Polynômes

Soit $\mathbb{K}$ un corps. (En pratique $\mathbb{R}$ ou $\mathbb{C}$).

I. Introduction

1. Définition et structure de $\mathbb{K}[X]$

Définition. *On appelle polynôme à une indéterminée à coefficients dans $\mathbb{K}$ tout suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang. Ainsi, l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, noté $\mathbb{K}[X]$ est égal à*

$$\mathbb{K}[X] = \{u \in \mathbb{K}^{\mathbb{N}} \ : \ \exists N \in \mathbb{N} \ : \ \forall n \geq N, \ u_n = 0\}$$

Proposition. *$(\mathbb{K}[X], +, .)$ est un sev de $\left(\mathbb{K}^{\mathbb{N}}, +, .\right)$*

Définition. *On définit sur $\mathbb{K}[X]$ un produit $\times$ par*

$$\forall (u, v) \in \mathbb{K}[X]^2, \ u \times v = \left(\sum_{k=0}^{n} u_k \, v_{n-k} \right)_{n \in \mathbb{N}}$$

Proposition. *$(\mathbb{K}[X], +, \times)$ est anneau commutatif.*

Définition. *On note $X = (0, 1, 0, .., 0, ...) = (\delta_{1,n})_{n \in \mathbb{N}}$*

Proposition. *Avec la convention, $X^0 = 1_{\mathbb{K}[X]}$, on a*

$$\forall k \in \mathbb{N}, \ X^k = (\delta_{k,n})_{n \in \mathbb{N}}$$

Remarque : Le polynôme $P = (a_0, a_1, ..., a_n, 0, .., 0, ...)$ qui est égal à $\left(\sum_{j=0}^{n} a_j \delta_{n,j} \right)_{n \in \mathbb{N}}$ est donc égal à $\sum_{k=0}^{n} a_k X^k$. On retrouve les notations habituelles.

Proposition. *La famille $(X^n))_{n \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$ appelée base canonique de $\mathbb{K}[X]$.*

Définition. *On dit qu'un polynôme est constant s'il est de la forme $\lambda 1_{\mathbb{K}[X]}$ avec $\lambda \in \mathbb{K}$. L'application $\phi : \mathbb{K} \to \mathbb{K}[X]$, $\lambda \mapsto \lambda 1_{\mathbb{K}[X]}$ étant injective, on identifie $\lambda 1_{\mathbb{K}[X]}$ et λ. En particulier, $1_{\mathbb{K}[X]}$ est noté 1.*
On dit qu'un polynôme est un monôme s'il est de la forme λX^k avec $\lambda \in \mathbb{K}$ et $k \in \mathbb{N}$.

Définition. *Soit $P = \sum_{k=0}^{n} a_k X^k$ et Q deux polynômes, on définit leur composé par*

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

Remarque : Pour tout polynôme P, on a $P \circ X = P$ ce qui explique que l'on note indifféremment P ou $P(X)$.

2. Degré et coefficient dominant d'un polynôme

Définition. *Si $P = (a_n)_{n\in\mathbb{N}} \in \mathbb{K}[X]$ est non nul alors l'ensemble $\{k \in \mathbb{N} : a_k \neq 0\}$ est non vide. On appelle degré de P son élément maximal. Par convention, le degré du polynôme nul est égal à $-\infty$.*

Définition. *Si $P = (a_n)_{n\in\mathbb{N}}$ est non nul alors on appelle coefficient dominant de P, le scalaire $a_{deg(P)}$. Sinon, le coefficient dominant est nul.*
On dit qu'un polynôme est unitaire si son coefficient dominant est égal à $1_{\mathbb{K}}$.

Proposition. *Tout polynôme non nul s'écrit de façon unique sous la forme λP_0 avec $\lambda \in \mathbb{K}^*$ et P_0 unitaire.*

Proposition. *Avec la convention $\forall n \in \mathbb{N}$, $n + (-\infty) = n$ et $-\infty + (-\infty) = -\infty$, on a :*

$$\forall (P, Q) \in \mathbb{K}[X]^2, \quad \deg(PQ) = \deg(P) + \deg(Q)$$

et le coefficient dominant d'un produit est le produit des coefficients dominants

Corollaire. *Le produit de deux polynômes non nuls est non nul.*
On dit que l'anneau $\mathbb{K}[X]$ est intègre.

Proposition. *Avec la convention $\forall n \in \mathbb{N}$, $max(n, -\infty) = n$ et $max(-\infty, -\infty) = -\infty$, on a*

$$\forall (P, Q) \in \mathbb{K}[X], \quad \deg(P + Q) \leq \max(\deg(P), \deg(Q))$$

avec égalité si $\deg(P) \neq \deg(Q)$

Remarque : Si $deg(P) = deg(Q)$ alors l'inégalité n'est pas forcément stricte (prendre $P = Q = X$) mais peut l'être (prendre $P = -Q$). Il y a en fait égalité si, et seulement si, la somme des coefficients dominants est non nulle.
Remarque : Si $degP = degQ$ et $dom(P) = dom(Q)$ alors $deg(P - Q) < deg(P)$.

Définition. *Soit n un entier, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n. Il s'agit d'un sev de $\mathbb{K}[X]$ de dimension $n + 1$ admettant $(1, X, .., X^n)$ comme base canonique.*

Proposition. *Soient P et Q deux polynômes.*
Si Q est non constant alors, $deg(P \circ Q) = deg(P)deg(Q)$.
Si Q est constant à a alors $P \circ Q$ est constant à $P(a)$.

II. Arithmétique dans $\mathbb{K}[X]$

1. Division euclidienne

Définition. *Soit $(P, Q) \in \mathbb{K}[X]^2$. On dit que P divise Q ou que P est un diviseur de Q ou que Q est un multiple de P et l'on note P/Q s'il existe $R \in \mathbb{K}[X]$ tel que $Q = PR$, ce qui est équivalent à $P\mathbb{K}[X] \subset Q\mathbb{K}[X]$.*

Définition. *On dit que deux polynômes P et Q sont associés lorsque P/Q et Q/P.*

Proposition. *Deux polynômes P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$*

Théorème. *Soit $(A, B) \in \mathbb{K}[X]^2$ avec B non nul alors il existe un unique couple de polynômes $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $deg(R) < deg(B)$.*

Définition. *On appelle idéal de $\mathbb{K}[X]$ tout sous-groupe $\mathcal{I}$ de $\mathbb{K}[X]$ tel que*

$$\forall (P, Q) \in \mathcal{I} \times \mathbb{K}[X], \quad PQ \in \mathcal{I}.$$

Théorème. *Soit $P \in \mathbb{K}[X]$, alors $P\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$.*
Réciproquement, si $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$, alors il existe un polynôme P tel que $\mathcal{I} = P\mathbb{K}[X]$.

Corollaire. *Si $\mathcal{I}$ est un idéal de $\mathbb{K}[X]$ distinct de $\{0_{\mathbb{K}[X]}\}$, alors il existe un unique polynôme unitaire tel que $\mathcal{I} = P\mathbb{K}[X]$.*

2. PGCD et PPCM

Théorème. *Soit P et Q deux polynômes tels que $(P,Q) \neq (0,0)$.*
On appelle PGCD de P et de Q et on note $P \wedge Q$, l'unique polynôme unitaire tel que

$$\forall D \in \mathbb{K}[X], \quad (D/P \text{ et } D/Q) \Leftrightarrow D/(P \wedge Q)$$

Il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $UP + VQ = P \wedge Q$ (Relation de Bézout).

Remarque : Pour tout polynôme unitaire P, on a $P \wedge 0 = P$

Proposition. *Soit $(P,Q) \in \mathbb{K}[X]^2$ et R le reste de la division Euclidienne de P par Q, alors $P \wedge Q = Q \wedge R$.*

Remarque : On peut obtenir le PGCD de deux polynômes A et B de façon constructive par l'algorithme d'Euclide :
On construit par récurrence la suite de polynômes $(R_n)_{n\in\mathbb{N}}$ par :

- $R_0 = A$, $R_1 = B$,
- pour tout $n \geq 1$, si R_n est nul alors R_{n+1} est nul et sinon R_{n+1} est le reste dans la division euclidienne de R_{n-1} par R_n.

La suite obtenue est presque nulle car sinon la suite $(deg(R_n))_{n\in\mathbb{N}}$ serait une suite d'entiers naturels strictement décroissante.
Soit n_0 le plus petit entier tel que R_{n_0} soit nul alors

$$\forall k \in [\![1, n_0 - 1]\!],\ R_k \wedge R_{k-1} = R_k \wedge R_{k+1}$$

donc $A \wedge B = R_{n_0-1} \wedge R_{n_0} = R_{n_0-1} \wedge 0$.
Soit D le polynôme unitaire obtenu en divisant R_{n_0-1} par son coefficient dominant, alors

$$D = A \wedge B$$

En remontant cet algorithme, on trouve un couple (U,V) tel que $AU + BV = 1$.

Définition. *Soit $(P_1, ..., P_r) \in \mathbb{K}[X]^r$.*
On appelle PGCD des polynômes P_1,..., P_r, et on note $P_1 \wedge ... \wedge P_r$, l'unique polynôme unitaire tel que

$$\forall D \in \mathbb{K}[X], \quad (\forall i \in [\![1, r]\!],\ D/P_i) \Leftrightarrow D/(P_1 \wedge ... \wedge P_r)$$

Il existe $(U_1, ..., U_r) \in \mathbb{K}[X]^r$ tel que $U_1P_1 + ... + U_rP_r = P_1 \wedge ... \wedge P_r$ (Relation de Bézout).

Définition. *Soit $(P,Q) \in \mathbb{K}[X]^2$.*
On appelle PPCM de P et de Q et on note $P \vee Q$, l'unique polynôme unitaire tel que

$$\forall M \in \mathbb{K}[X], \quad (P/M \text{ et } Q/M) \Leftrightarrow (P \vee Q)/M$$

3. Polynômes premiers entre eux

Définition. *Soit $(P,Q) \in \mathbb{K}[X]^2$.*
Si $P \wedge Q = 1_{\mathbb{K}[X]}$, on dit que P et Q sont premiers entre eux.

Proposition. *(Théorème de Bezout) Soit $(P,Q) \in \mathbb{K}[X]^2$ alors P et Q sont premiers entre eux si et seulement si*

$$\exists (U,V) \in \mathbb{K}[X]^2 \ :\ 1_{\mathbb{K}[X]} = UP + VQ$$

Remarque : S'il existe $(U,V) \in \mathbb{K}[X]^2$ tel que $D = UP + VQ$, on ne peut pas conclure que $D = P \wedge Q$ mais seulement que $P \wedge Q/D$.
Il faut que, de plus, D soit un polynôme unitaire divisant P et Q pour conclure que $D = P \wedge Q$.

Corollaire. *Soit $(P_1, ..., P_r, Q) \in \mathbb{K}[X]^{r+1}$ si $\forall k \in [\![1, r]\!],\ P_i \wedge Q = 1$, alors* $\left(\prod_{k=1}^{r} P_i\right) \wedge Q = 1$.

Proposition. *Soit a et b deux complexes distincts alors les polynômes $X-a$ et $X-b$ sont premiers entre eux. Plus généralement, pour tout couple d'entiers non nuls (n,m), les polynômes $(X-a)^n$ et $(X-b)^m$ sont premiers entre eux.*

Proposition. *(Théorème de Gauss) Soit $(P,Q,R)\in\mathbb{K}[X]^3$ alors*

$$(P/QR \text{ et } P\wedge Q=1_{\mathbb{K}[X]})\Rightarrow P/R$$

Corollaire. *Soit $(P_1,...,P_r,Q)\in\mathbb{K}[X]^{r+1}$ tel que*

$$\forall k\in[\![1,r]\!],\ P_i/Q \ \text{ et } \ \forall(k,k')\in[\![1,r]\!]^2,\ k\neq k'\Rightarrow P_k\wedge P_{k'}=1_{\mathbb{K}[X]}$$

alors $\displaystyle\prod_{k=1}^{r}P_i/Q$.

Définition. *Soit $(P_1,...,P_r)\in\mathbb{K}[X]^r$. Les polynômes $P_1,...,P_r$ sont dits premiers entre eux dans leur ensemble si $P_1\wedge...\wedge P_r=1$ et ils sont dits premiers entre eux deux à deux si*

$$\forall(k,k')\in[\![1,r]\!]^2,\ k\neq k'\Rightarrow P_k\wedge P_{k'}=1$$

Proposition. *Si les polynômes $P_1,...,P_r$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble.*

Proposition. *(Théorème de Bezout) Soit $(P_1,...,P_r)\in\mathbb{K}[X]^r$ alors les polynômes $P_1,...,P_r$ sont premiers entre eux dans leur ensemble si et seulement si*

$$\exists(U_1,...,U_r)\in\mathbb{K}[X]^r\ :\ P_1U_1+...+P_rU_r=1$$

4. Décomposition en irréductibles

Définition. *Un polynôme P est dit irréductible si*
- *P n'est pas constant*
- *$\forall(Q,R)\in\mathbb{K}[X]^2,\ P=QR\ \Rightarrow\ Q$ ou R est constant*

Autrement dit P n'est pas constant et ses seuls diviseurs sont les polynômes constants non nuls et les polynômes qui lui sont associés.

Proposition. *Un polynôme de degré 1 est irréductible.*

Théorème. *(admis)*
Soit P un polynôme non constant alors il existe $\lambda\in\mathbb{K}^*$, il existe des polynômes irréductibles unitaires distincts $(P_1,...,P_k)$ et des entiers naturels non nuls $(\alpha_1,..,\alpha_r)$ tels que

$$P=\lambda\prod_{k=1}^{r}P_i^{\alpha_i}$$

De plus cette décomposition est unique à l'ordre près.

III. Racines

1. Multiplicité

Définition. *A tout polynôme* $P = \sum_{k=0}^{n} a_k X^k$, *on associe la fonction* $\tilde{P} : x \mapsto \sum_{k=0}^{n} a_k x^k$

Proposition. *L'application* $\mathbb{K}[X] \to \mathcal{F}(\mathbb{K}, \mathbb{K})$, $P \mapsto \tilde{P}$ *est un morphisme d'anneaux et une application linéaire.*

Remarque : P et $\tilde{P}$ sont distincts mais nous allons dans la suite justifier que l'on peut les identifier. (Cela découlera du caractère infini de $\mathbb{K}$).

Définition. *Soit* $P \in \mathbb{K}[X]$. *On dit que* $a \in \mathbb{K}$ *est une racine de* P *si* $\tilde{P}(a) = 0$.

Remarque : Par abus, le scalaire $\tilde{P}(a)$ sera noté $P(a)$.
Remarque : On a également $P \tilde{\circ} Q = \tilde{P} \circ \tilde{Q}$.

Proposition. *Soit* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$ *alors* a *est une racine de* P *si et seulement si* $X - a$ *divise* P *i.e. si et seulement s'il existe* $Q \in \mathbb{K}[X]$ *tel que* $P = (X - a)Q$.

Proposition. *Soit* $P \in \mathbb{K}[X]$ *et* a_1,... ,a_r r *éléments distincts de* $\mathbb{K}$ *alors* a_1,..., a_r *sont racines de* P *si et seulement si* $(X - a_1)...(X - a_r)$ *divise* P *i.e. si et seulement s'il existe* $Q \in \mathbb{K}[X]$ *tel que* $P = (X - a_1)...(X - a_r)Q$.

Définition. *Soit* $P \in \mathbb{K}[X]$ *non nul et* $a \in \mathbb{K}$.
On appelle ordre de multiplicité de la racine a *le plus grand entier* m *tel que* $(X - a)^m$ *divise* P.
Ainsi, a *est une racine de* P *si et seulement si elle est de multiplicité non nulle.*
Si l'ordre de multiplicité, m, *de* a *est 1, on dit que* a *est une racine simple de* P. *Si* $m > 1$ *alors on dit que* a *est une racine multiple de* P.
En particulier, si $m = 2$, *on dit que* a *est racine double et si* $m = 3$, *on dit que* a *est racine triple.*

Corollaire. *Soit* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$.
Alors a *est une racine de* P *de multiplicité* m *si, et seulement si,*

$$\exists Q \in \mathbb{K}[X] \ : \ P = (X - a)^m Q \quad et \ Q(a) \neq 0$$

Proposition. *Soit* $P \in \mathbb{K}[X]$ *et* a_1,...,a_r r *éléments distincts de* $\mathbb{K}$ *alors* a_1,...,a_r *sont racines de* P *de multiplicités respectives supérieures à* m_1,..., m_r *si et seulement si* $(X - a_1)^{m_1}...(X - a_r)^{m_r}$ *divise* P.

Proposition. *Soit* $P \in \mathbb{K}[X]$ *et* a_1,...,a_r r *éléments distincts de* $\mathbb{K}$ *alors* a_1,...,a_r *sont racines de* P *de multiplicités respectives* m_1,..., m_r *si et seulement s'il existe* $Q \in \mathbb{K}[X]$ *tel que*

$$P = (X - a_1)^{m_1}...(X - a_r)^{m_r} Q \quad et \quad Q(a_1) \times ... \times Q(a_r) \neq 0$$

2. Théorème d'interpolation de Lagrange

Corollaire. *Tout polynôme de degré* n *a au plus* n *racines comptées avec leurs multiplicités.*

Corollaire. *Si* P *et* Q *sont deux polynômes de degré inférieur ou égal à* n *coïncidant en* $n + 1$ *points, alors* $P = Q$.

Corollaire. *Tout polynôme ayant une infinité de racines est nul.*

Corollaire. *L'application* $\Phi : \mathbb{K}[X] \to \mathcal{F}(\mathbb{K}, \mathbb{K})$, $P \mapsto \tilde{P}$ *est injective.*
Cela permet d'identifier un polynôme P *et sa fonction polynomiale associée qui sera par la suite notée* P. *Cette identification est valable car on considère un corps* $\mathbb{K}$ *égal à* $\mathbb{R}$ *ou* $\mathbb{C}$ *infini.*

Proposition. *Soit $a_1,\ldots,a_r$ r éléments distincts de $\mathbb{K}$. Alors pour tout $i \in [\![1,r]\!]$*

$$\exists! L_i \in \mathbb{K}_{r-1}[X] \ : \ \forall j \in [\![1,r]\!], \quad L_i(a_j) = \delta_{i,j} \quad \text{et } L_i \text{ est donné par : } L_i = \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$$

Théorème. *Soit $a_1,\ldots,a_r$ r éléments distincts de $\mathbb{K}$ et $b_1,\ldots,b_r$ r éléments non forcément distincts de $\mathbb{K}$. Alors $\exists! P \in \mathbb{K}_{r-1}[X] \ : \ \forall i \in [\![1,r]\!], \quad P(a_i) = b_i$.*

Le polynôme P est donné par : $P = \sum_{j=1}^{r} b_j L_j$

3. Polynômes scindés

Définition. *Soit $P \in \mathbb{K}[X]$. On dit que P est scindé dans $\mathbb{K}$ lorsqu'il est un produit de polynômes à coefficients dans $\mathbb{K}$ et de degré 1.*

Proposition. *Un polynôme P est scindé si et seulement s'il admet $deg(P)$ racines dans $\mathbb{K}$ comptées avec leurs multiplicités.*

Exemple. *Soit $a \in \mathbb{K}$ alors $(X-a)^k$ est scindé sur $\mathbb{K}$ car a est une racine de multiplicité k. Le polynôme X^2+1 est scindé sur $\mathbb{C}$ car possède deux racines simples i et $-i$ mais n'est pas scindé sur $\mathbb{R}$.*

Exemple. *Le polynôme X^n-1 est scindé sur $\mathbb{C}$ car possède n racines simples distinctes :*

$$X^n - 1 = \prod_{k=1}^{n}(X - e^{\frac{2ik\pi}{n}})$$

Lorsqu'un polynôme est scindé (ce qui est le cas dans $\mathbb{C}$), il existe des relations entre ces coefficients et ses racines.

Exemple. *Si $P = aX^2+bX+c = a(X-x_1)(X-x_2)$ avec $a \neq 0$ alors*

$$\begin{cases} -b/a = (x_1+x_2) \\ \ \ c/a = x_1x_2 \end{cases}$$

Exemple. *Si $P = aX^3+bX^2+cX+d = a(X-x_1)(X-x_2)(X-x_3)$ avec $a \neq 0$ alors*

$$\begin{cases} -b/a = (x_1+x_2+x_3) \\ \ \ c/a = (x_1x_2+x_1x_3+x_2x_3) \\ -d/a = x_1x_2x_3 \end{cases}$$

Proposition. *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ de degré n (i.e. $a_n \neq 0$) scindé de racines $x_1,\ldots,x_r$ (non forcément distinctes) alors $P = a_n \prod_{i=1}^{r}(X-x_i)$ et*

$$\frac{a_{n-1}}{a_n} = -\sum_{i=1}^{r} x_i \quad \text{et} \quad \frac{a_0}{a_n} = (-1)^n \prod_{i=1}^{r} x_i.$$

Remarque : Plus généralement, $\forall k \in [\![0,n-1]\!]$, $\dfrac{a_k}{a_n} = (-1)^{n-k} \displaystyle\sum_{I \in \mathcal{P}_k([\![1,n]\!])} \prod_{i\in I} x_i$ où $\mathcal{P}_k([\![1,n]\!])$ est l'ensemble des parties à k éléments de $[\![1,n]\!]$.

Exercice. *Soit $\theta \in \mathbb{R}$. Montrer que le polynôme $(X+1)^n - e^{i\theta}$ est scindé sur $\mathbb{C}$. En déduire que*

$$\forall \phi \in \mathbb{R}, \quad \prod_{k=0}^{n-1} \sin\left(\phi + \frac{k\pi}{n}\right) = \frac{\sin(n\phi)}{2^{n-1}}.$$

4. Théorème de d'Alembert-Gauss et décomposition

Théorème. *Théorème de d'Alembert-Gauss (admis) :*
Tout polynôme à coefficients dans $\mathbb{C}$ non constant admet au moins une racine dans $\mathbb{C}$. On dit que $\mathbb{C}$ est algébriquement clos.

Proposition. *Tout polynôme non constant à coefficients complexes est scindé*

Corollaire. *Tout polynôme à coefficients complexes non constant de degré n a exactement n racines comptées avec leurs multiplicité.*

Corollaire. *Les irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré un.*

Proposition. *Soit P un polynôme non constant à coefficients dans $\mathbb{C}$ alors il existe $\lambda \in \mathbb{C}^*$, des complexes distincts $(x_1, ..., x_r)$ et des entiers naturels non nuls $(\alpha_1, .., \alpha_r)$ tels que*

$$P = \lambda \prod_{k=1}^{r} (X - x_i)^{\alpha_i}$$

De plus cette décomposition est unique à l'ordre près.
Dans ce cas, λ est le coefficient dominant de P, les complexes $(x_1, ..., x_r)$ sont les racines de P et sont de multiplicités respectives $(\alpha_1, .., \alpha_r)$.

Proposition. *Soit $(x_1, ..., x_r)$ des complexes distincts et $(\alpha_1, .., \alpha_r, \beta_1, ..., \beta_r)$ des entiers naturels. Les polynômes $P = \prod_{k=1}^{r} (X - x_i)^{\alpha_i}$ et $Q = \prod_{k=1}^{r} (X - x_i)^{\beta_i}$ vérifient*

$$P \wedge Q = \prod_{k=1}^{r} (X - x_i)^{Min(\alpha_i, \beta_i)} \quad \text{et} \quad P \vee Q = \prod_{k=1}^{r} (X - x_i)^{Max(\alpha_i, \beta_i)}$$

Définition. *Soit $P = \sum_{n \in \mathbb{N}} a_n X^n$ un polynôme complexe. On note $\bar{P} = \sum_{n \in \mathbb{N}} \bar{a}_n X^n$.*

Proposition. *Soient P et Q deux polynômes complexes et $\lambda \in \mathbb{C}$.*
On a $\overline{P + \lambda Q} = \overline{P} + \overline{\lambda Q}$, $\overline{PQ} = \overline{P}\,\overline{Q}$, $\overline{P \circ Q} = \overline{P} \circ \overline{Q}$ et $\overline{P}\left(\overline{\lambda}\right) = \overline{P(\lambda)}$.

Remarque : Dans $\mathbb{R}$ tous les polynômes ne sont pas scindés.
Par exemple, le polynôme $X^2 + 1$ est scindé dans $\mathbb{C}$ mais pas dans $\mathbb{R}$.

Corollaire. *Les irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré un et les polynômes de degré deux de discriminant strictement négatif.*

Corollaire. *Soit $P \in \mathbb{C}[X]$, $a \in \mathbb{C}$ une racine de P de multiplicité m alors $\bar{a}$ est une racine de $\bar{P}$ de multiplicité m.*

Théorème. *Décomposition des polynômes à coefficients réels :*
Soit P un polynôme non constant à coefficients dans $\mathbb{R}$ alors il existe $\lambda \in \mathbb{R}^*$, des réels distincts $(x_1, ..., x_r)$, des réels $(a_1, ..., a_p, b_1, ..., b_p)$, et des entiers naturels non nuls $(\alpha_1, .., \alpha_r, \beta_1, ..., \beta_p)$ tels que

$$P = \lambda \prod_{k=1}^{r} (X - x_i)^{\alpha_i} \prod_{k=1}^{p} (X^2 + a_k X + b_k)^{\beta_i}$$

avec $\forall k \in [\![1, p]\!]$, $a_k^2 - 4b_k < 0$. De plus cette décomposition est unique à l'ordre près.
Le réel λ est le coefficient dominant de P et les complexes $x_1, ..., x_r$ sont les racines réelles de P.

IV. Dérivation

Définition. *On définit la dérivée du polynôme* $P = \sum_{k=0}^{deg(P)} a_k X^k$ *par* $P' = \sum_{k=1}^{deg(P)} k a_k X^{k-1}$

On définit les dérivées successives de P *par récurrence : pour tout entier* n *non nul la dérivée* $(n+1)$*-ème de* P*, notée* $P^{(n+1)}$*, est la dérivée de la dérivée* n*-ème de* P*,* $P^{(n)}$*.*

En particulier, la dérivée seconde de P *notée* $P^{(2)}$ *ou* P" *est égale à* $\sum_{k=2}^{deg(P)} k(k-1)a_k X^{k-2}$

Remarque : Il n'y a bien sûr, pas de différence entre la dérivée de la fonction polynomiale $\tilde{P}$ et la fonction polynomiale associée au polynôme P' i.e. $\tilde{P}' = \widetilde{P'}$.

Proposition. *Soit* $P \in \mathbb{K}[X]$*. On a* $P' = 0 \Leftrightarrow P \in \mathbb{K}_0[X]$*.*

Corollaire. *Soit* $(P, Q) \in \mathbb{K}[X]^2$*. On a* $P' = Q' \Leftrightarrow P - P(0) = Q - Q(0)$*.*

Proposition. *Soit* $P \in \mathbb{K}[X]$*. On a* $deg(P') \leq deg(P) - 1$ *avec égalité si* P *n'est pas constant. De plus, si* P *est non constant, alors* $dom(P') = dom(P) \times deg(P)$

Proposition. *Soit* $P \in \mathbb{K}[X]$ *de degré* d *alors*

- $\forall k \in [\![0, d]\!]$, $\deg(P^{(k)}) = d - k$ *et* $dom(P^{(k)}) = \dfrac{d!}{(d-k)!}\, domP$
- $\forall k \in \mathbb{N}$, $k > deg(P) \Rightarrow P^{(k)} = 0$

Proposition. *Soit* $(P, Q) \in \mathbb{K}[X]^2$*,* $(k, n) \in \mathbb{N}$ *et* $(\lambda, \mu) \in \mathbb{K}^2$ *alors*

- $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$
- $(PQ)' = PQ' + P'Q$
- $\left(P^k\right)' = kP'P^{k-1}$
- *Formule de Leibniz :* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$
- $(P \circ Q)' = Q' \times P' \circ Q$

Proposition. *Soit* n *un entier et* $a \in \mathbb{K}$ *alors*

$$\forall k \in [\![0, n]\!],\ ((X-a)^n)^{(k)}) = n(n-1)...(n-k+1)(X-a)^{n-k} = \frac{n!}{(n-k)!}(X-a)^{n-k}$$

Proposition. *Formule de Taylor pour les polynômes :*
Soit $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$ *alors*

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

Corollaire. *Soit* $P \in \mathbb{K}[X]$*,* $a \in \mathbb{K}$ *et* $r \in \mathbb{N}$*.*

Le reste dans la division euclidienne de P *par* $(X-a)^r$ *est* $\sum_{i=0}^{r-1} \frac{P^{(i)}(a)}{i!}(X-a)^i$*.*

Corollaire. *Soit* $P \in \mathbb{K}[X]$*,* $a \in \mathbb{K}$ *et* k *un entier non nul alors*

$$(X-a)^k / P \Leftrightarrow P(a) = P'(a) = .. = P^{(k-1)}(a) = 0$$

Ainsi, a *est une racine de multiplicité supérieure à* k *si et seulement si elle est racine des polynômes* P*,* P'*,... et* $P^{(k-1)}$*.*
En particulier, a *est une racine multiple si et seulement si elle est racine de* P *et* P'*.*

Remarque : Ce résultat permer de démontrer très rapidement qu'un polynôme P est à racines simples : il suffit qu'il n'ait pas de racine en commun avec sa dérivée.
Par exemple, si on prend le polynôme $P = X^n - e^{i\theta}$, alors $P' = nX^{n-1}$. Comme P' n'a qu'une racine, 0, et comme 0 n'est pas racine de P, on peut en déduire que les racines de P sont simples sans les calculer (ce que l'on sait faire néanmoins).

Corollaire. *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Il y a équivalence entre*

1. *a est une racine de P de multiplicité m*
2. *$P(a) = P'(a) = .. = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.*

Corollaire. *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ une racine de P alors a est une racine de multiplicité m de P si et seulement si a est une racine de multiplicité $m-1$ de P'.*

Proposition. *Si $P \in \mathbb{R}[X]$ est un polynôme scindé simple (i.e. scindé à racines simples) de degré supérieur ou égal à deux, alors P' est aussi un polynôme scindé simple.*

Remarque : Ce résultat n'est pas conservé dans $\mathbb{C}[X]$: $X^3 - 1$ est scindé simple dans $\mathbb{C}$ mais $3X^2$ n'est pas scindé simple dans $\mathbb{C}$.

Proposition. *Si $P \in \mathbb{R}[X]$ est un polynôme scindé de degré supérieur ou égal à deux, alors P' est aussi un polynôme scindé.*

Remarque : Ce résultat est conservé dans $\mathbb{C}[X]$ mais sans intérêt car tout polynôme non constant à coefficients complexes est scindé