynôme est un élément de l'ensemble $\mathbf{N} \cup \{-\infty\}$ et :

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

■

DÉFINITION 8 (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* $[P]_{\deg(P)}$, *qui est par définition non nul, est appelé coefficient dominant de* P. *On le note On le note* $\operatorname{dom}(P)$.
2. *Si* $\operatorname{dom}(P) = 1$, *alors* P *est dit unitaire.*

Remarque 9 (polynôme normalisé). — Si $P \in \mathbf{K}[X] \setminus \{0\}$, alors le polynôme

$$\widehat{P} := \frac{1}{\operatorname{dom}(P)} P$$

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

PROPOSITION 10 (PROPRIÉTÉS DU DEGRÉ). — *On étend la relation d'ordre usuelle* $\leqslant$ *et l'addition* $+$ *sur* $\mathbf{N}$ *à* $\mathbf{N} \cup \{-\infty\}$ *en posant, pour tout* $(n, m) \in (\mathbf{N} \cup \{-\infty\})^2$ *:*

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

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

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

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

PROPOSITION 11 (INTÉGRITÉ DE $\mathbf{K}[X]$). — *L'anneau* $(\mathbf{K}[X],+,\times)$ *est intègre.*

EXERCICE 12 (COEFFICIENT DOMINANT D'UN PRODUIT DE POLYNÔMES). — Soient $P,Q\in\mathbf{K}[X]$ des polynômes non nuls. Démontrer : $\mathrm{dom}(PQ)=\mathrm{dom}(P)\,\mathrm{dom}(Q)$. □

EXERCICE 13 (DEGRÉ ET COEFFICIENT DOMINANT D'UNE COMPOSÉE DE POLYNÔMES). — Soit $(P,Q)\in\mathbf{K}[X]^2$. On suppose que $\deg(Q)\geqslant 1$.

1. Démontrer que : $\deg(P\circ Q)=\deg(P)\deg(Q)$.
2. Conjecturer puis démontrer un résultat concernant $\mathrm{dom}(P\circ Q)$.

□

EXERCICE 14 (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 $P\left(X^2\right)=X^2P$ 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 $P\circ Q=X$.

□

QUESTION. — Soit $n\in\mathbf{N}$. L'ensemble $\left\{P\in\mathbf{K}[X]\ :\ \deg(P)=n\right\}$ est-il un sous-espace vectoriel de $\mathbf{K}[X]$?

DÉFINITION 15 ($\mathbf{K}_n[X]$). — *Pour tout* $n\in\mathbf{N}$ *on pose :*

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

THÉORÈME 16 (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* $n+1$.

EXERCICE 17 ($\mathbf{K}[X]$ 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. □

THÉORÈME 18 (DES DEGRÉS ÉCHELONNÉS DANS $\mathbf{K}_n[X]$). — *Soit* $n\in\mathbf{N}$. *Toute famille* $(P_0,P_1,\dots,P_n)\in\mathbf{K}[X]^{n+1}$ *vérifiant*

$$\forall\, k\in[\![0,n]\!]\qquad \deg(P_k)=k$$

est une base de $\mathbf{K}_n[X]$.

THÉORÈME 19 (DES DEGRÉS ÉCHELONNÉS DANS $\mathbf{K}[X]$). — *Toute famille* $(P_n)_{n\in\mathbf{N}}\in\mathbf{K}[X]^{\mathbf{N}}$ *vérifiant*

$$\forall\, n\in\mathbf{N}\qquad \deg(P_n)=n$$

est une base de $\mathbf{K}[X]$.

§ 3. DIVISION EUCLIDIENNE

THÉORÈME 20 (DIVISION EUCLIDIENNE DANS $\mathbf{K}[X]$). — *Soit $(A,B) \in \mathbf{K}[X]^2$ tel que $B \neq 0_{\mathbf{K}[X]}$. Alors, existe un unique couple $(Q,R) \in \mathbf{K}[X]^2$ tel que*

$$\begin{cases} & A = BQ + R \\ \underline{et} & \\ & \deg(R) < \deg(B). \end{cases}$$

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

EXERCICE 21. — Effectuer la division euclidienne de $A := X^5 + X^4 + X^3 + X^2 + X + \alpha$ par $B := X^2 + X + 1$, où $\alpha \in \mathbf{K}$. □

DÉFINITION 22 (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 $A = BQ$.*

EXERCICE 23. — 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 :

$$A \text{ divise } B \implies \deg(A) \leqslant \deg(B)\ .$$

La réciproque est-elle vraie ?

□

PROPOSITION 24 (CRITÈRE DE DIVISIBILITÉ VIA LA DIVISION EUCLIDIENNE). — *Soit $(A,B) \in \mathbf{K}[X]^2$. On suppose $B \neq 0_{\mathbf{K}[X]}$. Alors :*

$$B \mid A \iff \textit{le reste de la division euclidienne de } A \textit{ par } B \textit{ est nul.}$$

EXERCICE 25. — 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 26. — 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 27. —

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 $P(b)$.

□

EXERCICE 28. — Soit $B \in \mathbf{K}[X]$ de degré $n \geqslant 1$. Soit

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

1. Démontrer que f est une application bien définie, qui est linéaire et surjective.
2. Est-elle injective ?
3. Déterminer son noyau.

□

§ 4. POLYNÔME DÉRIVÉ

NOTATION. — Ici la lettre **K** désigne un sous-corps de **C**.

DÉFINITION 29 (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*

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

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

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

Remarque 30 (degré du polynôme dérivé). — Soit $P \in \mathbf{K}[X]$. Alors

$$\deg\left(P'\right) = \begin{cases} -\infty & \text{si} \quad \deg(P) \leqslant 0 \\ \deg(P) - 1 & \text{si} \quad \deg(P) \geqslant 1. \end{cases}$$

■

PROPOSITION 31 (LINÉARITÉ DE LA DÉRIVATION DE POLYNÔMES). — *L'application*

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

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

THÉORÈME 32 (DÉRIVÉES DE PRODUITS DE POLYNÔMES ET FORMULE DE LEIBNIZ). —

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

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

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

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

3. *Soient* $(P, Q) \in \mathbf{K}[X]^2$. *Pour tout* $n \in \mathbf{N}^*$ *:*

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)}\, Q^{(n-k)} \qquad [\textit{formule de Leibniz}].$$

DÉMONSTRATION. —

1. Les deux applications :

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

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

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

et

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

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 $(i,j)\in\mathbf{N}^2$, $f\left(X^i,X^j\right)=g\left(X^i,X^j\right)$. Nous calculons :

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

et

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

pour conclure.

2. Nous raisonnons par récurrence sur le nombre de polynômes en jeu.
Pour tout $n\in\mathbf{N}_{\geqslant 2}$, nous définissons le prédicat $\mathscr{P}(n)$ par :

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

Le prédicat $\mathscr{P}(2)$ est vrai, d'après la propriété 1.
Soit $n\in\mathbf{N}_{\geqslant 2}$ tel que $\mathscr{P}(n)$ 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 $\displaystyle\sum_{j=1}^{n+1}P_j'\left(\prod_{\substack{i=1\\ i\neq j}}^{n+1}P_i\right)$, 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 $\mathscr{P}(n)$ par :

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

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

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

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 $\displaystyle\sum_{k=1}^{n+1}\binom{n}{k-1}P^{(k)}\,Q^{(n+1-k)}$, 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 $k \in [\![1,n]\!]$, $\binom{n}{k-1}+\binom{n}{k}=\binom{n+1}{k}$ (relation de Pascal), $\binom{n}{n}=1=\binom{n+1}{n+1}$ et $\binom{n}{0}=1=\binom{n+1}{0}$, nous pouvons conclure :

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

■

LEMME 33 (POLYNÔMES DÉRIVÉS ITÉRÉS DE $(X-a)^k$). — *Soit $(k,\ell,a)\in \mathbf{N}^*\times\mathbf{N}\times\mathbf{K}$.*

$$\left[(X-a)^k\right]^{(\ell)}=\begin{cases}\dfrac{k!}{(k-\ell)!}(X-a)^{k-\ell} & \text{si } \ell\leqslant k\\ 0 & \text{si } \ell>k\,.\end{cases}$$

DÉMONSTRATION. — Nous raisonnons par récurrence.

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

$$\forall\,\ell\in\mathbf{N},\qquad \left[(X-a)^k\right]^{(\ell)}=\begin{cases}\dfrac{k!}{(k-\ell)!}(X-a)^{k-\ell} & \text{si } \ell\leqslant k\\ 0 & \text{si } \ell>k\,.\end{cases}$$

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

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

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 $\mathscr{P}(1)$ est vraie.

• Hérédité. Supposons $\mathscr{P}(k)$ vraie pour un $k\in\mathbf{N}$ fixé et démontrons $\mathscr{P}(k+1)$.

– Comme $\deg\left((X-a)^{k+1}\right)=k+1$, pour tout $\ell>k+1$:

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

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

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

D'où

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

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

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

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

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

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

■

THÉORÈME 34 (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 $\left((X-a)^k\right)_{k\in[\![0,n]\!]}$ 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 $\ell \in [\![1, n]\!]$. On dérive ℓ fois le polynôme P et on applique le lemme précédent pour obtenir :

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

En évaluant en a, il vient :

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

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

■

EXERCICE 35. —

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

□

EXERCICE 36. — Soit $n \in \mathbf{N}$. Soit $a \in \mathbf{K}$.

1. Justifier que la famille $\mathscr{B}_a := \left(1, X-a, (X-a)^2, \dots, (X-a)^n\right)$ 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 $\mathscr{B}_a$?

□

§ 5. RACINES D'UN POLYNÔME

DÉFINITION 37 (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 $P(\alpha) = 0$.*

DÉFINITION 38 (SPECTRE D'UN POLYNÔME). — *Soit $P \in \mathbf{K}[X]$. On note $\mathrm{Spec}_{\mathbf{K}}(P)$ l'ensemble des racines de P dans $\mathbf{K}$, i.e. :*

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

Remarque 39 (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 $\mathrm{Spec}_{\mathbf{L}}(P)$ l'ensemble des racines de P (considéré comme polynôme à coefficients dans $\mathbf{L}$) dans $\mathbf{L}$:

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

On a naturellement l'inclusion :

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

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

EXERCICE 40 (SPECTRE RÉEL ET COMPLEXE DE $X^n + X^{n-1} + \ldots + X + 1$). — Soient $n \in \mathbf{N}^*$ et $P = \sum_{k=0}^{n} X^k$. Déterminer $\mathrm{Spec}_{\mathbf{R}}(P)$ et $\mathrm{Spec}_{\mathbf{C}}(P)$. □

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 $\mathrm{Spec}(P)$.

PROPOSITION 41 (CRITÈRE POUR ÊTRE UNE RACINE VIA LA DIVISIBILITÉ)). — *Soit $P \in \mathbf{K}[X]$. Soit $\alpha \in \mathbf{K}$. Alors :*

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

PROPOSITION 42 (FACTORISATION D'UN POLYNÔME POSSÉDANT n RACINES DISTINCTES). — *Soit $P \in \mathbf{K}[X]$. Soient $\alpha_1, \ldots, \alpha_n$ des éléments de $\mathbf{K}$ deux-à-deux distincts. Alors :*

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

COROLLAIRE 43 (NOMBRE MAXIMAL DE RACINES D'UN POLYNÔME NON NUL). — *Tout polynôme non nul de $\mathbf{K}[X]$ possède au plus $\deg(P)$ racines dans $\mathbf{K}$.*

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

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

Le polynôme P étant non nul, Q l'est également. Donc $\deg(P) = n + 1 + \deg(Q)$ et $\deg(Q) \geqslant 0$. Ainsi $\deg(P) \geqslant n + 1$. Contradiction. ■

COROLLAIRE 44 (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 $P = 0$.*

HYPOTHÈSE SUR LE CORPS K. — Dans la suite, on suppose que $\mathbf{K}$ est un sous-corps de $\mathbf{C}$. Alors :

- pour tout $n \in \mathbf{Z}$, $n \neq 0$ dans $\mathbf{K}$;
- le corps $\mathbf{K}$ contient $\mathbf{Q}$ et est donc infini.

PROPOSITION 45 (POLYNÔME VERSUS FONCTION POLYNOMIALE). — *Si $P \in \mathbf{K}[X]$, on lui associe la fonction*

$$\widetilde{P} \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ x & \longmapsto & P(x)\,. \end{array} \right.$$

L'application

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

est injective.

DÉMONSTRATION. — L'application φ est clairement linéaire. Démontrons que son noyau est réduit au polynôme nul. Soit $P \in \mathbf{K}[X]$ tel que $\widetilde{P} = 0$. 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). ■

Remarque 46 (identification entre polynôme et fonction polynomiale). — Une fonction de $\mathbf{K}$ dans $\mathbf{K}$ est dite polynomiale si elle est égale à $\widetilde{P}$, pour un $P \in \mathbf{K}[X]$. En d'autre 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 $\widetilde{P}$. ■

EXERCICE 47 (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 $\mathbb{F}_p$. On peut donc considérer la $\mathbb{F}_p$-algèbre $\mathbb{F}_p[X]$ des polynômes à coefficients dans $\mathbb{F}_p$. Soit $P = X \in \mathbb{F}_p[X]$ et $Q = X^p \in \mathbb{F}_p[X]$. Comparer les deux applications :

$$\widehat{P} \left| \begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & P(x) \end{array} \right. \quad \text{et} \quad \widehat{Q} \left| \begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & Q(x) \end{array} \right.$$

et commenter. □

EXERCICE 48 (DÉTERMINANT DE VANDERMONDE). — Si $n \in \mathbf{N}_{\geqslant 2}$ 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 $\left((\alpha_j)^{i-1}\right)_{1\leqslant i,j\leqslant n}$.

1. Soient $\alpha_1,\dots,\alpha_n$ des scalaires deux-à-deux distincts.
   (a) Justifier que la fonction
   $$P \left| \begin{array}{ccc} \mathbf{K} & \longrightarrow & \mathbf{K} \\ x & \longmapsto & V(\alpha_1,\dots,\alpha_n,x) \end{array} \right.$$
   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 $(\alpha_1,\dots,\alpha_n) \in \mathbf{K}^n$:
   $$V(\alpha_1,\dots,\alpha_n) = \prod_{1\leqslant i<j\leqslant n} (\alpha_j - \alpha_i) \qquad \text{[formule à connaître]}\,.$$

□

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

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

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

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-ème 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 $1\leqslant k\leqslant n$, la fonction P est polynomiale de degré inférieur ou égal à n et son coefficient devant x^n est :

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

1.(b) Soit $k\in[\![1,n]\!]$. 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

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

2. Nous raisonnons par récurrence sur l'entier $n\geqslant 2$.

- Définition du prédicat. Nous posons, pour tout $n\in\mathbf{N}_{\geqslant 2}$:

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

- Initialisation à $n=2$.

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

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

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

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

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

DÉFINITION 49 (POLYNÔME DE $\mathbf{K}[X]$ SCINDÉ SUR $\mathbf{K}$). — *Soit $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$. On dit que P est scindé sur $\mathbf{K}$ s'il existe $\alpha_1, \dots, \alpha_n \in \mathbf{K}$ tels que*

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

Remarque 50 (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). ■

Exemple 51. —

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 $\mathbf{C}$.

■

Le caractère scindé d'un polynôme dépendant du corps considéré, on évitera de parler de polynôme scindé sans préciser de corps, pour préférer l'expression : le polynôme est scindé sur tel corps.

EXERCICE 52. — Soit $(a, b, c) \in \mathbf{K}^3$, 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.

□

THÉORÈME 53 (DE D'ALEMBERT-GAUSS). — *Tout polynôme de $\mathbf{C}[X]$ de degré supérieur ou égal à 1 possède au moins une racine dans $\mathbf{C}$.*

COROLLAIRE 54 (TOUT POLYNÔME DE $\mathbf{C}[X]$ EST SCINDÉ SUR $\mathbf{C}$). — *Soit $P \in \mathbf{C}[X]$ tel que $\deg(P) \geqslant 1$. Alors P est scindé sur $\mathbf{C}$, i.e. il existe et $(\alpha_1, \dots, \alpha_n) \in \mathbf{C}^n$ tels que*

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

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

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

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

DÉFINITION 55 (ORDRE DE MULTIPLICITÉ D'UNE RACINE). — *Soit $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$. Soit $\alpha \in \mathbf{K}$ une racine de P. L'ensemble*

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

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

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

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

Remarque 56. — Soit $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$, soit $\alpha \in \mathbf{K}$ une racine de P. Alors $1 \leqslant \mathrm{mult}(\alpha, P) \leqslant \deg(P)$. ■

THÉORÈME 57 (CARACTÉRISATION DE L'ORDRE DE MULTIPLICITÉ D'UNE RACINE). — *Soient $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$, $\alpha \in \mathbf{K}$ une racine de P. et $n \in [\![1, \deg(P)]\!]$. Les assertions suivantes sont équivalentes.*

1. $n = \mathrm{mult}(\alpha, P)$
2. *$(X-a)^n$ divise P et $(X-a)^{n+1}$ ne divise pas P.*
3. *Pour tout $k \in [\![0, n-1]\!]$, $P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$.*

DÉMONSTRATION. — Soit $\mathscr{E} := \left\{k \in \mathbf{N}^* \ : \ (X-\alpha)^k \text{ divise } P\right\}$. Ainsi, $\mathrm{mult}(\alpha, P) = \max(\mathscr{E})$.

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

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

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

$$P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k = \underbrace{\sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!}(X-a)^k}_{\text{degré < n}} + \sum_{k=n}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

$$\underset{(\star)}{=} (X-a)^n \underbrace{\left(\sum_{k=n}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^{\overbrace{k-n}^{\geqslant 0}}\right)}_{\text{quotient}} + \underbrace{\sum_{k=0}^{n-1} \frac{P^{(k)}(a)}{k!}(X-a)^k}_{\text{reste}}$$

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 $\left((X-a)^k\right)_{k \in [\![0,n-1]\!]}$ est une famille libre de polynômes (théorème des degrés échelonnés), $P^{(k)}(a) = 0$ pour tout $k \in [\![0, n-1]\!]$.
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 $n = \deg(P)$ (dans ce cas l'identité $(\star)$ livrerait $P = 0$) donc $\deg(P) \geqslant n+1$ et

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

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

$3 \Rightarrow 2$. Supposons que pour tout $k \in [\![0, n-1]\!]$, $P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$. Alors $\deg(P) \geqslant n$ (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

$$P = \sum_{k=n}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^k \underset{(\star\star)}{=} (X-a)^n \left(\sum_{k=n}^{\deg(P)} \frac{P^{(k)}(a)}{k!}(X-a)^{\overbrace{k-n}^{\geqslant 0}} \right).$$

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

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

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

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

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

EXERCICE 58 (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

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

où

- $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont des les racines deux-à-deux distinctes de P dans $\mathbf{K}$;
- $n_1, n_2, \ldots, n_r$ sont des entiers naturels non nuls.

Préciser l'ordre de multiplicité de la racine α_k de P, pour tout $k \in [\![1, r]\!]$. □

EXERCICE 59 (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 $\overline{\alpha}$ est également racine de P.
2. Démontrer $\operatorname{mult}(\alpha, P) = \operatorname{mult}\left(\overline{\alpha}, P\right)$.

□

EXERCICE 60 (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 $\alpha_1, \ldots, \alpha_n$ 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?

□

EXERCICE 61. — Démontrer qu'il n'existe pas de triplet (a, b, c) de nombres réels tels que

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

□

EXERCICE 62 (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 $\prod_{k=1}^{n} \sin\left(\dfrac{k\pi}{n+1}\right)$. □

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

THÉORÈME 63 (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*

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

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

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

et

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

§ 6. IDÉAUX DE $\mathbf{K}[X]$

1. IDÉAL D'UN ANNEAU COMMUTATIF

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

DÉFINITION 64 (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) $\forall\, a \in A, \quad \forall\, x \in I, \quad ax \in I$.

PROPOSITION 65 (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 :

$$\forall\, a \in A, \quad \forall\, x \in I, \quad ax \in I.$$

PROPOSITION 66 (OPÉRATIONS SUR LES IDÉAUX). — *Soit $I_1, I_2, \ldots, I_n$ des idéaux de A.*

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

2. EXEMPLES D'IDÉAUX DE $\mathbf{K}[X]$

Exemple 67 (idéaux triviaux de $\mathbf{K}[X]$). — Les parties $\{0\}$ et $\mathbf{K}[X]$ sont des idéaux de $\mathbf{K}[X]$, appelés idéaux triviaux. ■

EXERCICE 68 (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 $B\mathbf{K}[X]$.

□

EXERCICE 69 (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 :
$$A \text{ et } B \text{ sont associés} \iff A\mathbf{K}[X] = B\mathbf{K}[X]\,.$$

□

EXERCICE 70. — 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 élements distincts de $\mathbf{K}$. Démontrer que $Z(a) + Z(b) = \mathbf{K}[X]$.

□

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

EXERCICE 71. — Justifier que $I := \{P \in \mathbf{K}[X] \,:\, P(0) = P(1) = 0\}$ est un idéal de $\mathbf{K}[X]$. □

3. DESCRIPTION DES IDÉAUX DE $\mathbf{K}[X]$

THÉORÈME 72 (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 un générateur de l'idéal I.

Remarque 73 (raffinement du précédent théorème). —

1. D'après l'exercice 68 et le théorème 72, 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 72, 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 69, 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.

■

EXERCICE 74. — 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

1. NOTIONS DE PGCD ET DE PPCM

DÉFINITION 75 (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*
$$A\mathbf{K}[X]\cap B\mathbf{K}[X]=(A\vee B)\,\mathbf{K}[X].$$

PROPOSITION 76 (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.

Exemple 77 (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 $A\vee B=\widehat{A}$.

■

EXERCICE 78 (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 $A\vee B=\widehat{A}\vee\widehat{B}$. □

DÉFINITION 79 (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* $A_1A_2\dots A_n\neq 0$*). 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*
$$A_1\mathbf{K}[X]\cap A_2\mathbf{K}[X]\cap\dots\cap A_n\mathbf{K}[X]=(A_1\vee A_2\vee\dots\vee A_n)\,\mathbf{K}[X].$$

Remarque 80 (lecture sur une décomposition en produit d'irréductibles). — Soit $(A,B)\in(\mathbf{K}[X]\setminus\{0\})^2$. Supposons que nous connaissions « la » décomposition de A et B en produit d'irréductibles. Quitte à autoriser des exposants nuls, nous pouvons écrire
$$A=\lambda P_1^{r_1}P_2^{r_2}\dots P_n^{r_n}\qquad\text{et}\qquad B=\mu P_1^{s_1}P_2^{s_2}\dots P_n^{s_n}$$
où

- $\lambda,\mu\in\mathbf{K}^*$;
- $P_1,P_2,\dots,P_n$ sont des polynômes irréductibles sur $\mathbf{K}$, unitaires, deux à deux distincts (ou deux à deux non associés, ce qui revient au même car ils sont unitaires) ;
- $r_1,r_2,\dots,r_n,s_1,s_2,\dots,s_n$ sont des entiers naturels (possiblement nuls ici).

Alors
$$A\wedge B=\prod_{k=1}^{n}P_k^{\min(r_k,s_k)}\qquad\text{et}\qquad A\vee B=\prod_{k=1}^{n}P_k^{\max(r_k,s_k)}.$$

■

2. PRIMALITÉ RELATIVE

DÉFINITION 81 (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 $A \wedge B = 1$.*

THÉORÈME 82 (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.

Exemple 83 (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. ■

EXERCICE 84. — 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 $C = A \wedge B$?

□

LEMME 85 (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.*

LEMME 86 (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 $(n,m) \in \mathbf{N}^* \times \mathbf{N}^*$.*

EXERCICE 87 (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 $A = A_0 D$ et $B = B_0 D$. Démontrer : $A_0 \wedge B_0 = 1$. □

THÉORÈME 88 (DE GAUSS). — *Soit $(A,B,C) \in (\mathbf{K}[X] \setminus \{0\})^3$. Alors*

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

PROPOSITION 89 (PRODUIT DU PGCD ET DU PPCM)). — *Soient $A \in \mathbf{K}[X]$ et $B \in \mathbf{K}[X]$ des polynômes unitaires. Alors*

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

3. UNE MÉTHODE DE CALCUL DU PGCD ET DU PPCM

Remarque 90 (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. ■

LEMME 91 (CLÉ POUR L'ALGORITHME D'EUCLIDE). — *Soit $(A,B) \in \mathbf{K}[X]^2$ tel que $A \neq 0$ et $\deg(B) \geqslant 1$. 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*

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

ALGORITHME 92 (ALGORITHME D'EUCLIDE POUR LE CALCUL DU PGCD). — *Soit $A \in \mathbf{K}[X] \setminus \{0\}$ et $B \in \mathbf{K}[X]$ tel que $\deg(() B) \geqslant 1$. 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 :*

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

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

⟶ *Si $\deg(R_1) = 0$, i.e. si R_1 est un polynôme constant non nul, alors $A \wedge B = 1$ et on s'arrête.*

⟶ *Si $\deg(R_1) \geqslant 1$, alors $\boxed{A \wedge B = B \wedge R_1}$ et on continue.*

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

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

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

⟶ *Si $\deg(R_2) = 0$, 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 $\boxed{A \wedge B = B \wedge R_1 = R_1 \wedge R_2}$ 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

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

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

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

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

⟶ *Si $\deg(R_{n+1}) = 0$, 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 $\boxed{A \wedge B = R_{n-1} \wedge R_n = R_n \wedge R_{n+1}}$ et on continue.*

PROPOSITION 93 (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 déroissante

$$\deg(B) > \deg(R_1) > \deg(R_2) > \ldots > \deg(R_n) > \deg(R_{n+1}) > \ldots$$

ce qui n'est pas possible. ■

PROPOSITION 94 (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

$$\deg\left(R_{n_0}\right) = 0 \quad \text{et } \deg(R_k) \neq 0, \text{ pour tout } k \in [\![1, n_0 - 1]\!].$$

On a

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

Le PGCD de A et B est donc calculé. ■

Méthode 95 (pour obtenir une relation de Bézout). — On considère de nouveau l'algorithme d'Euclide 92. À partir des divisions euclidiennes encadrées, nous pouvons former une relation de Bézout en « remontant » l'algorithme. ■

EXERCICE 96 (COMPLEXITÉ DE L'ALGORITHME D'EUCLIDE). — Majorer le nombre de divisions euclidiennes effectuées lors de la mise en œuvre de l'algorithme d'Euclide. □

EXERCICE 97. — Calculer le PGCD et le PPCM de $A = X^5 + 3X^4 + X^3 + 2X^2 + X + 1$ et $B = X^4 + 2X^3 + 3X^2 + 1$. □

EXERCICE 98. — Soient $(a, b) \in \mathbf{K}[X]^2$ et $(n, m) \in (\mathbf{N}^*)^2$. Déterminer $(X - a)^n \wedge (X - b)^m$. □

EXERCICE 99 (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

1. NOTION DE POLYNÔME IRRÉDUCTIBLE SUR UN CORPS

DÉFINITION 100 (POLYNÔME IRRÉDUCTIBLE SUR UN CORPS). — *Soit $P \in \mathbf{K}[X]$. P est dit irréductible sur $\mathbf{K}$ si*

$$\begin{cases} & \deg(P) \geqslant 1 \\ \text{et} & \\ & \forall (P_1, P_2) \in \mathbf{K}[X]^2 \qquad P = P_1 P_2 \Longrightarrow (P_1 \in \mathbf{K}_0[X] \text{ ou } P_2 \in \mathbf{K}_0[X]). \end{cases}$$

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

Remarque 101. — 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 $\mathbf{K}[X]$. ■

Remarque 102 (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). ■

Exemple 103. — Le polynôme $X^2 + 1$ est irréductible sur $\mathbf{R}$, mais réductible sur $\mathbf{C}$. ■

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.

EXERCICE 104 (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 $\deg(P) \in \{2,3\}$. 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 $\mathbf{R}$.

□

LEMME 105 (PGCD DE DEUX POLYNÔMES IRRÉDUCTIBLES). — *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 $\deg(() D) \geqslant 1$. Comme D divise A, il existe $Q \in \mathbf{K}[X]$ tel que $A = DQ$. Comme A est irréductible et $\deg(D) \geqslant 1$, 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. ■

2. DÉCOMPOSITION D'UN POLYNÔME EN PRODUIT DE POLYNÔMES IRRÉDUCTIBLES

THÉORÈME 106 (DÉCOMPOSITION D'UN POLYNÔME EN PRODUIT DE POLYNÔMES IRRÉDUCTIBLES). — *Soit $P \in \mathbf{K}[X]$ tel que $\deg(P) \geqslant 1$.*

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 :*

$$P = \mathrm{dom}(P)\, P_1^{n_1} \dots P_r^{n_r}.$$

2. *Cette décomposition de P en produit de facteurs irréductibles est unique à l'ordre près, i.e. étant donnés $s \in \mathbf{N}^*$, 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 :*

$$P = \mathrm{dom}(P)\, Q_1^{m_1} \dots Q_s^{m_s}$$

alors

- *$r = s$*
- *il existe une bijection $\sigma : [\![1, r]\!] \longrightarrow [\![1, r]\!]$ telle que*

$$\forall i \in [\![1, r]\!] \qquad Q_i = P_{\sigma(i)} \quad et \quad m_i = n_{\sigma(i)}.$$

DÉMONSTRATION. — Quitte à remplacer P par son normalisé, on peut supposer que $\mathrm{dom}(P) = 1$.

- Existence. On raisonne par récurrence forte sur le degré de P. Pour tout $d \in \mathbf{N}^*$, notons $\mathscr{P}(d)$ 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 $\deg(P) = 1$. 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 $\mathscr{P}(k)$ vraie pour tout $k \in [\![1, d]\!]$. 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 $P = AB$, $\deg(A) \geqslant 1$ et $\deg(B) \geqslant 1$. Puisque

$$\deg(A) + \deg(B) = \deg(AB) = \deg(P) = d + 1$$

nous en déduisons $\deg(A) \in [\![1,d]\!]$ et $\deg(B) \in [\![1,d]\!]$. 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

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

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 ($i \in [\![1,r]\!]$, $j \in [\![1,s]\!]$), 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 $n_1 \geqslant 1$), 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 105, $P_1 = Q_1$. D'après le lemme 105 et le lemme 86, $P_1^{n_1}$ est premier avec les polynômes $Q_2^{m_2},\dots,Q_s^{m_s}$. Grâce au lemme 85, 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 $n_1 \leqslant m_1$. 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, $j \in [\![1,s]\!]$.

■

EXERCICE 107. — 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 ? □

3. IRRÉDUCTIBLES DE $\mathbf{C}[X]$ ET IRRÉDUCTIBLES DE $\mathbf{R}[X]$

THÉORÈME 108 (DESCRIPTION DES IRRÉDUCTIBLES DE $\mathbf{C}[X]$ (RESP. $\mathbf{R}[X]$)). —

1. *Soit $P \in \mathbf{C}[X]$.*
$$P \text{ est irréductible sur } \mathbf{C} \iff \deg(P) = 1.$$
2. *Soit $P \in \mathbf{R}[X]$.*
$$P \text{ est irréductible sur } \mathbf{R} \iff \left|\begin{array}{l} \deg(P) = 1 \\ \text{ou} \\ P \text{ est de degré 2 et de discriminant strictement négatif.}\end{array}\right.$$

4. DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{C}[X]$

COROLLAIRE 109 (DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{C}[X]$). — *Soit $P \in \mathbf{C}[X]$ tel que $\deg(P) \geqslant 1$. La décomposition de P en produit de facteurs irréductibles dans $\mathbf{C}[X]$ est « de la forme »*

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

où

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

DÉMONSTRATION. — Il s'agit d'une conséquence des théorèmes 106 et 108. ■

***Remarque 110.* —** L'entier r est le nombre de racines complexes deux-à-deux distinctes de P, les complexes $\alpha_1, \ldots, \alpha_r$ sont les racines complexes deux-à-deux distinctes de P et pour tout $k \in [\![1, r]\!]$, n_k est l'ordre de multiplicité de la racine α_k de P. ■

***Remarque 111.* —** Soit $P \in \mathbf{C}[X]$ de degré supérieur ou égale à 1. Soient $\alpha_1, \ldots, \alpha_r$ les racines complexes deux-à-deux distinctes de P et $n_1, \ldots, n_r$ leurs multiplicités respectives. Alors, dans le corps des fractions rationnelles $\mathbf{C}(X)$:

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

■

5. DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{R}[X]$

COROLLAIRE 112 (DÉCOMPOSITION EN PRODUIT D'IRRÉDUCTIBLES DANS $\mathbf{R}[X]$). — *Soit $P \in \mathbf{R}[X]$ tel que $\deg(P) \geqslant 1$. 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 $\mathbf{R}$*

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

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

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

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

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

où

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

DÉMONSTRATION. — Il s'agit d'une conséquence des théorèmes 106 et 108. ■

EXERCICE 113. — Décomposer le polynôme $P = X^4 + 16$ en produit d'irréductibles dans $\mathbf{C}[X]$, puis dans $\mathbf{R}[X]$. □

EXERCICE 114. — Soit $n \in \mathbf{N}_{\geqslant 2}$. 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 $\mathbf{R}[X]$.

□