Polynômes et fractions rationnelles

Dans tout ce qui suit, $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$. Les applications de ce champ sont innombrables dans tous les champs des mathématiques.

1 Anneau des polynômes à une indéterminée.

Les polynômes sont introduits dans le secondaire via les fonctions polynomiales. Ces deux notions sont en réalité distinctes et la notion de polynôme est plus abstraite, intrinsèquement liée à la suite de ses coefficients. Prenons le cas du corps $\mathbb{K}$ à deux éléments $\{0,1\}$. Sur ce corps, le polynôme $X^2 - X$ est un polynôme non nul de degré 2. Pourtant, $0^2 = 0$ et $1^2 = 1$, donc sa fonction polynomiale est nulle. Rappelons que $\mathbb{K}^{\mathbb{N}}$ désigne l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{K}$, i.e des suites à valeurs dans $\mathbb{K}$.

1.1 Opérations dans $\mathbb{K}[X]$.

Définition 1 *Soit $(p_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ une suite numérique. On dit qu'elle est à support fini (ou presque nulle) lorsque*

$$\exists N \in \mathbb{N}, \forall n \geq N, p_n = 0$$

L'ensemble de ces suites est noté $\mathbb{K}^{(\mathbb{N})}$.

☞ **Remarque**
L'intérêt de ces suites apparaît lors de procédés de sommations. On peut sommer sur tous les entiers sans qu'il y ait de souci de définition ou de convergence.

Théorème 1 (admis) *Il existe un objet X appelé indéterminée et un ensemble, noté $\mathbb{K}[X]$, muni d'une addition et d'une multiplication vérifiant les points suivants :*

- $\forall P \in \mathbb{K}[X], \exists!(p_n)_{n\in\mathbb{N}} \in K^{(\mathbb{N})}, P = \sum_{n=0}^{+\infty} p_n X^n$.
- *Les règles algébriques usuelles sur l'addition et la multiplication dans $\mathbb{K}$ se prolongent sur $\mathbb{K}[X]$.*

Les éléments de $\mathbb{K}[X]$ sont appelés polynômes à coefficients dans $\mathbb{K}$.

☞ **Remarque**
Soit $P \in \mathbb{K}[X]$. En notant P sous la forme unique $\sum_{n=0}^{+\infty} p_n X^n$, la suite $(p_n)_{n\in\mathbb{N}}$ est appelée suite des coefficients de P. Elle caractérise entièrement le polynôme P.

Exemple 1 *Soit $a \in \mathbb{K}$ un scalaire. On peut l'identifier au polynôme constant $P = aX^0 + 0X^1 + \cdots + 0X^n + \ldots$. On appelle polynôme nul le polynôme dont tous les coefficients sont nuls. Les règles de calcul sont transparentes. On peut considérer l'indéterminée X comme un polynôme en l'écrivant sous la forme $0X^0 + 1X^1 + 0X^2 + \ldots$.*

$$2(1 + X^2 - X^3) - (2 + X) = 2 + 2X^2 - 2X^3 - 2 - X = -X + 2X^2 - 2X^3$$

$$(1 + X - X^2)(1 + X) = 1 + X - X^2 + X + X^2 - X^3 = 1 + 2X - X^3$$

Définition 2 *Soit $(P, Q) \in \mathbb{K}[X]^2$. On note $P = \sum_{k=0}^{+\infty} p_k X^k$. On définit alors la composée $P \circ Q$ comme le polynôme $\sum_{k=0}^{+\infty} p_k Q^k$.*

☞ **Remarque**
Cette définition est légitime, puisqu'il s'agit d'une combinaison linéaire de puissances d'un polynôme.

Notation
On peut également noter $P \circ Q$ sous la forme $P(Q)$. On constate alors que $P(X) = P \circ X = P$.

1.2 Degré

Définition 3 *Soit* $P \in \mathbb{K}[X]$. *Si* P *est non nul de coefficients* $(p_k)_{k\in\mathbb{N}}$, *l'entier* $\max\{n \in \mathbb{N}, p_n \neq 0\}$ *est appelé le degré de* P. *Si* $P = 0$, *on convient que son degré vaut* $-\infty$.

Notation
Il est noté $deg(P)$ *ou* d^oP *ou encore* $d(P)$.

Définition 4 *Soit* $P \in \mathbb{K}[X]$ *non nul. Alors son coefficient d'indice* $d(P)$ *est appelé coefficient dominant de* P. *Si ce coefficient dominant vaut* 1, *on dit que* P *est un polynôme unitaire.*

⚠ **Attention**
Ne parlez jamais de coefficient dominant d'un polynôme sans avoir vérifié qu'il est non nul.

Notation
On rencontre la notation $dom(P)$ *pour le coefficient dominant de* P, *mais elle n'a rien d'universelle.*

Propriété 1 *Soit* $(P, Q) \in \mathbb{K}[X]^2$. *Alors*

- $d(P + Q) \leq \max(d(P), d(Q))$. *Il y a égalité si* $d(P) \neq d(Q)$.
- $d(PQ) = d(P) + d(Q)$.
- *Si* $d(Q) \geq 1$, $d(P \circ Q) = d(P)d(Q)$.

Démonstration. Posons $P = \sum_{n=0}^{+\infty} p_n X^n$ et $Q = \sum_{n=0}^{+\infty} q_n X^n$ où $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ sont deux suites numériques à support fini.

- Si l'un des polynômes est nul, l'inégalité est assurée avec la convention $\max(-\infty, n) = n$ pour tout entier naturel n. Sinon, on écrit
$$P + Q = \sum_{n=0}^{+\infty} (p_n + q_n)X^n$$
Pour tout $k \geq \max(d(P), d(Q)) + 1$, $p_k + q_k = 0 + 0 = 0$, donc $d(P + Q) \leq \max(d(P), d(Q))$. Supposons que $d(P) \neq d(Q)$. On se place dans le cas où $d(P) > d(Q)$. Alors P est non nul et son coefficient dominant $p_{d(P)}$ est non nul, tandis que $q_{d(P)}$ est nul, ainsi le coefficient de degré $d(P)$ de $P + Q$ vaut $p_{d(P)}$ et est non nul. Par conséquent, le degré de $P + Q$ vaut $d(P) = \max(d(P), d(Q))$. L'autre cas est symétrique.

  ⚠ **Attention**
  Pour tout entier naturel n, X^n *et* $-X^n$ *sont de degré* n, *mais* $X^n - X^n = 0$ *est de degré* $-\infty$.

- Si l'un des polynômes est nul, l'égalité est assurée avec la convention $n + (-\infty) = -\infty$ pour tout entier naturel n. Sinon
$$PQ = \left(\sum_{k=0}^{+\infty} p_k X^k\right)\left(\sum_{m=0}^{+\infty} q_m X^m\right) = \sum_{k=0}^{+\infty}\sum_{m=0}^{+\infty} p_k q_m X^{m+k}$$
On regroupe alors les termes de même degré
$$PQ = \sum_{n=0}^{+\infty}\left(\sum_{k+m=n} p_k q_m\right)X^n$$
Soit n un entier supérieur ou égal à $d(P) + d(Q) + 1$, soit k et m deux entiers naturels tels que $k + m = n$. Si $k \geq d(P) + 1$, alors $p_k = 0$, donc $p_k q_m = 0$. Sinon, $k \leq d(P)$, donc $m = n - k \geq d(P) + d(Q) + 1 - d(P) = d(Q) + 1$, puis $q_m = 0$ et $p_k q_m = 0$. On en déduit que $\sum_{m+k=n} p_k q_m = 0$. Ainsi, $d(PQ) \leq d(P) + d(Q)$.
Soit k et m deux entiers naturels tels que $k + m = d(P) + d(Q)$. En reprenant les mêmes arguments que précédemment, le seul terme a priori non nul dans la somme est celui pour $k = d(P)$ et $m = d(Q)$, qui vaut alors $p_{d(P)}q_{d(Q)}$ et est effectivement non nul. Conclusion, $d(PQ) = d(P) + d(Q)$.
- Si $P = 0$, alors $P \circ Q = 0$ et on a l'égalité des degrés indiquée. Sinon, on écrit
$$P \circ Q = \sum_{k=0}^{d(P)} p_k Q^k$$
Or pour tout k dans $[\![0, d(P)]\!]$, $d(Q^k) = kd(Q)$ en généralisant l'égalité précédente par récurrence. Comme Q est non constant, tous ces degrés sont différents, donc la somme est du degré de $p_{d(P)}Q^{d(P)}$, puisque $p_{d(P)}$ est non nul. Comme $d(Q^{d(P)}) = d(P)d(Q)$, le résultat s'ensuit.

Exemple 2 *Soit* $P = 1 + X + X^2$ *et* $Q = -1 + X^3$. *Alors* $d(P) = 2$ *et* $d(Q) = 3$. *D'autre part,* $P + Q = X + X^2 + X^3$ *vérifie* $d(P + Q) = 3 = \max(2, 3) = \max(d(P), d(Q))$. *De plus,* $PQ = -1 - X - X^2 + X^3 + X^4 + X^5$ *est de degré* $5 = 2 + 3$. *Enfin,* $P \circ Q = 1 + (1 + X^3) + (1 + X^3)^2 = 3 + 3X^3 + X^6$ *est de degré* $6 = 2 \times 3$.

Exercice 1 *Montrer que l'égalité* $d(P \circ Q) = d(P)d(Q)$ *n'est pas toujours vérifiée si* $d(Q) = 0$.

Propriété 2 (Règle du produit nul) *Soit* $(P, Q) \in \mathbb{K}[X]^2$. *On a l'équivalence* $PQ = 0 \iff (P = 0 \vee Q = 0)$

Démonstration. Soit $(P, Q) \in \mathbb{K}[X]^2$. On suppose que $PQ = 0$ et $P \neq 0$. Alors, $d(PQ) = d(P) + d(Q) = -\infty$. Comme $d(P) \in \mathbb{N}$, on en déduit que $d(Q) = -\infty$, donc $Q = 0$.

Exemple 3 *Soit* $(A, B) \in \mathbb{K}[X]^2$ *tels que* $X^2A = XB$. *Alors* $X(XA - B) = 0$. *Or* $X \neq 0$, *donc* $XA - B = 0$, *i.e* $XA = B$. *On a ainsi pu « simplifier » par* X, *mais il ne s'agit pas d'une division.*

Définition 5 *Soit* n *un entier naturel. On note* $\mathbb{K}_n[X]$ *l'ensemble des polynômes de degré au plus* n.

Propriété 3 *Pour tout entier naturel* n, *l'espace* $\mathbb{K}_n[X]$ *est stable par combinaison linéaire.*

Démonstration. Soit $(P, Q) \in (\mathbb{K}_n[X])^2$, $(\lambda, \mu) \in \mathbb{K}^2$. Alors

$$d(\lambda P + \mu Q) \leq \max(d(\lambda P), d(\mu Q)) = \max(d(\lambda) + d(P), d(\mu) + d(Q)) \leq \max(d(P), d(Q)) \leq n$$

⚠ **Attention**
Pour $n \neq 0$, *il n'est pas stable par produit.*

Propriété 4 *L'ensemble des éléments inversibles de* $\mathbb{K}[X]$ *est l'ensemble des polynômes de degré* 0, *i.e des polynômes constants non nuls.*

Démonstration. Soit P un élément inversible de $\mathbb{K}[X]$. Alors il existe un polynôme Q tel que $PQ = 1$. Alors $d(P) + d(Q) = d(1) = 0$. D'autre part, P et Q ne sont pas nuls, donc $d(P)$ et $d(Q)$ sont des entiers. Par conséquent, $d(P) = 0$. Réciproquement, soit P un polynôme de degré 0. Alors, P est un polynôme constant non nul p_0. Alors le polynôme constant $Q = 1/p_0$ vérifie $QP = PQ = 1$.

1.3 Divisibilité dans $\mathbb{K}[X]$.

Définition 6 *Soit* $(P, Q) \in \mathbb{K}[X]^2$. *On dit que* P *divise* Q *lorsqu'il existe un polynôme* R *dans* $\mathbb{K}[X]$ *tel que* $Q = PR$. *On dit alors que* Q *est un multiple de* P.

Exemple 4 *Soit* $P = 1 + X + X^2 + X^3$ *et* $Q = 1 + X$. *En posant* $R = 1 - X + X^2$, *on constate que* $QR = (1 + X)(1 - X + X^2) = 1 - X + X^2 + X - X^2 + X^3 = 1 + X^3 = P$. *Cela prouve que* Q *divise* P.

Propriété 5 *Soit* $(P, Q) \in \mathbb{K}[X]^2$. *Alors, on a l'équivalence :* P *divise* Q *et* Q *divise* P *si et seulement s'il existe un scalaire* λ *non nul tel que* $P = \lambda Q$. *On dit qu'alors* P *et* Q *sont associés.*

Démonstration. On évacue le cas des polynômes nuls où tout fonctionne bien. Notons R un polynôme tel que $PR = Q$, alors $d(P) + d(R) = d(Q)$. Comme les degrés sont des entiers naturels, on en déduit que $d(P) \geq d(Q)$. L'autre relation de divisibilité fournit $d(P) \leq d(Q)$. On en déduit que $d(P) = d(Q)$, donc que $d(R) = 0$, i.e R est un polynôme constant non nul. Réciproquement, si P est de la forme λQ avec λ un scalaire non nul, alors les polynômes constants λ et $1/\lambda$ donnent les relations de divisibilité attendues.

Théorème 2 (Théorème de la division euclidienne) *Soit* $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$. *Alors il existe un unique couple* (Q, R) *de polynômes tel que*

$$A = BQ + R \quad et \quad [d(R) < d(B)]$$

Le polynôme Q *est appelé le quotient de la division euclidienne de* A *par* B, *le polynôme* R *est appelé le reste de la division euclidienne de* A *par* B.

Exemple 5 *Produire le schéma de division euclidienne en tableau.*
Soit $A = 2 - X + X^2 + X^3$ *et* $B = 1 - X$. *Pour effectuer la division euclidienne, on compare les termes dominants de* A *et* B. $A = 2 - X + X^2 + X^3 - X^2B + X^2(1 - X) = -X^2B + 2 - X + X^2 + X^3 + X^2 - X^3 = -X^2B + 2 - X + 2X^2$. *On recommence avec* $A_1 = 2 - X + X^2$ *et* $B = 1 - X$. $A_1 = -XB + 2 - X + X^2 + X(1 - X) = -XB + 2 - X + X^2 + X - X^2 = -XB + 2$. *Enfin,* $2 = 0 \times B + 2$ *et* $d(2) = 0 < 1 = d(B)$. *Ainsi,* $A = (-X^2 - X)B + 2$ *est l'écriture recherchée en posant* $Q = -X - X^2$ *et* $R = 2$.

Démonstration. Si A est nul, il suffit de choisir $(Q,R)=(0,0)$. On prouve l'existence par récurrence forte. Pour tout tout entier naturel n, on note $\mathcal{H}_n$ l'assertion : « $\forall A\in\mathbb{K}[X], d(A)=n, \exists (Q,R)\in\mathbb{K}[X], A=QB+R\wedge d(R)<d(B)$ ».
Initialisation : $n=0$. Si $d(B)>0$, on choisit $(Q,R)=(0,A)$. Si $d(B)=0$, alors B est constant non nul et il suffit de choisir $(Q,R)=(A/B,0)$.
Hérédité. Soit $n\in\mathbb{N}$ tel que $\forall k\in[\![0,n]\!], \mathcal{H}_k$. Soit $A\in\mathbb{K}[X]$ tel que $d(A)=n+1$, on note $A=aX^{n+1}+A'$ avec $a\neq 0$ et $A'\in\mathbb{K}_n[X]$. On écrit également $B=bX^p+B'$ avec $p=d(B)$, $b\neq 0$ et $B'\in\mathbb{K}_{p-1}[X]$.
Si $p>n+1$, alors on propose $(Q,R)=(0,A)$ qui convient. On suppose dorénavant $p\leq n+1$, ce qui permet de définir $P=A-\frac{a}{b}X^{n+1-p}B=A'-\frac{a}{b}X^{n+1-p}B'$. Ce polynôme vérifie $d(P)<n+1$ car $d(A')\leq n$ et $d(X^{n+1-p}B')\leq n$. On lui applique alors l'hypothèse de récurrence : on dispose de (Q',R') tel que $P=Q'B+R'$ et $d(R')<d(B)$. On en déduit alors

$$A=P+\frac{a}{b}X^{n+1-p}B=Q'B+R'+\frac{a}{b}X^{n+1-p}B=(Q'+\frac{a}{b}X^{n+1-p})B+R'$$

En posant, $Q=Q'+\frac{a}{b}X^{n+1-p}$ et $R=R'$, on a alors $A=BQ+R$ et $d(R')=d(R)<d(B)$. L'existence est ainsi validée par récurrence forte.
Passons à l'unicité. Soit (Q_0,R_0) un autre couple satisfaisant ces critères. Alors $B(Q-Q_0)=R_0-R$. On en déduit que $d(B)+d(Q-Q_0)=d(R-R_0)$. De plus, $d(R-R_0)\leq\max(d(R),d(R_0))<d(B)$. On en déduit que $d(B)+d(Q-Q_0)<d(B)$. Comme B est non nul, $d(B)\neq-\infty$, de sorte qu'on peut soustraire $d(B)$ des deux côtés et obtenir $d(Q-Q_0)<0$. Par conséquent, $Q-Q_0=0$ et $R-R_0=B(Q-Q_0)=0$. Finalement, $(Q,R)=(Q_0,R_0)$.

Corollaire
Soit $(A,B)\in\mathbb{K}[X]\times\mathbb{K}[X]^*$. *Alors* B *divise* A *si et seulement si le reste de la division euclidienne de* A *par* B *est nul.*

Démonstration. Posons $A=BQ+R$ la division euclidienne de A par B. Si $R=0$, alors la relation de divisibilité est claire. Si B divise A, on dispose de $P\in\mathbb{K}[X]$ tel que $A=BP$, ce qui s'écrit également $A=BP+0$. Or $d(0)=-\infty<d(B)$ puisque B est non nul. On a ainsi une division euclidienne de A par B. D'après l'unicité du reste, $R=0$.

2 Racines d'un polynôme.

Définition 7 *Soit* $P\in\mathbb{K}[X]$ *tel que* $P=\sum_{k=0}^n p_kX^k$. *On appelle fonction polynomiale associée à* P, *l'application* $\mathbb{K}\to\mathbb{K}, x\mapsto\sum_{k=0}^n p_kx^k=P(x)$. *Elle est parfois notée* $\tilde{P}$

Propriété 6 *On note* $\mathcal{F}(\mathbb{K},\mathbb{K})$ *l'ensemble des applications de* $\mathbb{K}$ *dans* $\mathbb{K}$. *Muni des opérations* $+,\times$ *issues de celle de* $\mathbb{K}$, *il vérifie toutes les règles algébriques usuelles. Il est également muni d'une multiplication externe via* $\mathbb{K}$ *et d'une composition interne.*

Propriété 7 *Soit* $(A,B)\in\mathbb{K}[X]^2, \lambda\in\mathbb{K}$, *alors on a les égalités d'applications dans* $\mathcal{F}(\mathbb{K},\mathbb{K})$ *:*

$$\widetilde{A+B}=\widetilde{A}+\widetilde{B},\quad \widetilde{\lambda A}=\lambda\widetilde{A},\quad \widetilde{A\times B}=\widetilde{A}\times\widetilde{B},\quad \widetilde{A\circ B}=\widetilde{A}\circ\widetilde{B}$$

Démonstration. Longue et ennuyeuse.

✎ **Méthode (Algorithme de Horner)**
Plaçons-nous dans le cas réel. Soit x *un réel et* $P=\sum_{k=0}^n p_kX^k$ *un polynôme de degré* n. *Pour évaluer* $P(x)$, *l'expression* $\sum_{k=0}^n p_kx^k$ *nécessite de calculer* $n+1$ *additions et* $\sum_{k=0}^n k=n(n+1)/2$ *multiplications. C'est un coût quadratique sur le degré du polynôme, alors qu'on peut procéder avec une complexité linéaire en le degré de* P. *On pose* $u_0=a_nx$ *et pour tout entier* k, $u_{k+1}=(u_k+a_{n-k})x$. *Alors* $u_n=P(x)$ *et le coût en opérations est* $2n$.

Définition 8 *Soit* $P\in\mathbb{K}[X]$ *et* $a\in\mathbb{K}$. *On dit que* a *est une racine (ou un zéro) de* P *lorsque* $P(a)=0$.

Théorème 3 *Soit* $P\in\mathbb{K}[X]$ *et* $a\in\mathbb{K}$. *On a l'équivalence :* a *est racine de* P *si et seulement si* $X-a$ *divise* P.

Démonstration. Le polynôme $B=X-a$ est non nul car de degré 1. On effectue alors la division euclidienne de P par B sous la forme $P=BQ+R$ avec $R=0$ ou $d(R)<d(B)$. Comme B est de degré 1, le polynôme R est constant (éventuellement nul). Pour évaluer cette constante, on évalue les fonctions polynomiales en a dans la division euclidienne : $P(a)=B(a)Q(a)+R(a)$. Comme $B(a)=0$, on en déduit que R est constant égal à $P(a)$.
Si a est racine de P, alors R est nul et la division euclidienne $P=(X-a)Q$ assure que $X-a$ divise P. Réciproquement, si $X-a$ divise P, le reste dans cette division euclidienne est nul, donc $P(a)=0$ et a est racine de P.

Propriété 8 *Soit* $P \in \mathbb{K}[X]$ *un polynôme non nul. Alors* $Z(P)$ *l'ensemble des racines est fini et* $|Z(P)| \leq d(P)$.

Démonstration. On en prouve la contraposée par récurrence sur le degré de P. Pour tout entier naturel n, on note $\mathcal{H}_n : \forall P \in \mathbb{K}_n[X], |Z(P)| \geq n+1 \Rightarrow P = 0$. Intialisation : pour $n = 0$. Soit $P \in \mathbb{K}_0[X]$ tel que $|Z(P)| \geq 1$. C'est donc un polynôme de degré au plus 0, il est donc constant. D'après l'hypothèse sur le nombre de ses racines, il en possède une, que l'on note a. Mais alors P est constant égal à $P(a)$, donc constant nul. Hérédité : Soit $n \in \mathbb{N}$ tel que $\mathcal{H}_n$ est vérifié. Démontrons que $\mathcal{H}_{n+1}$ est vérifiée. Soit $P \in \mathbb{K}_{n+1}[X]$ tel que $|Z(P)| \geq n+2$. Notons a un élément de $Z(P)$. D'après la propriété précédente, $X - a$ divise P. On note alors Q un polynôme tel que $P = (X-a)Q$ et on a l'égalité de degrés $d(P) = 1 + d(Q)$. De plus, on dispose de $a_1, \ldots, a_{n+1}$ $n+1$ scalaires distincts et distincts de a dans $Z(P)$ par hypothèse. Mais alors $\forall i [\![1, n+1]\!], 0 = P(a_i) = (a - a_i)Q(a_i)$. D'après la règle du produit nul dans $\mathbb{K}$, on en déduit que $Z(Q) \supset \{a_1, \ldots, a_{n+1}\}$. On peut ainsi appliquer l'hypothèse de récurrence $\mathcal{H}_n$ au polynôme Q, ce qui assure que $Q = 0$, donc que $P = 0$.

☞ **Remarque**
On utilise souvent cette propriété via sa contraposée. Si on trouve un nombre de racines strictement supérieur au degré de P*, alors* P *est le polynôme nul.*

Propriété 9 *Soit* P *un polynôme. On suppose que* P *possède un nombre de racines strictement plus grand que son degré. Alors* P *est le polynôme nul.*

Exemple 6 *On considère un polynôme* P *qui vérifie* $P(X+1) = P(X)$*. Si* P *possède une racine (notons-la* a*), alors* $P(a+1) = P(a) = 0$*, donc* $a+1$ *est également racine. Par une récurrence rapide, on démontre que* $a+n$ *est racine de* P *pour tout entier relatif* n*, donc que* P *possède une infinité de racines. D'après la propriété précédente, cela signifie que* $P = 0$.

Propriété 10 *L'application* $\mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}, P \mapsto \widetilde{P}$ *est une injection. Autrement dit, un polynôme est uniquement déterminé par sa fonction polynomiale.*

Démonstration. Soit $(P, Q) \in (\mathbb{K}[X])^2$ tel que $\widetilde{P} = \widetilde{Q}$. Alors, $\widetilde{P - Q} = \widetilde{P} - \widetilde{Q} = 0$. Par conséquent, le polynôme $P - Q$ possède une infinité de racines, puisque $\mathbb{K}$ est infini. D'après la propriété précédente, $P - Q$ est le polynôme nul, donc $P = Q$.

⚠ **Attention**
Cette propriété est spécifique au cas où $\mathbb{K} = \mathbb{R}$ *ou* $\mathbb{C}$*. En cryptographie, on utilise typiquement des ensembles* $\mathbb{K}$ *finis pour lesquels cette propriété est fausse.*

Définition 9 *Soit* $P \in \mathbb{K}[X]$ *non nul et* a *une racine de* P*. Alors* $\max\{k \in \mathbb{N} | (X-a)^k \mid P\}$ *est appelé multiplicité de la racine* a *dans* P*. Si* a *n'est pas racine, on convient que sa multiplicité dans* P *vaut* 0.

Notation
Pas de notation universelle dans la littérature, on pourra employer $\omega_P(a)$ *par exemple.*

Exemple 7 *Soit* $P = X^4 - 2X^2 + 1$*. Alors* $P(1) = 0$*, donc* $X-1$ *divise* P*. Plus précisément,* $P = (X-1)(X^3 + X^2 - X - 1)$*. Posons* $Q = X^3 + X^2 - X - 1$*. Alors* $Q(1) = 0$*, donc* $X-1$ *divise* Q*. Plus précisément,* $Q = (X-1)(X^2 + 2X + 1)$*. Posons alors* $R = X^2 + 2X + 1$*. Il vérifie* $R(1) = 4 \neq 0$*, donc* $(X-1)^2$ *divise* P*, mais* $(X-1)^3$ *ne divise pas* P*. Conclusion,* 1 *est racine double de* P.

☞ **Remarque**
Nous verrons des outils plus efficaces que des divisions successives pour déterminer les multiplicités de racines dans la suite du cours.

Définition 10 *Soit* $P \in \mathbb{K}[X]$*. On dit que* P *est scindé lorsqu'il peut s'écrire comme produit de polynômes de degré* 1*. On dit que* P *est simplement scindé lorsque* P *est produit de polynômes de degré* 1 *tous distincts.*

Exemple 8 *Pour tout entier* n *non nul,* $X^n - 1$ *est simplement scindé car égal à* $\prod_{k=1}^{n}(X - \omega^k)$ *avec* $\omega = \exp(2i\pi/n)$*. Dans* $\mathbb{R}[X]$*,* $X^2 + 1$ *n'est pas scindé (sinon il aurait une racine réelle).*

Propriété 11 *Soit* $P \in \mathbb{K}[X]$*,* n *un entier naturel non nul,* $(a_1, \ldots, a_n) \in \mathbb{K}^n$ *un* n*-uplet de scalaires tous distincts. On suppose que* $\forall i \in [\![1, n]\!], P(a_i) = 0$*. Alors* $\prod_{i=1}^{n}(X - x_i)$ *divise* P

Démonstration. On établit cette propriété par récurrence sur n. Initialisation $n = 1$: il s'agit de la propriété $P(a) = 0 \iff X - a \mid P$. Hérédité : Soit n un entier naturel non nul tel que la propriété est vraie. Montrons-la au rang $n+1$. Soit $(a_1, \dots, a_{n+1})$ un $n+1$-uplet de scalaires tous distincts tel que $\forall i [\![1, n+1]\!], P(a_i) = 0$. En particulier, $P(a_{n+1}) = 0$, donc $X - a_{n+1}$ divise P. On note alors Q tel que $P = (X - a_{n+1})Q$ et $\forall i [\![1, n]\!], (a_i - a_{n+1})Q(a_i) = 0$. Comme les $(a_i)_i$ sont distincts de a_{n+1}, on en déduit que $Q(a_i) = 0$. Par hypothèse de récurrence, $\prod_{i=1}^{n}(X - a_i)$ divise Q. Alors $\prod_{i=1}^{n+1}(X - a_i)$ divise P.

Propriété 12 *Soit $P \in \mathbb{K}[X]$, n un entier naturel non nul, $(a_1, \dots, a_n) \in \mathbb{K}^n$ un n-uplet de scalaires tous distincts. Soit $(m_1, \dots, m_n)$ une famille de n entiers naturels tous non nuls. On suppose que pour tout i dans $[\![1, n]\!]$, $(X - a_i)^{m_i}$ divise P. Alors $\prod_{i=1}^{n}(X - a_i)^{m_i}$ divise P.*

Démonstration. Reprendre la méthode précédente par récurrence. Comme les m_i sont non nuls, on fait bien descendre le degré après factorisation par $(X - a_i)^{m_i}$.

Propriété 13 (Relations coefficients-racines) *[Formules de Viète] Soit $n \in \mathbb{N}^*$, $P = \sum_{i=0}^{n} p_i X^i \in \mathbb{K}[X]$ un polynôme scindé de degré n. On suppose que P est scindé. On note $P = p_n \prod_{i=1}^{n}(X - a_i)$ une factorisation scindée de P. Alors*

$$p_n \sum_{i=1}^{n} a_i = -p_{n-1} \quad \text{et} \quad p_n \prod_{i=1}^{n} a_i = (-1)^n p_0$$

☞ **Remarque**
Si P est unitaire, la somme des racines (éventuellement répétées) est l'avant dernier coefficient de P. Le produit de ses racines (éventuellement répétées) vaut, à un signe près, le coefficient constant.

Démonstration. Il s'agit de sélectionner les terme de degré X^{n-1} dans le produit $p_n \prod_{i=1}^{n}(X - a_i)$. Ces termes n'apparaissent qu'en sélectionnant $n-1$ fois le terme X et 1 fois le terme $-a_i$. Autrement dit,

$$p_n X^n + p_{n-1} X^{n-1} + \dots = p_n X^n + p_n X^{n-1} \sum_{i=1}^{n} (-a_i) + \dots$$

D'après l'unicité du coefficient de degré $n-1$, on obtient

$$p_n \sum_{i=1}^{n} a_i = -p_{n-1}$$

L'autre égalité vient de l'évaluation en 0 qui donne $p_0 = \sum_{i=0}^{n} p_i 0^i = p_n \prod_{i=1}^{n}(0 - a_i) = p_n (-1)^n \prod_{i=1}^{n} a_i$.

3 Dérivation dans $\mathbb{K}[X]$.

Définition 11 *Soit $P \in \mathbb{K}[X]$ de degré n. Si $n \in \mathbb{N}$, on le note sous la forme $P = \sum_{k=0}^{n} a_k X^k$. Le polynôme $\sum_{k=1}^{n} k a_k X^{k-1}$ est appelé polynôme dérivé de P, il est noté P'. Si $P = 0$, on définit $P' = 0$.*

☞ **Remarque**
On dit parfois qu'il s'agit d'une dérivation formelle. Il n'est pas question de dérivabilité ici, on a simplement défini la dérivée formelle d'un polynôme à l'aide de la liste de ses coefficients.

Propriété 14 *Soit $(P, Q) \in \mathbb{K}[X]^2, (\lambda, \mu) \in \mathbb{K}^2$. Alors*

- $P' = 0 \iff d(P) \leq 0$.
- *Si P est non constant, $d(P') = d(P) - 1$. Si P est constant, $d(P') = -\infty$.*
- $(\lambda P + \mu Q) = \lambda P' + \mu Q'$.
- $(PQ)' = P'Q + PQ'$.
- $(P \circ Q) = Q'(P' \circ Q)$.

Démonstration.
- Si $P = 0$, c'est évident. Sinon, $P' = 0 \iff \forall n \in \mathbb{N}^*, p_n = 0 \iff d(P) \leq 0$.
- Si P est non constant de degré n, le terme dominant de P' vaut $n p_n X^{n-1}$. Comme $p_n \neq 0$, $n p_n \neq 0$. Ainsi, $d(P') = n - 1 = d(P) - 1$.

— Avec des notations évidentes,
$$\lambda P + \mu Q = \sum_{i=0}^{\max(d(P),d(Q))} (\lambda p_k + \mu q_k) X^k$$
La définition du polynôme entraîne
$$(\lambda P + \mu Q)' = \sum_{i=1}^{\max(d(P),d(Q))} k(\lambda p_k + \mu q_k) X^{k-1} = \lambda \sum_{k=1}^{d(P)} k p_k X^{k-1} + \mu \sum_{k=1}^{d(Q)} k q_k X^{k-1} = \lambda P' + \mu Q'$$

— Simplifions nous la vie en traitant d'abord le cas des monômes. Soit m et n deux entiers naturels. Si m ou n est nul, X^m ou X^n est de dérivée nulle, puisque constant. Supposons à présent m et n tous deux non nuls. Alors $(X^m X^n)' = (X^{m+n})' = (m+n)X^{m+n-1} = mX^{m-1}X^n + X^m nX^{n-1} = (X^m)'X^n + X^m(X^n)'$, ce qui établit la formule souhaitée par les monômes. Dans le cas général, on utilise la linéarité précédemment démontrée :
$$(PQ)' = \left(\sum_{m=0}^{+\infty} p_m X^m \sum_{n=0}^{+\infty} q_n X^n \right)' = \left(\sum_{(n,m)\in\mathbb{N}^2} p_m q_n X^{m+n} \right)' = \sum_{(n,m)\in\mathbb{N}^2} p_m q_n (X^{m+n})'$$
D'après la propriété sur les dérivations de produits de monômes, on en déduit que
$$(PQ)' = \sum_{(n,m)\in\mathbb{N}^2} p_m q_n \left[(X^m)'X^n + X^m (X^n)' \right] = \sum_{(n,m)\in\mathbb{N}^2} p_m q_n (X^m)'X^n + \sum_{(n,m)\in\mathbb{N}^2} p_m q_n X^m (X^n)'$$
On reconnaît des produits polynomiaux
$$(PQ)' = \sum_{m\in\mathbb{N}} p_m (X^m)' \sum_{n\in\mathbb{N}} q_n X^n + \sum_{m\in\mathbb{N}} p_m X^m \sum_{n\in\mathbb{N}} q_n (X^n)'$$
Toujours d'après la linéarité,
$$(PQ)' = P'Q + PQ'$$

— Si P est nul, $P' = 0$, $P' \circ Q = 0$ et $P \circ Q = 0$, donc l'égalité est assurée. Sinon, on note $P = \sum_{k=0}^{n} p_k X^k$, ce qui entraîne $P \circ Q = \sum_{k=0}^{n} p_k Q^k$. En généralisant rapidement ce qui précède par récurrence,, on en déduit que $(P \circ Q)' = \sum_{k=1}^{n} p_k k Q' Q^{k-1} = Q'(P' \circ Q)$.

Propriété 15 *Soit $P \in \mathbb{R}[X]$ et $\widetilde{P}$ sa fonction polynomiale. Alors $\widetilde{P}$ est dérivable et*
$$\widetilde{P}' = \widetilde{P'}$$

Démonstration. Immédiate d'après vos connaissances sur la dérivation des fonctions monomiales.

Définition 12 *On définit par récurrence les dérivées sucessives d'un polynôme P. On convient que $P^{(0)} = P$, on pose $P^{(1)} = P'$ et $\forall k \in \mathbb{N}, P^{(k+1)} = \left(P^{(k)}\right)'$.*

Exemple 9 *Soit $(k,n) \in \mathbb{N}^2$. Alors*
$$(X^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k} & si\ k < n \\ k! & si\ k = n \\ 0 & si\ k > n \end{cases}$$

Propriété 16 (Formule de Leibniz) *Soit $(P,Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$. Alors*
$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$$

Démonstration. Calquer la preuve dans le cas des fonctions réelles. Il s'agit d'une récurrence se basant sur la relation triangulaire de Pascal.

Théorème 4 (Formule de Taylor polynomiale) *Soit $P \in K[X]$ de degré n, $a \in \mathbb{K}$ Alors*
$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

En particulier, le coefficient d'indice k de P n'est autre que $P^{(k)}(0)/k!$ pour tout entier naturel k.

Démonstration. On note $P = \sum_{j=0}^{n} p_j X^j$. Soit $k \in [\![0, n]\!]$. D'après la linéarité de la dérivation et la formule sur les dérivées itérées des monômes, on a

$$P^{(k)} = \sum_{j=0}^{n} p_j \left(X^j\right)^{(k)} = \sum_{j=k}^{n} p_j \frac{k!}{(k-j)!} X^{k-j}$$

L'évaluation en 0 donne alors

$$P^{(k)}(0) = k! p_k$$

On retrouve alors la formule indiquée pour $a = 0$. Dans le cas général, on applique ce qui précède à $Q = P(X + a)$. Cela entraîne

$$Q = \sum_{k=0}^{n} \frac{Q^{(k)}(0)}{k!} X^k$$

Or pour tout entier r, $Q^{(r)} = P^{(r)}(X + a)$ (récurrence facile puisque $(X + a)' = 1$), et $P = Q(X - a)$. On en déduit que

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

Propriété 17 *Soit $P \in \mathbb{K}[X]$ non nul et a une racine de P. Alors la multiplicité de a dans P vaut*

$$\min\{k \in \mathbb{N} | P^{(k)}(a) \neq 0\}$$

Démonstration. Soit k un entier non nul. Via la formule de Taylor polynomiale, on écrit la division euclidienne de P par $(X - a)^k$:

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

ce qui est valide puisque le degré de $\sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!} (X - a)^j$ vaut au plus $k - 1 < k = d((X - a)^k)$. On a alors l'équivalence

$$(X - a)^k \mid P \iff \sum_{j=0}^{k-1} \frac{P^{(j)}(a)}{j!} (X - a)^j = 0 \iff \forall j \in [\![0, k-1]\!], P^{(j)}(a) = 0$$

On a alors l'égalité annoncée.

Propriété 18 *Soit $P \in \mathbb{K}[X]$ non nul et a une racine de P. Alors la multiplicité de a dans P vaut n si et seulement si*

$$P(a) = 0, \quad P'(a) = 0, \quad \ldots, \quad P^{(n-1)}(a) = 0, \quad P^{(n)}(a) \neq 0$$

Démonstration. Il s'agit d'une refomulation du minimum précédent.

Exemple 10 *Reprenons le polynôme $P = X^4 - 2X^2 + 1$. Alors $P(1) = 0, P' = 4X^3 - 4X, P'(1) = 0, P'' = 12X^2 - 4$, $P''(1) = 8 \neq 0$, donc 1 est racine de multiplicité 2 de P.*

4 Polynômes irréductibles et factorisations

4.1 Généralités

Définition 13 *Soit $P \in \mathbb{K}[X]$. Le polynôme P est dit irréductible lorsqu'il est non constant et*

$$\forall (Q, R) \in \mathbb{K}[X]^2, P = QR \Rightarrow [d(Q) = 0 \vee d(R) = 0]$$

Autrement dit, P ne possède pas d'autres factorisations qu'en facteurs constants et associés à P.

Propriété 19 *Soit $P \in \mathbb{K}[X]$ non constant. P est irréductible si et seulement si les seuls diviseurs de P sont les polynômes constants et les polynômes associés à P.*

Exemple 11 *Tout polynôme de degré* 1 *est irréductible. Soit* P *un polynôme de degré supérieur ou égal à* 2 *tel que* P *admet une racine, alors* P *n'est pas irréductible. En effet, en notant a une telle racine,* $X - a$ *divise* P *et* $d(X - a) < d(P)$ *puisque* $d(P) \geq 2$*, ce qui fournit une factorisation non triviale de* P*. La réciproque est fausse en général : le polynôme* $X^4 + 1$ *n'a pas de racine dans* $\mathbb{R}$*, pourtant,* $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ *est une factorisation non triviale de* P*. La réciproque est vraie dans le cas* $n = 2$ *et* $n = 3$*. Soit* P *un polynôme de degré* 2 *ou* 3 *sans racines. Soit* $P = QR$ *une factorisation de* P*. Alors* Q *et* R *sont sans racines, sinon* P *en aurait. Par conséquent,* Q *et* R *ne sont pas de degré* 1*. Si* P *est de degré* 2*, cela indique que* $d(Q) = 2$ *ou* $d(R) = 2$ *donc qu'il s'agit d'une factorisation triviale. Ainsi,* P *est irréductible. Si* P *est de degré* 3*,* $d(Q) + d(R) = 3$*, donc* Q *et* R *ne sont pas de degré* 2*. Ainsi,* $d(Q) = 3$ *ou* $d(R) = 3$*, et la factorisation est triviale et* P *est irréductible.*

Propriété 20 *Soit* P *un polynôme non constant. Alors* P *possède un diviseur irréductible. En particulier, si* P *n'est pas irréductible,* P *possède un diviseur irréductible de degré strictement inférieur à* $d(P)$*.*

Démonstration. On note $A = \{Q \in D(P) | d(Q) \geq 1\}$, puis $\Delta = \{d(R) | R \in A\}$. Comme P est non constant, A contient P, donc est non vide. On en déduit que Δ est une partie non vide de $\mathbb{N}^*$. Elle possède donc un minimum r et il existe un polynôme R non constant de degré r minimal qui divise P. Montrons que R est irréductible. Soit D un diviseur de R, par transitivité de la relation de divisibilité, D divise P. Si D n'est pas constant, alors D appartient à A. Par minimalité de r, $d(D) \geq r$. D'autre part, D divise R, donc $d(D) \leq r$. Ainsi, D et R sont associés. Ainsi, les seuls factorisations de R sont triviales et R est irréductible.

4.2 Classification sur $\mathbb{C}$

Théorème 5 (Théorème de D'Alembert-Gauss) *Soit* $P \in \mathbb{C}[X]$ *non constant. Alors* P *admet une racine.*

Démonstration. Admis. Il nous faut des outils d'analyse pour le démontrer.

Propriété 21 *Soit* $P \in \mathbb{C}[X]$ *non constant. Alors* P *est scindé.*

Démonstration. On établit ce résultat par récurrence sur le degré de P. Soit P de degré 1. Alors il est clair que P est scindé. Soit n un entier naturel non nul tel que le résultat est vrai. Soit P un polynôme de degré $n+1$. D'après le théorème de D'Alembert-Gauss, P admet une racine a, donc $X - a$ divise P. On écrit alors $P = (X - a)Q$, ce qui implique que $d(Q) = n$. On lui applique l'hypothèse de récurrence. Q est alors produit de polynômes de degré 1. En regroupant avec $X - a$, P s'écrit comme produit de polynômes de degré 1.

Propriété 22 *Les polynômes irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1*.*

Démonstration. Soit P un polynôme irréductible de $\mathbb{C}[X]$. Il est non constant par définition des irréductibles. D'après le théorème de D'Alembert-Gauss, il possède une racine a. Mais alors $X - a$ divise P et $X - a$ n'est pas constant. Par conséquent, P est associé à $X - a$ et P est de degré 1. La réciproque a déjà été mentionnée.

Théorème 6 *Soit* $P \in \mathbb{C}[X] \backslash \{0\}$*. Alors* P *se factorise de manière unique (à l'ordre près) sous la forme suivante :*

$$P = \alpha \prod_{i=1}^{r} (X - a_i)^{n_i}$$

où $\alpha \in \mathbb{C}^*$, $r \in \mathbb{N}$, $a_1, \ldots, a_r$ *complexes distincts et* $n_1, \ldots, n_r$ *des entiers naturels non nuls*

Démonstration. Posons $n = d(P)$. n est un entier puisque $P \neq 0$.
Existence. On propose $\alpha = \text{dom}(P)$, $r = |Z(P)|$ le nombre de zéros distincts de P, $a_1, \ldots, a_r$ la liste des zéros distincts de P et $n_1, \ldots, n_r$ leurs multiplicités respectives. Posons $Q = \alpha \prod_{i=1}^{r} (X - a_i)^{n_i}$. Alors Q divise P puisque $(X - a_i)^{n_i}$ divise P pour tout i dans $[\![1, r]\!]$ par définition des multiplicités des racines de P et car celles-ci sont distinctes dans la liste énoncée. On dispose donc de $R \in \mathbb{C}[X]$ tel que $P = QR$. Montrons que R est constant. Si ce n'est pas le cas, il possède une racine a d'après le théorème de D'Alembert-Gauss. Mais alors $P(a) = Q(a)R(a) = 0$, donc a est une racine de P, i.e il existe i dans $[\![1, r]\!]$ tel que $a = a_i$, mais alors $(X - a_i)^{n_i + 1}$ divise P, ce qui contredit la multiplicité n_i de la racine a_i. Conclusion, R est constant. Comme P et Q ont même coefficient dominant, R est unitaire, donc $R = 1$, puis $P = Q$, ce qui prouve l'existence de la factorisation indiquée.
Unicité. Soit $P = \beta \prod_{j=1}^{q} (X - b_j)^{m_j}$ une autre telle factorisation de P. Alors $\text{dom}(P) = \beta$ puisque tous les monômes sont unitaires. Soit $j \in [\![1, q]\!]$. Alors $(X - b_j)^{m_j}$ divise P, donc b_j est une racine de P de multiplicité au moins m_j. Comme b_j est différent de tous les autres $b_k, k \neq j$, $(X - b_j)^{m_j + 1}$ ne divise pas P, donc $\omega_P(b_j) = m_j$. D'autre part $\forall z \in \mathbb{C} \backslash \{b_1, \ldots, b_q\}, P(z) \neq 0$, donc $Z(P) = \{b_1, \ldots, b_q\}$ et $q = |Z(P)|$.

☞ **Remarque**
On peut écrire $P = dom(P)\prod_{a\in Z(P)}(X-a)^{\omega_P(a)} = dom(P)\prod_{a\in\mathbb{C}}(X-a)^{\omega_P(a)}$*, mais cette écriture magique ne doit pas se substituer à une compréhension fine de la factorisation précédente.*

Propriété 23 *Soit* $(P,Q)\in\mathbb{C}[X]^2$ *tous deux non nuls. On note* $Z(P)$ *et* $Z(Q)$ *les ensembles de leurs racines respectives. Alors* P *divise* Q *si et seulement si* $Z(P)\subset Z(Q)$ *et pour tout racine* a *de* P*, sa multiplicité dans* P *est inférieure ou égale à sa multiplicité dans* Q*.*

Démonstration. Si P divise Q, soit $a\in Z(P)$ de multiplicité α alors $(X-a)^\alpha$ divise P donc divise Q par transitivité. Ainsi, a est une racine de Q de mutliplicité au moins α. Réciproquement, si l'on a la condition sur les racines, comme on travaille dans $\mathbb{C}[X]$, on peut factoriser les polynômes P et Q comme précédemment, on dispose alors de complexes $(a_1,\dots,a_p,a_{p+1},\dots,a_n)$, d'entiers naturels non nuls $\alpha_1,\dots,\alpha_p,\beta_1,\dots\beta_n$ tels que $\forall i[\![1,p]\!],\alpha_i\le\beta_i$, de complexes non nuls λ et μ tels que

$$P=\lambda\prod_{i=1}^{p}(X-a_i)^{\alpha_i}\quad\text{et}\quad Q=\mu\prod_{i=1}^{n}(X-a_i)^{\beta_i}$$

Mais alors

$$Q=\frac{\mu}{\lambda}\prod_{i=p+1}^{n}(X-a_i)^{\beta_i}\prod_{i=1}^{p}(X-a_i)^{\beta_i-\alpha_i}P$$

donc P divise Q.

4.3 Classification sur $\mathbb{R}$

Notation
Pour tout $P=\sum_{n=0}^{+\infty}p_nX^n\in\mathbb{C}[X]$*, on pose* $\overline{P}=\sum_{n=0}^{+\infty}\overline{p_n}X^n$*.*

Propriété 24 *Soit* $(P,Q)\in\mathbb{C}[X]^2$*. Alors* $\overline{PQ}=\overline{P}\,\overline{Q}$ *et* $P\in\mathbb{R}[X]\iff\overline{P}=P$*.*

Démonstration. Laissée à titre d'exercice.

Propriété 25 *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont les polynômes de degré* 1 *et les polynômes de degré* 2 *de discriminant strictement négatif.*

Démonstration. Soit $P\in\mathbb{R}[X]$ irréductible. Supposons $d(P)\ge 2$. On peut voir P comme élément de $\mathbb{C}[X]$. Alors P admet une racine complexe α d'après le théorème de D'Alembert-Gauss. Mais alors comme P est à coefficients réels, $\overline{P(\alpha)}=P(\overline{\alpha})=0$, donc $\overline{\alpha}$ est une racine de P. D'autre part, α n'est pas réel car sinon P n'est pas irréductible, donc $\alpha\neq\overline{\alpha}$. On en déduit que $(X-\alpha)(X-\overline{\alpha})$ divise P, ce que l'on écrit

$$P=(X^2-2\mathfrak{Re}(\alpha)X+|\alpha|^2)Q$$

avec $Q\in\mathbb{C}[X]$. Or $P=\overline{P}=\overline{(X^2-2\mathfrak{Re}(\alpha)X+|\alpha|^2)Q}=(X^2-2\mathfrak{Re}(\alpha)X+|\alpha|^2)\overline{Q}$. Par intégrité de $\mathbb{R}[X]$, $Q=\overline{Q}$, donc Q est à coefficients réels. Cette factorisation de P irréductible dans $\mathbb{R}[X]$ implique que Q est constant non nul. Ainsi, P est un polynôme de degré 2, et son discriminant vaut $Q^2(4\mathfrak{Re}(\alpha)^2-4|\alpha|^2)<0$.

Propriété 26 *Soit* $P\in\mathbb{R}[X]$ *et* α *une racine complexe non réelle de* P*. Alors* α *et* $\overline{\alpha}$ *ont même multiplicité.*

Démonstration. On rappelle que $\overline{\alpha}$ est également une racine de P. Notons k la multiplicité de α comme racine de P. Alors il existe $Q\in\mathbb{C}[X]$ tel que $P=(X-\alpha)^kQ$, donc $P=\overline{P}=(X-\overline{\alpha})^k\overline{Q}$. Donc $(X-\overline{\alpha})^k$ divise P, donc la multiplicité (notons-la k') de $\overline{\alpha}$ comme racine de P est supérieure ou égale à k, i.e $k\le k'$. En appliquant le même raisonnement à $\overline{\alpha}$, on obtient $k'\le k$. Conclusion, $k=k'$, les multiplcités sont égales.

Théorème 7 *Soit* $P\in\mathbb{R}[X]\backslash\{0\}$*. Alors* P *se factorise de manière unique (à l'ordre près) sous la forme*

$$P=\alpha\prod_{i=1}^{r}(X-a_i)^{n_i}\prod_{i=1}^{q}(X^2+b_iX+c_i)^{m_i}$$

où $\alpha\in\mathbb{R}^*$*,* r,q *des entiers naturels,* $a_1,\dots,a_r$ *des réels distincts,* $n_1,\dots,n_r$ *des entiers naturels non nuls,* $(b_1,c_1),\dots,(b_q,c_q)$ *des couples de réels distincts tels que* $\forall i\in[\![1,q]\!],b_i^2-4c_i<0$ *et* $m_1,\dots,m_q$ *des entiers naturels non nuls.*

Démonstration. **Existence.** En voyant P comme élément de $\mathbb{C}[X]$, on peut le factoriser sous la forme

$$P = \alpha \prod_{i=1}^{r} (X - a_i)^{n_i}$$

où $\alpha = \text{dom}(P)$, r le nombre de racines distinctes de P, $a_1, \dots, a_r$ les racines complexes distinctes de P et $n_1, \dots, n_r$ leurs multiplicités respectives. On partitionne les racines entre racines réelles et racines complexes non réelles. Quitte à réordonner, en posant $q = |Z(P) \cap \mathbb{R}|$, on peut supposer $a_1, \dots, a_q$ réelles et $a_{q+1}, \dots, a_r$ non réelles. Soit $j \in [\![q+1, r]\!]$, alors $\overline{a_j}$ est une racine complexe non réelle de P, donc il existe $k \in [\![q+1, r]\!] \backslash \{j\}$ tel que $\overline{a_j} = a_k$. De plus, leurs multiplicités sont égales, donc $n_j = n_k$. Mais alors

$$(X - a_j)^{n_j}(X - a_k)^{n_k} = \left((X - a_j)(X - \overline{a_j})\right)^{n_j} = (X^2 - 2\mathfrak{Re}(a_j)X + |a_j|^2)^{n_j}$$

On peut alors proposer $b_j = -2\mathfrak{Re}(a_j)$ et $c_j = |a_j|^2$ qui vérifient bien $b_j^2 - 4c_j = 4(\mathfrak{Re}(a_j)^2 - |a_j|^2) < 0$ puisque a_j est non réel. En regroupant ainsi les racines complexes conjuguées de P, on obtient la factorisation souhaitée.
Unicité Admise, c'est uniquement du codage.

5 Corps des fractions rationnelles à une indéterminée.

Aucun élément théorique sur ce qui suit n'est exigible, cette partie du cours a des objectifs purement calculatoires de calculs de dérivées et de primitives pour l'analyse.

5.1 Opérations dans $\mathbb{K}(X)$.

Théorème 8 (admis) *Il existe un ensemble, noté $\mathbb{K}(X)$, muni d'une addition et d'une multiplication vérifiant les points suivants :*

- $K[X] \subset \mathbb{K}(X)$.
- *Tout élément non nul F de $\mathbb{K}(X)$ possède un inverse, i.e $\exists G \in \mathbb{K}(X), FG = 1$. Cet inverse est alors unique et noté $1/F$.*
- *Tout élément F de $\mathbb{K}(X)$ peut se mettre sous la forme P/Q, où $P \in \mathbb{K}[X]$ et $Q \in \mathbb{K}[X]\backslash\{0\}$.*
- *Toutes les règles algébriques usuelles sur les fractions de $\mathbb{K}$ s'étendent à $\mathbb{K}(X)$.*

L'ensemble $\mathbb{K}(X)$ est appelé corps des fractions rationnelles à une indéterminée sur $\mathbb{K}$ et ses éléments appelés fractions rationnelles à coefficients dans $\mathbb{K}$.

Exemple 12 *Par exemple, $F = \frac{-X^2+X+1}{X^3+X-2}$ est une fraction rationnelle non nulle. Son inverse est $\frac{1}{F} = \frac{X^3+X-2}{-X^2+X+1}$. De même $G = \frac{1}{X+1}$ est une fractionnelle non nulle d'inverse $\frac{1}{G} = \frac{X+1}{1}$ que l'on peut réécrire $\frac{1}{G} = X + 1$. On a alors*

$$FG = \frac{-X^2+X+1}{X^3+X-2}\frac{1}{X+1} = \frac{-X^2+X+1}{(X^3+X-2)(X+1)} = \frac{-X^2+X+1}{X^4+X^3+X^2-X-2}$$

$$\frac{F}{G} = \frac{-X^2+X+1}{X^3+X-2}(X+1) = \frac{-X^3+2X+1}{X^3+X-2}$$

$$F + G = \frac{-X^2+X+1}{X^3+X-2} + \frac{1}{X+1} = \frac{(-X^2+X+1)(X+1)}{(X^3+X-2)(X+1)} + \frac{(X^3+X-2)}{(X^3+X-2)(X+1)}$$

$$F + G = \frac{(-X^2+X+1)(X+1) + (X^3+X-2)}{(X^3+X-2)(X+1)} = \frac{3X-1}{(X^3+X-2)(X+1)} = \frac{3X-1}{X^4+X^3+X^2-X-2}$$

Propriété 27 *Soit $F \in \mathbb{K}(X)$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X]^*$ avec Q unitaire tel que $F = P/Q$ et P et Q n'ont aucun diviseur commun non constant. Cette écriture unique est appelée forme irréductible de F.*

Démonstration. Admis

Exemple 13 *La fraction* $F = \frac{X^3+X^2+X+1}{X^2+2X+1}$ *se « simplifie » via* $F = \frac{(X+1)(X^2+1)}{(X+1)^2} = \frac{X^2+1}{X+1}$. *Comme les diviseurs non constants de* $X+1$ *sont associés à* $X+1$ *et ceux-ci ne divise pas* X^2+1 *puisque* -1 *n'est pas racine de* X^2+1, *on a bien obtenu la forme irréductible de* F.

Définition 14 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. Alors les zéros de* P *sont appelés les zéros de* F, *tandis que les zéros de* Q *sont appelés les pôles de* F. *La multiplicité d'un pôle de* F *est la multiplicité de ce scalaire comme racine de* Q.

Définition 15 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. Alors* $\tilde{F} : \mathbb{K}\backslash Z(Q), x \mapsto P(x)/Q(x) = F(x)$ *est appelée fonction rationnelle associée à* F.

Définition 16 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. Alors* $d(P) - d(Q)$ *est appelé le degré de* F, *noté* $d(F)$ *(avec la convention* $-\infty - n = -\infty$.*)*

Propriété 28 *Soit* $(F, G) \in K(X)^2$. *Alors*

- *Le degré de* F *est indépendant des polynômes* P, Q *tels que* $F = P/Q$.
- $d(FG) = d(F) + d(G)$
- *Si* G *est non nul,* $d(F/G) = d(F) - d(G)$.

Démonstration. À titre d'exo, si vous avez du temps à perdre.

Définition 17 *Soit* $F \in \mathbb{K}(X)$ *de forme irréductible* P/Q. *On définit alors la dérivée (formelle) de* F *via* $\frac{P'Q-PQ'}{Q^2}$.

Propriété 29 *Soit* $(F, G) \in (\mathbb{K}[X])^2, \lambda \in \mathbb{K}[X]$.

- *Linéarité :* $(F + \lambda G)' = F' + \lambda G'$
- *Leibniz :* $(FG)' = F'G + FG'$.
- *Si* F *est non nul,* $\left(\frac{1}{F}\right)' = -\frac{F'}{F^2}$.
- *Si* G *est non nul,* $\left(\frac{F}{G}\right)' = \frac{F'G-FG'}{G^2}$.
- $d(F') \leq d(F) - 1$.

Démonstration. À titre d'exercice si vous avez du temps à perdre.

Définition 18 *Soit* $F \in \mathbb{K}(X)$. *On définit par récurrence la dérivée itérée de* F, *via* $F^{(1)} = F'$, $F^{(n+1)} = \left(F^{(n)}\right)'$ *pour tout entier naturel* n.

☞ **Remarque**
Les définitions précédentes du degré et de la dérivée utilisent la forme irréductible de F, *mais sont en réalité valides avec toutes les formes non simplifiées de* F.

5.2 Décomposition en éléments simples

Exemple 14 *Prenons la fonction rationnelle* $f : \mathbb{R}\backslash\{-1,1\} \to \mathbb{R}, x \mapsto \frac{1}{x^2-1}$. *Elle est infiniment dérivable comme toute fonction rationnelle. Soit* $x \in \mathbb{R}\backslash\{-1,1\}$. *Alors* $f'(x) = \frac{-2x}{(x^2-1)^2} = -2x(x^2-1)^{-2}$, *puis* $f''(x) = -2(x^2-1)^{-2} - 2x(-2)(2x)(x^2-1)^{-3} = (-2(x^2-1)+8x^2)(x^2-1)^{-3} = 2(3x^2+1)(x^2-1)^{-3}$. *Les calculs semblent devenir de plus en plus inextricables. On peut pourtant s'en sortir en transformant d'abord* f.
On remarque astucieusement que $f(x) = \frac{1}{2}\frac{1}{1-x} + \frac{1}{2}\frac{1}{1+x}$. *Or, via une récurrence laissée à votre bon soin,*

$$\forall n \in \mathbb{N}, \left(\frac{1}{1-X}\right)^{(n)} = \frac{n!}{(1-X)^{n+1}}, \left(\frac{1}{1+X}\right)^{(n)} = \frac{n!(-1)^n}{(1+X)^{n+1}}$$

ce qui donne directement

$$f^{(n)}(x) = \frac{n!}{2}\left(\frac{1}{(1-x)^{n+1}} + \frac{(-1)^n}{(1+x)^{n+1}}\right)$$

On peut poursuivre l'utilisation de cette forme pour la détermination de primitives. Par linéarité, $x \mapsto \frac{1}{2}\ln|1-x| + \frac{1}{2}\ln|1+x|$ *est une primitive de* f *sur un intervalle inclus dans* $\mathbb{R}\backslash\{-1,1\}$.

Exemple 15 *Quelques exemples de décompositions en éléments simples dans* $\mathbb{R}[X]$ *et* $\mathbb{C}[X]$.

1.
$$\frac{1}{1-X^2} = \frac{1/2}{1-X} + \frac{1/2}{1+X}$$

2.
$$\frac{X}{1-X^2} = \frac{1/2}{1-X} - \frac{1/2}{1+X}$$

3. *On admet qu'il existe trois réels* a, b, c *tels que*
$$F = \frac{1}{(X-1)(X+3)^2} = \frac{a}{X-1} + \frac{b}{X+3} + \frac{c}{(X+3)^2}$$
Pour les déterminer, on évalue $(F(X-1))(1) = \frac{1}{4^2} = a$, $(F(X+3)^2)(-3) = \frac{1}{-4} = c$. *Si l'on note* $G = \frac{1}{X-1} = F(X+3)^2 = a\frac{(X+3)^2}{X-1} + b(X+3) + c$, *la dérivée de* G *donne*
$$G' = -\frac{1}{(X-1)^2} = a(X+3)R + b$$
On évalue cette dernière fraction rationnelle en -3, *ce qui donne* $b = -1/16$. *Finalement, on a*
$$\frac{1}{(X-1)(X+3)^2} = \frac{1/16}{X-1} + \frac{-1/16}{X+3} + \frac{-1/4}{(X+3)^2}$$

4. *Dans* $\mathbb{R}[X]$, *on admet qu'il existe un unique* $(a, b, c, d) \in \mathbb{R}^4$ *tel que*
$$F = \frac{X^2+4}{(X^2+1)^2} = \frac{aX+b}{X^2+1} + \frac{cX+d}{(X^2+1)^2}$$
On remarque que F *est paire, i.e* $F(-X) = F(X)$. *Mais alors, on a*
$$F = \frac{-aX+b}{X^2+1} + \frac{-cX+d}{(X^2+1)^2}$$
Par unicité du quadruplet (a, b, c, d), $a = -a$ *et* $c = -c$, *donc* $a = 0$ *et* $c = 0$. *De plus, on évalue* $F(X^2+1)^2$ *en* i *ce qui entraîne* $d = -1 + 4 = 3$. *On écrit de plus la limite de* X^2F *quand* X *tend vers* $+\infty$, *ce qui entraîne* $1 = b$. *En conclusion,*
$$F = \frac{1}{X^2+1} + \frac{3}{(X^2+1)^2}$$

Propriété 30 *Soit* $F \in \mathbb{K}(X)$ *et* P/Q *sa forme irréductible. On suppose que* Q *est simplement scindé sous la forme* $\prod_{i=1}^{n}(X-\lambda_i)$ *où les* λ_i *sont tous distincts. On suppose de plus que* $d(F) < 0$. *Alors*
$$F = \sum_{i=1}^{n} \frac{P(\lambda_i)}{Q'(\lambda_i)} \frac{1}{X-\lambda_i}$$

☞ **Remarque**
Pour tout i *dans* $[\![1, n]\!]$, $Q'(\lambda_i) \neq 0$ *car* λ_i *est racine simple de* Q.

Démonstration. Admis. On peut proposer l'explication suivante à défaut d'une démonstration complète. Un grand théorème d'arithmétique permet d'affirmer qu'il existe des scalaires $\alpha_1, \dots, \alpha_n$ tels que $F = \sum_{i=1}^{n} \frac{\alpha_i}{X-\lambda_i}$. Soit $i \in [\![1, n]\!]$. Montrons que $\alpha_i = P(\lambda_i)/Q'(\lambda_i)$. On pose $G = \sum_{j\neq i} \frac{\alpha_j}{X-\lambda_j}$ de sorte que $F = \frac{\alpha_i}{X-\lambda_i} + G$ et λ_i n'est pas pôle de G. On écrit alors
$$P(X-\lambda_i) = \alpha_i Q + GQ(X-\lambda_i)$$
puis on dérive
$$P'(X-\lambda_i) + P = \alpha_i Q' + GQ + G'Q(X-\lambda_i) + GQ'(X-\lambda_i)$$
Comme λ_i n'est pas pôle de G, il n'est pas non plus pôle de G′ et on peut évaluer les fractions précédentes en λ_i ce qui donne, puisque $Q(\lambda_i) = 0$,
$$P(\lambda_i) = \alpha_i Q'(\lambda_i)$$

Exemple 16 *Soit $n \in \mathbb{N}^*$. On considère $Q = X^n - 1$. Il est simplement scindé sur $\mathbb{C}$ via les racines n-ièmes de l'unité : $Q = \prod_{i=1}^{n}(X - \omega^i)$ en posant $\omega = \exp(2i\pi/n)$. On applique la propriété précédente à la fraction $1/Q = 1/(X^n - 1)$, ce qui donne*

$$\frac{1}{X^n - 1} = \sum_{i=1}^{n} \frac{1(\omega^i)}{Q'(\omega^i)} \frac{1}{X - \omega^i}$$

Or $\forall i \in [\![1, n]\!], Q'(\omega^i) = n\left(\omega^i\right)^{n-1} = \frac{n}{\omega^i}$. On en déduit

$$\frac{1}{X^n - 1} = \sum_{i=1}^{n} \frac{\omega^i}{n} \frac{1}{X - \omega^i}$$

Imaginons un instant que n est impair. Alors -1 n'est pas racine n-ième de l'unité, ce qui donne l'évaluation

$$\frac{n}{2} = \sum_{i=1}^{n} \frac{\omega^i}{1 + \omega^i} = \sum_{i=1}^{n} \frac{1}{1 + \omega^i}$$

Propriété 31 *Soit $P \in \mathbb{K}[X]$ non nul scindé. On l'écrit sous la forme $P = \lambda(X - \alpha_1)^{k_1} \dots (X - \alpha_n)^{k_n}$ où les α_i sont des scalaires distincts et les k_i des entiers naturels non nuls.. Alors*

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{k_i}{X - a_i}$$

Démonstration. On a déjà vu la dérivée de ce genre de polynômes :

$$P' = \sum_{i=1}^{n} k_i (X - a_i)^{k_i - 1} \prod_{\substack{j=1 \\ j \neq i}}^{n} (X - a_j)^{k_j} = \sum_{i=1}^{n} k_i \frac{P}{X - a_i} = P \sum_{i=1}^{n} \frac{k_i}{X - a_i}$$

On en déduit

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{k_i}{X - a_i}$$

Les physiciens parlent parfois de dérivée logarithmique.

Exemple 17 *Soit n un entier naturel supérieur ou égal à 2. On cherche à évaluer $\sum_{\omega \in \mathbb{U}_n \setminus \{1\}} \frac{1}{1-\omega}$. On pense alors au polynôme $X^n - 1$ dont les racines forment $\mathbb{U}_n$. En factorisant $X - 1$, on a $X^n - 1 = (X - 1)(1 + X + \cdots + X^{n-1})$ et on pose $P = 1 + X + \cdots + X^{n-1}$ qui se factorise sous la forme simplement scindée $\prod_{\omega \in \mathbb{U}_n \setminus \{1\}} (X - \omega)$. En appliquant ce qui précède, on obtient*

$$\frac{P'}{P} = \sum_{\omega \in \mathbb{U}_n \setminus \{1\}} \frac{1}{X - \omega}$$

De plus, $P' = 1 + 2X + 3X^2 + \cdots + (n-1)X^{n-2}$ fournit $P'(1) = 1 + 2 + \cdots + (n-1) = n(n-1)/2$. En outre $P(1) = n$. Conclusion,

$$\sum_{\omega \in \mathbb{U}_n \setminus \{1\}} \frac{1}{1 - \omega} = \frac{n - 1}{2}$$