Chapitre 27

Polynômes 2

$$L_i := \frac{\displaystyle\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}} (X - a_j)}{\displaystyle\prod_{\substack{0\leqslant j\leqslant n\\ j\neq i}} (a_i - a_j)}$$

Expression du i-ième polynôme de Lagrange

Dans ce chapitre, on poursuit l'étude des polynômes. En particulier, on va commencer l'étude arithmétique des polynômes et ébaucher une comparaison entre $\mathbb{Z}$ et $\mathbb{K}[X]$.

Chapitre 27 : Polynômes 2

I, Composition de polynômes

1) Définition

Soit $P \in \mathbb{K}[X]$ qu'on écrit $P = \sum_{k=0}^{n} a_k X^k$

où $n \in \mathbb{N}$ et $\forall k$, $a_k \in \mathbb{K}$

Soit $Q \in \mathbb{R}[X]$

Le polynôme composé P par Q noté $P \circ Q$ est déf par :

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

On remplace X par Q dans l'expr. de P

Rq : ce polynôme est aussi noté $P(Q)$

ex : $P = 3X^2 + 2X - 1$

$P(X^2) = 3X^4 + 2X^2 - 1$

$P(X+1) = P \circ (X+1) = 3(X+1)^2 + 2(X+1) - 1$

Rq : $P, Q \in \mathbb{R}[X]$

Alors $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$

On a $X \in \mathbb{R}[X]$

On peut calculer $P \circ X$

On a $P \circ X = P$

ie, on a $P(X) = P$

2) Propriétés

Prop : $P_1, P_2, Q \in \mathbb{K}[X]$

1) $(P_1 + P_2) \circ Q = P_1 \circ Q + P_2 \circ Q$

2) $(P_1 \times P_2) \circ Q = P_1 \circ Q \times P_2 \circ Q$

3) $(P \circ Q) \circ R = P \circ (Q \circ R)$

4) ⚠ Un polynôme n'est pas linéaire

$$P \circ (Q + R) \neq P \circ Q + P \circ R$$

5) $\deg(P \circ Q) = \deg P \times \deg Q$ si $\deg(Q) \geq 1$

démo :

5) Oq $\deg Q \geq 1$ avec $n := \deg P$

On écrit $P = \sum_{k=0}^{n} a_k X^k$ $(a_n \neq 0)$

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

$$= a_n \cdot Q^n + \sum_{k=0}^{n-1} a_k \cdot Q^k$$

$\deg Q^k = k \times \deg Q$

$\deg Q^n = n \cdot \deg Q$

donc $\deg(a_n \, Q^n) = n \deg Q \leq \max_{k \in [\![0, n-1]\!]} \deg(a_k, Q^k)$

$\leq \max \deg(Q^k)$

et $\max_{k \in [\![0,n-1]\!]} k \cdot \deg(Q) < n \cdot \deg Q$ car $\deg Q \geq 1$

donc $\deg\left(a_n \cdot Q^n + \sum_{k=0}^{n-1} a_k Q^k\right) = \deg(a_n \cdot Q^n)$
$= n \cdot \deg Q$
$= \deg P \cdot \deg Q$

Ctr ex $\deg(P \circ Q) \neq \deg P \times \deg Q$ si $\deg Q = 0_{ou} -\infty$

On prend $P = X^2 - 4$ $\quad \deg P = 2$
$Q = 2$ $\quad \deg Q = 0$
$P(Q) = 4 - 4 = 0$
$\deg P \circ Q = -\infty \neq \deg P \times Q = 0$

II, Arithmétique des polynômes

1) Division euclidienne des polynômes

Prop : Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$

Alors $\exists ! (Q, R) \in \mathbb{K}[X]^2 : A = BQ + R$ et $\deg R < \deg B$

démo :

Unicité : Soient $(Q_1, R_1), (Q_2, R_2) \in \mathbb{K}[X]^2$ tq $A = BQ_1 + R_1$
$A = BQ_2 + R_2$

avec $\deg R_1 < \deg B$ et $\deg R_2 < \deg B$

On écrit $BQ_1 + R_1 = BQ_2 + R_2$
donc $B(Q_1 - Q_2) = R_2 - R_1$

En degré :

$$\deg B + \deg(Q_1 - Q_2) = \deg(R_2 - R_1)$$

Osq $Q_1 \neq Q_2$

On a donc $Q_1 - Q_2 \neq 0$

donc, $\deg(Q_1 - Q_2) \in \mathbb{N}$

donc, $\deg(B) + \deg(Q_1 - Q_2) \geqslant \deg B$

donc, $\deg(R_2 - R_1) \geqslant \deg(B)$

Or, $\deg(R_2 - R_1) \leqslant \max(\deg R_2, \deg R_1)$

$< \deg B$

Absurde

donc $Q_1 = Q_2$

donc $R_2 - R_1 = B \cdot (Q_1 - Q_2) = 0$

CCL : on a $Q_1 = Q_2$ et $R_1 = R_2$

Existence : On fait une preuve par récurrence sur $\deg A$

Initialisation : Si $\deg A < \deg B$, on a déjà notre DE : $A = B \cdot 0 + A$

quotient $\to 0$ reste A

Hérédité forte : Soit $n \in \mathbb{N}^*$

On suppose qu'on sait faire la DE de P par B si $\deg P \leqslant n$

On considère A un polynôme de degré $n+1$.

Osq $n+1 \geqslant \deg B$

On écrit $A = \sum_{k=0}^{n+1} a_k X^k$ avec $a_{n+1} \neq 0$

et $B = \sum_{k=0}^{p} b_k X^k$ avec $b_p \neq 0$

et $p \leqslant n+1$

On veut éliminer le coeff en X^{n+1} de A

On fait $A - \frac{a_{n+1}}{b_p} B \cdot X^{(n+1)-p}$

Dans cette expr, les termes en X^{n+1} se simplifient

On a donc $\deg\left(A - \frac{a_{n+1}}{b_p} B \cdot X^{n+1-p}\right) < n+1$

On peut appliquer l'hyp de récurrence à ce polynôme

Soient donc $(Q,R) \in \mathbb{K}[X]$ tq $A - \frac{a_{n+1}}{b_p} . B . X^{n+1-p} = BQ + R$

et $\deg R < \deg B$

On a $A = \underbrace{B . \left(\frac{a_{n+1}}{b_p} X^{n+1-p} + Q\right)}_{\text{quotient}} + \underbrace{R}_{\text{reste}}$

Rq : l'assertion qu'on démontre est :

$P(n)$: " $\forall P \in \mathbb{K}_n[X], \exists (Q,R) \in \mathbb{K}[X]^2 : \begin{cases} P = BQ + R \\ \deg R < \deg B \end{cases}$ "

Ex :

$$\begin{array}{r|l}
5X^4 + 3X^3 - 2X + 1 & X - 5 \\
\cline{2-2}
5X^4 - 25X^3 & 5X^3 + 28X^2 + 140X \\
\cline{1-1}
28X^3 - 2X + 1 & \quad + 698 \\
28X^3 - 140X^2 & \\
\cline{1-1}
140X^2 - 2X + 1 & \\
140X^2 - 700X & \\
\cline{1-1}
698X + 1 & \\
698X - 3490 & \\
\cline{1-1}
\end{array}$$

d'où $5X^4+3X^3-2X+1 = (X-5)(5X^3+28X^2+140X+698)$
$+3491$

2) Divisibilité

Rappel : $a, b \in \mathbb{Z}$
$a \mid b \overset{\Delta}{\text{ssi}} \exists k \in \mathbb{Z} : b = k.a$

Déf : Soient $A, B \in \mathbb{K}[X]$
On dit que A divise B $_{\text{dans } \mathbb{K}[X]}$ et on note $A \mid B$
$\overset{\Delta}{\text{ssi}} \; \exists C \in \mathbb{K}[X] : B = A.C$

Rq : on peut faire cette déf dans n'importe quel anneau (commutatif)
rappel : anneau : $A(A, +, \times)$ tq :
- $(A, +)$ grp commutatif, de neutre 0
- "$\times$" possède un neutre dans A noté 1
- distributivité : $(a+b) \times c = a \times c + b \times c$, etc...

ex : $(\mathbb{Z}, +, \times, 0, 1)$
$(M_n(\mathbb{K}), +, \times, 0_n, I_n)$ sont commutatifs
$(L(E), +, \circ, 0_{L(E)}, Id_E)$

Ex . $X-1 \mid X^2-1$ dans $\mathbb{R}[X]$
car $X^2-1 = (X-1)(X+1)$

. $X-i \mid X^2+1$ dans $\mathbb{C}[X]$
car $X^2+1 = (X-i)(X+i)$

. $a, b, c \in \mathbb{R}$ avec $a \neq 0$, $\Delta = b^2-4ac \geq 0$
alors $\left(X - \frac{-b+\sqrt{\Delta}}{2a}\right) \mid aX^2+bX+c$

démo du dernier point :

il faut calculer : $\left(X - \frac{-b+\sqrt{\Delta}}{2a}\right) a \left(X - \frac{-b-\sqrt{\Delta}}{2a}\right) = aX^2 + bX + c$

- $P \in \mathbb{K}[X]$
  $P(0) = 0 \Rightarrow X \mid P$

si $P(0)=0$ on a $P = \sum_{k=1}^{n} a_k X^k = X \cdot \left(\sum_{k=1}^{n} a_k X^{k-1}\right)$

on a bien $X \mid P$

<u>Rappel</u> : on a montré que
$\forall P \in \mathbb{K}[X], \forall \alpha \in \mathbb{K}, \; P(\alpha) = 0 \Leftrightarrow \exists Q \in \mathbb{R}[X] :$
$P = (X-\alpha) \cdot Q$
$\Leftrightarrow (X-\alpha) \mid P$

Les propriétés de "|" dans $\mathbb{Z}$ sont pour la plupart encore vraies dans $\mathbb{K}[X]$

- $\left.\begin{matrix} P \mid Q \\ Q \mid R \end{matrix}\right\} \Rightarrow P \mid R$
- $P \mid P$
- $\left\{\begin{matrix} P \mid Q \\ Q \neq 0 \end{matrix}\right. \Rightarrow \deg P \leqslant \deg Q$

- $\forall P \in \mathbb{K}[X], \; P \mid 0$
  (en effet : $0_{\mathbb{K}[X]} = 0_{\mathbb{K}[X]} \cdot P$)

On a $2X \mid X$
En effet, $X = 2X \cdot \frac{1}{2}$ et on a aussi $X \mid 2X$
car $2X = X \cdot 2$

mais $2X \neq X$

$\left.\begin{array}{l} \cdot\ P \mid Q \\ P \mid R \end{array}\right\} \Rightarrow \forall (U,V) \in \mathbb{K}[X]^2,\ P \mid Q\cdot U + R\cdot V$

$\cdot\ P \mid Q \Rightarrow Z_{\mathbb{K}}(P) \subset Z_{\mathbb{K}}(Q)$

démo : on écrit $Q = P \cdot R$
Soit $\alpha \in Z_{\mathbb{K}}(P)$
On a $Q(\alpha) = P(\alpha) \cdot R(\alpha) = 0$
donc $\alpha \in Z_{\mathbb{K}}(Q)$

Rappel dans $\mathbb{Z}$: $\forall n \in \mathbb{Z}\ (0 \mid n \Rightarrow n = 0)$

de m̂, $\forall P \in \mathbb{R}[X],\ (0 \mid P \Rightarrow P = 0)$

démo : soit $P \in \mathbb{K}[X]$ tq $0 \mid P$
soit donc $R \in \mathbb{K}[X]$ tq $P = 0 \cdot R$ donc $P = 0$

3) Inversibles de $\mathbb{K}[X]$

Déf : Soit $P \in \mathbb{K}[X]$
On dit que P est inversible dans $\mathbb{K}[X]$
ssi $\exists Q \in \mathbb{R}[X] : P \cdot Q = 1$
On note $\mathcal{U}(\mathbb{K}[X])$ ou $\mathbb{K}[X]^{\times}$
l'ens. des inversibles de $\mathbb{K}[X]$

Prop : $\mathcal{U}(\mathbb{K}[X]) = \mathbb{K}^*$

démo : Soient $P, Q \in \mathbb{K}[X]$ tq $P \cdot Q = 1$
donc $\deg P + \deg Q = \deg 1 = 0$
donc, $\deg P = \deg Q = 0$
donc, $P \in \mathbb{K}^*$

Prop : Soient P et $Q \in \mathbb{K}[X]$ tq $P \mid Q$ et $Q \mid P$

alors $\exists \lambda \in \mathbb{K}^*$: $P = \lambda \cdot Q$

on dit que P et Q sont associés

démo : Osq $P \mid Q$ et $Q \mid P$
Soient donc $R, T \in \mathbb{K}[X]$ tq : $Q = P \cdot R$ et $P = Q \cdot T$

donc $Q = Q \cdot T \cdot R$

. Si $Q = 0$, c̃ $Q \mid P$ on a $0 \mid P$ donc $P = 0$
donc on a $P = 1 \cdot Q$

. Si $Q \neq 0$
c̃ $Q = Q \cdot T \cdot R$, on a $1 = TR$

rappel : $\mathbb{K}[X]$ est intègre
$PQ = 0 \Rightarrow P = 0$ ou $Q = 0$
. ⚠ $M_n(\mathbb{K})$ ou $\mathcal{L}(E)$ ne sont pas intègres

. $\left.\begin{array}{l} Q \neq 0 \\ QP_1 = QP_2 \end{array}\right\} \Rightarrow P_1 = P_2$

(démo : $Q(P_1 - P_2) = 0$
or $Q \neq 0$ donc $P_1 - P_2 = 0$)

donc $T, R \in \mathbb{K}^*$

III, Racines multiples

1) Rappel

Prop : α racine de $P \iff (X-\alpha) \mid P$

démo : ($\Leftarrow$) $X-\alpha \mid P \Rightarrow Z_{\mathbb{K}}((X-\alpha)) \subset Z_{\mathbb{K}}(P)$

$\alpha \in Z_{\mathbb{K}}(P)$

($\Rightarrow$) On fait une DE

Osq $P(\alpha) = 0$

On fait la DE de P par $(X-\alpha)$

Soit donc $Q, R \in \mathbb{K}[X]$ tq $P = (X-\alpha)Q + R$ $(*)$

avec $\deg R < \deg (X-\alpha) = 1$

ie $\deg R \leqslant 0$ ie $R \in \mathbb{K}$ on note $c := R$

On évalue $(*)$ en α

$P(\alpha) = (\alpha - \alpha) Q(\alpha) + c$

donc $c = P(\alpha) = 0$

donc $(*)$ s'écrit : $P = (X-\alpha) Q$

donc $(X-\alpha) \mid Q$

2) Multiplicité d'une racine

Déf : $P \neq 0$, $a \in \mathbb{K}$

La multiplicité de a en tant que racine de P est l'entier : $\max \left\{ k \in \mathbb{N} \mid (X-a)^k \mid P \right\}$

notée dans le cours $m_a(P)$

. si $m_a(P) = 0$: a n'est pas racine

. si $m_a(P) \geq 1$: a est racine

. si $m_a(P) = 1$: on dit que a est racine simple

. si $m_a(P) = 2$: a est racine double

Convention : $m_a(0) = +\infty$

Ex : $(X+1)^2 \, X^3 \, (X-2)$

-1 est rac. double, 0 est racine triple

2 est racine simple

Lemme : $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $n \in \mathbb{N}^*$

Alors a est racine de P de multiplicité n

$$\iff$$

$$\exists Q \in \mathbb{K}[X] : \begin{cases} P = (X-a)^n \cdot Q \\ Q(a) \neq 0 \end{cases}$$

démo :

$\Rightarrow$ Osq $m_a(P) = n$

on sait que $(X-a)^n \mid P$

et $(X-a)^{n+1} \nmid P$

Soit donc $Q \in \mathbb{K}[X]$ tq $P = (X-a)^n \cdot Q$

Mq $Q(a) \neq 0$

Si on avait $Q(a) = 0$ alors on aurait $(X-a) \mid Q$

donc, on aurait $(X-a) \cdot (X-a)^n \mid Q \cdot (X-a)^n$

ie $(X-a)^{n+1} \mid P$: absurde

($\Leftarrow$) Osq $\exists Q \in \mathbb{K}[X] : P = (X-a)^n \cdot Q$ et $Q(a) \neq 0$

Fixons un tel Q

On a $(X-a)^n \mid P$

donc $m_a(P) \geqslant n$

Supposons $m_a(P) \geqslant n+1$ et écrivons $P = (X-a)^{n+1} \cdot R$

avec $R \in \mathbb{K}[X]$

On écrit $(X-a)^n Q = (X-a)^{n+1} R$

donc $Q = (X-a) \cdot R$

Absurde car $Q(a) \neq 0$

Prop:

1) $m_\alpha(P \cdot Q) = m_\alpha(P) + m_\alpha(Q)$

2) $m_\alpha(P+Q) \geqslant \min(m_\alpha(P), m_\alpha(Q))$

Rq : on voit une analogie entre

$$v_p(\cdot) : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$$
$$m_\alpha(\cdot) : \mathbb{K}[X] \to \mathbb{N} \cup \{\infty\}$$
$$\deg(\cdot) : \mathbb{K}[X] \to \mathbb{N} \cup \{-\infty\}$$

démo :

1) On écrit $P = (X-\alpha)^{m_P} \cdot R$ où $m_P := m_\alpha(P)$

$Q = (X-\alpha)^{m_Q} \cdot S$ où $m_Q := m_\alpha(Q)$

et $R(\alpha) \neq 0$, $S(\alpha) \neq 0$

On a $P \cdot Q = (X-\alpha)^{m_P + m_Q} \cdot R \cdot S$

On a $RS(\alpha) = R(\alpha) \cdot S(\alpha) \neq 0$

d'après le lemme, $m_\alpha(PQ) = m_P + m_Q$

2) Contre-exemple de l'égalité

On cherche $P, Q \in \mathbb{K}[X]$

$\alpha \in \mathbb{K}$

tq $m_\alpha(P+Q) > \min(m_\alpha(P), m_\alpha(Q))$

$m_\alpha(P) = n \quad (n \in \mathbb{N}^*)$

- $P = (X-\alpha)^n$

$Q = (X-\alpha)^n \left[(X-\alpha) - 1 \right]$

On a $m_\alpha(P) = n$

$m_\alpha(Q) = n$

et $P+Q = (X-\alpha)^n \left[\cancel{1} + X - \alpha - \cancel{1} \right] = (X-\alpha)^{n+1}$

$m_\alpha(P+Q) = n+1$

On écrit $P = (X-\alpha)^n \cdot R$

$Q = (X-\alpha)^m \cdot S \quad (*)$

Qsq $n \leq m$

$(*)$ s'écrit $Q = (X-\alpha)^n \left[(X-\alpha)^{m-n} \cdot S \right]$

donc $P+Q = (X-\alpha)^n \left[R + (X-\alpha)^{m-n} \cdot S \right]$

donc $m_\alpha(P+Q) \geq n = \min(m_\alpha(P), m_\alpha(Q))$

Rq si $m \neq n$ ie si $n < m$

alors $\left(R + (X-\alpha)^{m-n} S \right)(\alpha) = R(\alpha) \neq 0$

Fait : $m_\alpha(P) \neq m_\alpha(Q)$

$$\Downarrow$$

$$m_\alpha(P+Q) = \min(m_\alpha(P), m_\alpha(Q))$$

3) Factorisation simultanée

Prop : $P \in \mathbb{K}[X]$, $r \in \mathbb{N}^*$

$\alpha_1, \dots, \alpha_r \in \mathbb{K}$ 2 à 2 $\neq$

$m_1, \dots, m_r \in \mathbb{N}^*$

Osq α_i est racine de P de multiplicité m_i pour tout $i \in [\![1, r]\!]$

Alors, $\exists Q \in \mathbb{K}[X] : P = \prod_{i=1}^{r} (X-\alpha_i)^{m_i} \cdot Q$

démo : Récurrence

$P(k)$: " $\exists Q \in \mathbb{K}[X] : P = \prod_{i=1}^{k} (X-\alpha_i)^{m_i} \cdot Q$ "

pour $k \in [\![1, r]\!]$.

$P(1)$: ok, c'est le lemme précédent, c'est la déf de $m_{\alpha_1}(P) = m_1$

Hérédité : Soit $k \in [\![1, r-1]\!]$ tq $P(k)$ est vraie
Soit donc $Q \in \mathbb{K}[X]$ tq : $P = \prod_{i=1}^{k} (X-\alpha_i)^{m_i} \cdot Q$

On sait que :

$$\forall P, Q, \alpha, \ m_\alpha(P \cdot Q) = m_\alpha(P) + m_\alpha(Q)$$

donc : $m_{\alpha_{k+1}}(P) = m_{\alpha_{k+1}}\left(\prod_{i=1}^{k}(X-\alpha_i)^{m_i}\cdot Q\right)$

$$= \left(\sum_{i=1}^{k} \underbrace{m_{\alpha_{k+1}}(X-\alpha_i)^{m_i}}_{=0}\right) + m_{\alpha_{k+1}}(Q)$$

car $(X-\alpha_i)^{m_i}(\alpha_{k+1}) = (\alpha_{k+1}-\alpha_i)^{m_i} \neq 0$

donc $m_{\alpha_{k+1}}(Q) = m_{\alpha_{k+1}}(P)$

donc on écrit $Q = (X-\alpha_{k+1})^{m_{k+1}}\cdot R$
avec $R \in \mathbb{K}[X]$

CCL : On a $P = \prod_{i=1}^{k+1}(X-\alpha_i)^{m_i}\cdot R$

donc $P(k+1)$ est vraie.

4) Majoration du nombre de racines

Théorème : Soit $n \in \mathbb{N}$

1) Un polynôme de degré n possède au plus n racines comptées avec multiplicité

2) Soit $P \in \mathbb{K}_n[X]$
Si P possède au moins $n+1$ racines comptées avec multiplicité, alors $P = 0$

<u>démo</u> : Soit $P \in \mathbb{K}[X]$ tq $\deg P = n$

Soient $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ les racines de P.

On note $m_i := m_{\alpha_i}(P)$ pour $i \in [\![1, r]\!]$

(On sait que $P \neq 0$ car $\deg P \neq -\infty$ donc P admet un nb fini de racines dans $\mathbb{K}$)

Soit donc $Q \in \mathbb{R}[X]$ tq $P = \prod_{i=1}^{r} (X - \alpha_i)^{m_i} \cdot Q$

On passe au degré.

On a $\deg P = \sum_{i=1}^{r} m_i + \deg(Q)$

Or $Q \neq 0$ (sinon, on aurait $P = 0$)

donc $\deg_n Q \geq 0$

donc : $\sum_{i=1}^{r} m_i \leq \deg(P)$

IV. Dérivation dans $\mathbb{K}[X]$

1) Lemme d'algèbre linéaire

<u>Lemme</u> : E $\mathbb{K}$-ev

Soient $f, g : \mathbb{K}[X] \to E$

$\forall n \in \mathbb{N}, f(X^n) = g(X^n) \Rightarrow f = g$

<u>démo</u> : Soit $P \in \mathbb{K}[X] \setminus \{0\}$

Mq $f(P) = g(P)$

On note $n := \deg(P)$

On a $P \in \mathbb{K}_n[X]$

On considère $f|_{\mathbb{K}_n[X]}$ et $g|_{\mathbb{K}_n[X]}$ qui coïncident

sur $(1, X, \dots, X^n)$ qui est une base de $\mathbb{K}_n[X]$

donc : $f|_{\mathbb{K}_n[X]} = g|_{\mathbb{K}_n[X]}$

donc en P, on a $f(P) = g(P)$

Rq : ce résultat reste vrai en remplaçant $(1, X, X^2, \dots)$ par n'importe quelle famille échelonnée de polynômes ie $(P_0, P_1, P_2, P_3, \dots)$ où $\forall i$, $\deg P_i = i$

Rappel : Soit $n \in \mathbb{N}$

Soit $(P_0, \dots, P_n) \in \mathbb{K}_n[X]^{n+1}$ tq $\forall i$, $\deg P_i = i$

alors $(P_0, \dots, P_n)$ base de $\mathbb{K}_n[X]$

2) Définition

Déf : Soit $P \in \mathbb{K}[X]$ qu'on écrit $P = \sum_{k=0}^{N} a_k X^k$

Le polynôme dérivé de P, noté P', est défini par :

$$P' = \sum_{k=1}^{N} k \cdot a_k X^{k-1}$$

Exemple : $(4X^3 - 5X^2 + 8X - 1)' = 12X^2 - 10X + 8$

On a, si $n \in \mathbb{N}^*$: $\left(\frac{(X-a)^n}{n!}\right)' = \frac{(X-a)^{n-1}}{(n-1)!}$

démo : On a : $(X-a)^n = \sum_{k=0}^{n} \binom{n}{k} (-a)^{n-k} X^k$

donc $((X-a)^n)' = \sum_{k=1}^{n} \binom{n}{k} (-a)^{n-k} \cdot k \cdot X^{k-1}$

on veut $(\dots)^{n-1}$

on a $k\binom{n}{k} = n\binom{n-1}{k-1}$ si $n \in \mathbb{N}^*$, $k \in \mathbb{Z}$

ou $k\binom{n}{k} = k \times \frac{n!}{(n-k)!\,k!}$

$n - k = (n-1) - (k-1)$

donc $k\binom{n}{k} = n \cdot \frac{(n-1)!}{((n-1)-(k-1))!\,(k-1)!} = n \cdot \binom{n-1}{k-1}$

$$\left((X-a)^n\right)' = \sum_{k=1}^{n} k\binom{n}{k}(-a)^{n-k} X^{k-1}$$

$$= n \cdot \sum_{k=1}^{n} \binom{n-1}{k-1}(-a)^{n-k} X^{k-1}$$

$$= n \cdot \sum_{k=1}^{n} \binom{n-1}{k-1}(-a)^{n-1-(k-1)} X^{k-1}$$

$$= n \cdot \sum_{l=0}^{n-1} \binom{n-1}{l}(-a)^{n-1-l} \cdot X^{l}$$

$$= n \cdot (X-a)^{n-1} \quad \text{(Newton)}$$

3) Propriétés de la dérivation

Prop : Soient $P, Q \in \mathbb{K}[X]$

1) a) $\deg P \leq 0$ (P constant) $\Rightarrow P' = 0$

b) $\deg P \geq 1 \Rightarrow \deg P' = \deg P - 1$

2) La dérivation est linéaire

$D : \mathbb{K}[X] \to \mathbb{K}[X]$ est linéaire

$P \mapsto P'$

3) $(P\cdot Q)' = P'\cdot Q + P\cdot Q'$

4) $(P\circ Q)' = (P'\circ Q)\times Q'$

démo :

1) ok

2) ok

3) Mq $\forall P, Q$, $(PQ)' = P'Q + P\cdot Q'$

Fixons Q

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

Il s'agit d'une propriété linéaire.

On introduit

$$f_Q : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$$
$$P \longmapsto (P\cdot Q)'$$

$$g_Q : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$$
$$P \longmapsto P'Q + P\cdot Q'$$

alors $f_Q, g_Q \in L(\mathbb{K}[X])$

1ère démo : on calcule

$$f_Q(P_1+\lambda P_2) = ((P_1+\lambda P_2)\cdot Q)' = (P_1 Q + \lambda P_2 Q)'$$
$$= (P_1 Q)' + \lambda (P_2\cdot Q)'$$
$$= f_Q(P_1) + \lambda f_Q(P_2)$$

idem pour g_Q

2ème démo :

Soit $R \in \mathbb{K}[X]$, on note $m_R : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$
$$P \longmapsto P\cdot R$$

On sait que :

$\forall P_1, P_2$, $(P_1+P_2)\cdot R = P_1\cdot R + P_2\cdot R$

$(\lambda P_1) R = \lambda \cdot (P_1 \cdot R)$

c'est la distributivité de $\times$ sur $+$, c'est vrai dans une algèbre en général !

groupe commutatif $\to$ $+$ groupe $\to$ $\cdot$ et x^{-1}, e

anneau $\to$ $+$ et $\times$

ev $\to$ $+$ et scalarisation

algèbre $\to$ $+, \times$, scalarisation

$f_Q(P) = (P\cdot Q)'$

$g_Q(P) = P'Q + P\cdot Q'$

On a $f_Q = D \circ m_Q$

et $g_Q = m_Q \circ D + m_{Q'}$

donc $f_Q, g_Q \in L(\mathbb{K}[X])$.

Mq $f_Q = g_Q$

On utilise le lemme

Il suffit de mq $\forall n \in \mathbb{N}, f_Q(X^n) = g_Q(X^n)$

Soit $n \in \mathbb{N}$

On note $Q = \sum_{k=0}^{N} a_k X^k$

On a $f_Q(X^n) = (QX^n)'$

$= \left(\sum_{k=0}^{N} a_k X^{k+n}\right)' = \sum_{k=0}^{N} (k+n) a_k X^{(k+n)-1}$

$= \sum_{l=n}^{N+n} l \cdot a_{l-n} \cdot X^{l-1}$

Rq : si $R = \sum_{k=0}^{N} b_k X^k$

alors $R' = \sum_{k=1}^{N} k \cdot b_k X^{k-1}$

On s'autorisera aussi à écrire $R' = \sum_{k=0}^{N} k\, b_k X^{k-1}$

On calcule $g_Q(X^n) = (X^n)' \cdot Q + X^n \cdot Q'$

$$= n X^{n-1} \cdot \sum_{k=0}^{N} a_k X^k + X^n \cdot \sum_{k=0}^{N} k a_k X^{k-1}$$

$$= \sum_{k=0}^{N} n \cdot a_k \cdot X^{k+n-1} + \sum_{k=0}^{N} k a_k X^{k+n-1}$$

$$= \sum_{k=0}^{N} (n+k)\, a_k X^{k+n-1}$$

On retrouve $f_Q(X^n)$

Bilan : $\forall P, Q$, $(PQ)' = P' \cdot Q + P \cdot Q'$

Corollaire : $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$

Alors $(P^n)' = n \cdot P^{n-1} \cdot P'$

démo : on fixe P

On note $\mathcal{P}(n)$: " $(P^n)' = n \cdot P^{n-1} \cdot P'$ " pour $n \in \mathbb{N}$

$\mathcal{P}(0)$: ok $1' = 0$

Hérédité : Soit $n \in \mathbb{N}$ tq $(P^n)' = n \cdot P^{n-1} \cdot P'$

Alors, $(P^{n+1})' = (P^n \cdot P)'$
$= (P^n)' \cdot P + P^n \cdot P'$
$= n P^{n-1} \cdot P' P + P^n \cdot P'$
$= P^n \cdot n \cdot P' + P^n \cdot P'$
$= (n+1) \cdot P^n \cdot P'$

4) On procède de la m̂ façon par linéarité
Fixe P et je relâche Q

On pose $\varphi_P : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$
$Q \longmapsto (Q \circ P)'$

$\psi_P : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]$
$Q \longmapsto (Q' \circ P) \times P'$

1°) $\varphi_P , \psi_P \in \mathcal{L}(\mathbb{K}[X])$

⚠ $Q \longmapsto P \circ Q$ n'est pas linéaire
démo : $(Q_1 + Q_2)^2 \neq Q_1^2 + Q_2^2$
mais $P \mapsto P \circ Q$ est linéaire
car $(P_1 + \lambda P_2) \circ Q = P_1 \circ Q + \lambda P_2 \circ Q$

on note $c_Q : \mathbb{K}[X] \to \mathbb{K}[X]$ est linéaire
$P \mapsto P \circ Q$

On a $\varphi_P = D \circ c_P$
$\psi_P = c_{Q'} \circ D = m_{P'} \circ c_P \circ D$

En effet, $m_{P'} \circ c_P \circ D(Q) = m_{P'}(c_P(D(Q))) = m_{P'}(c_P(Q'))$
$= m_{P'}(Q' \circ P) = (Q' \circ P) \cdot P'$

donc φ_P et ψ_P sont linéaires

Mq $\varphi_P = \psi_P$. Il suffit de Mq $\forall n \in \mathbb{N}$, $\varphi_P(X^n) = \psi_P(X^n)$.
Soit $n \in \mathbb{N}$, on a : $\varphi_P(X^n) = (X^n \circ P)' = (P^n)'$
et $\psi_P(X^n) = [(X^n)' \circ P] \times P' = [(nX^{n-1}) \circ P] \times P' = nP^{n-1} \times P'$
On a bien $(P^n)' = n.P^{n-1}.P'$

4) Dérivation formelle et dérivation usuelle

Prop : Soit $P \in \mathbb{R}[X]$

$$\widetilde{P}' = \widetilde{P'}$$

démo : on dispose de

$$\begin{array}{ccccc} \mathbb{R}[X] & \longrightarrow & \mathcal{E}^{\infty}(\mathbb{R},\mathbb{R}) & \longrightarrow & \mathcal{E}^{\infty}(\mathbb{R},\mathbb{R}) \\ P & \longmapsto & \widetilde{P} & \longmapsto & (\widetilde{P})' \end{array}$$

$$\begin{array}{ccc} \rightarrow \mathbb{R}[X] & \longrightarrow & \mathcal{E}^{\infty}(\mathbb{R},\mathbb{R}) \\ \rightarrow P' & \longmapsto & \widetilde{P'} \end{array}$$

Ces deux appli. sont linéaires.
Il s'agit : $D_{\mathcal{E}^{\infty}(\mathbb{R},\mathbb{R})} \circ \widetilde{\cdot}$

$\widetilde{\cdot} \circ D_{\mathbb{R}[X]}$

Elles coïncident sur $(X^n)_{n\in\mathbb{N}}$
En effet, $\begin{pmatrix} \mathbb{R} \to \mathbb{R} \\ t \mapsto t^n \end{pmatrix}' = \begin{array}{c} \mathbb{R} \to \mathbb{R} \\ t \mapsto n\,t^{n-1} \end{array}$

5) Formule de Taylor polynomiale

Prop : Soit $P \in \mathbb{K}[X]$; $n := \deg P$, $a \in \mathbb{K}$

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

démo :

reformulation : $P = T_{\tilde{P}, \deg P, n}$

Soit $P \in \mathbb{K}[X]$

On note $n := \deg P$

On se place dans $\mathbb{K}_n[X]$

La famille $\left(\frac{(X-a)^k}{k!} \right)_{k \in [\![0, n]\!]}$ est échelonnée et de bonne taille, c'est une base de $\mathbb{K}_n[X]$

Soit donc $(\lambda_0, \lambda_1, \dots, \lambda_n) \in \mathbb{K}^{n+1}$ tq $P = \sum_{k=0}^{n} \lambda_k \cdot P_k$ $(*)$

où $P_k = \frac{(X-a)^k}{k!}$ pour $k \in \mathbb{N}$

Dérivons $(*)$ $P' = \sum_{k=1}^{n} \lambda_k (P_k)'$

$= \sum_{k=1}^{n} \lambda_k P_{k-1}$

Plus généralement :

si $\ell \in [\![0, n]\!]$: $P^{(\ell)} = \sum_{k=\ell}^{n} \lambda_k P_{k-\ell}$ $(**)$

Soit $\ell \in [\![0, n]\!]$, on évalue $(**)$ en a :

$$P^{(\ell)}(a) = \sum_{k=\ell}^{n} \lambda_k P_{k-\ell}(a)$$

Or, $\forall i > 0$, $P_i(a) = \frac{(X-a)^i}{i!}(a) = 0$

et $P_0 = 1 = \frac{(X-a)^0}{0!} = 1$

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

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

6) Caractérisation de la multiplicité

Prop !! $P \in \mathbb{K}[X]$
$\alpha \in \mathbb{K}$
$k \in \mathbb{N}^*$

α est racine de P de multiplicité k $\iff \begin{cases} P(\alpha) = P'(\alpha) = \dots = P^{(k-1)}(\alpha) = 0 \\ P^{(k)}(\alpha) \neq 0 \end{cases}$

démo :

$(\Rightarrow)$ Osq $m_\alpha(P) = k$
On écrit $P = (X-\alpha)^k \cdot Q$
avec $Q(\alpha) \neq 0$

Astuce : on décompose Q dans $\left((X-\alpha)^i\right)_{i\in\mathbb{N}}$

ie on écrit $Q = \sum_{k=0}^{N} b_\ell (X-\alpha)^\ell$

On a : $b_0 = Q(\alpha)$ $\in \mathbb{R}^\times$

On écrit $P = (X-\alpha)^k \cdot Q$
$= \sum_{\ell=0}^{N} b_\ell (X-\alpha)^{k+\ell}$
$= \sum_{i=k}^{N+k} b_{i-\ell} (X-\alpha)^i$
$= 0 + 0(X-\alpha) + 0 \cdot \dfrac{(X-\alpha)^2}{2} + \dots + 0 \cdot \dfrac{(X-\alpha)^{k-1}}{(k-1)!}$
$+ b_0 \cdot k! \dfrac{(X-\alpha)^k}{k!} + \dots + b_N \cdot N! \dfrac{(X-\alpha)^N}{N!}$

On, $P = \sum_{i=0}^{\deg P} P^{(i)}(\alpha) \cdot \frac{(X-\alpha)^i}{i!}$ (Taylor)

Or, la famille $\left(\frac{(X-\alpha)^i}{i!}\right)_{i \in [\![0, \deg P]\!]}$ est libre

donc, en identifiant les coeffs de ces deux CL, on obtient :

$$\begin{cases} P'(\alpha) = P''(\alpha) = \dots = P^{(l-1)}(\alpha) = 0 \\ P^{(l)}(\alpha) = l!\, b_0 \neq 0 \text{ car } b_0 \neq 0 \end{cases}$$

$\Leftarrow$ Osq $P(\alpha) = \dots = P^{(k-1)}(\alpha) = 0$
$P^{(k)}(\alpha) \neq 0$

Mq $m_\alpha(P) = k$

Taylor : $P = 0 + 0 \cdot (X-\alpha) + \dots + 0 \cdot \frac{(X-\alpha)^{k-1}}{(k-1)!}$

$$+ \underbrace{P^{(k)}(\alpha)}_{\neq 0} \cdot \frac{(X-\alpha)^k}{k!} + \lambda_{k+1} \frac{(X-\alpha)^{k+1}}{(k+1)!}$$

$$+ \dots + \lambda_n \cdot \frac{(X-\alpha)^n}{n!}$$

$$P = (X-\alpha)^k \underbrace{\left[\underbrace{\frac{P^{(k)}(\alpha)}{k!}}_{\neq 0} + \sum_{i=1}^{n-k} \lambda_{k+i} (X-\alpha)^i \right]}_{Q}$$

On a $Q(\alpha) = \frac{P^{(k)}(\alpha)}{k!} \neq 0$

donc $m_\alpha(P) = k$

V, Polynômes irréductibles et factorisation

1) Poly irréductible

Déf : Soit $P \in \mathbb{R}[X]$
On dit que P est irréductible dans $\mathbb{K}[X]$ $\overset{\Delta}{\text{ssi}}$

1) P n'est pas constant ie $\deg P \geqslant 1$

2) $\forall Q, R \in \mathbb{K}[X]$, $P = QR \Rightarrow Q$ constant ou R constant

Ex : . X^2+1 n'est pas irréductible dans $\mathbb{C}[X]$
On a $X^2+1 = (X-i)(X+i)$

. X^2+1 est irréductible dans $\mathbb{R}[X]$

démo : Soient $Q, R \overset{\in \mathbb{R}[X]}{}$ tq $X^2+1 = Q \cdot R$
Mq Q ou R est cst.
Absurde : Osq $\deg R, \deg Q \geqslant 1$
Nécessairement, on a $\deg R = \deg Q = 1$
On écrit $Q = aX+b$ avec $a, b \in \mathbb{R}$
On a $Q\left(-\frac{b}{a}\right) = 0$

donc $X^2+1\left(-\frac{b}{a}\right) = Q \cdot R\left(-\frac{b}{a}\right) = 0$

donc $\left(-\frac{b}{a}\right)^2 + 1 = 0$

ie $\left(-\frac{b}{a}\right)^2 = -1$ absurde car $\left(-\frac{b}{a}\right)^2 \geqslant 0$

Fait 1 :
Soit $P \in \mathbb{K}[X]$
alors $\deg P = 1 \Rightarrow P$ irréductible

Fait 2 : $\left.\begin{array}{l} P \in \mathbb{K}[X], \\ \deg P \geq 2 \\ \exists \alpha \in \mathbb{K} : P(\alpha) = 0 \end{array}\right\} \Rightarrow P$ n'est pas irréductible

2) Polynôme scindé

Déf : Soit $P \in \mathbb{K}[X]$ avec $\deg P \geq 1$
On dit que P est scindé dans $\mathbb{K}$ $\overset{\Delta}{\text{ssi}}$

$\exists n \in \mathbb{N}^*, \exists \alpha_1, \dots, \alpha_n \in \mathbb{K}^n, \exists \lambda \in \mathbb{K}$:

$$P = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

Rq : les α_i ne sont pas supposés 2 à 2 $\neq$

Ex : • $X^3 (X-2)^2$ est scindé dans $\mathbb{R}$

• $(X^2 - 1)^8$ est scindé dans $\mathbb{R}$

• $(X^2 + 1)^8$ n'est pas scindé dans $\mathbb{R}$ mais l'est dans $\mathbb{C}$

3) Factorisation dans $\mathbb{C}[X]$

a) Théorème de d'Alembert - Gauss

Th : Soit $P \in \mathbb{C}[X]$ alors

$$\deg P \geq 1 \Rightarrow Z_{\mathbb{C}}(P) \neq \emptyset$$

b) Irréductibles de $\mathbb{C}[X]$

Corollaire :
Les irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1

démo : d'Alembert - Gauss + Fait 1 + Fait 2

c) Décomposition en irréductibles dans $\mathbb{C}[X]$

Idée 💡

$\mathbb{Z}$	$\mathbb{C}[X]$
$\mathcal{P}$ ⟷	$\{(X-\alpha) \mid \alpha \in \mathbb{C}\}$
inversibles de $\mathbb{Z}$ $\mathcal{U}(\mathbb{Z}) = \{\pm 1\}$	inversibles de $\mathbb{C}[X]$ $\mathcal{U}(\mathbb{C}[X]) = \mathbb{C}^*$
$n \neq 0$	$P \neq 0$
$\lvert n \rvert$	$\deg P$
$n = \underbrace{(\pm 1)}_{\in \mathcal{U}(\mathbb{Z})} \prod_{i=1}^{\wedge} p_i^{\alpha_i}$	$P = \underbrace{\lambda}_{\in \mathbb{K}^{\times} = \mathcal{U}(\mathbb{C}[X])} \prod_{i=1}^{\wedge} (X-\alpha_i)^{m_i}$
$v_p(n)$	$m_\alpha(P)$

Théorème :

Soit $P \in \mathbb{C}[X]$ non constant

a) Alors $\exists\, r \in \mathbb{N}^*$
$\exists\, \alpha_1, \ldots, \alpha_r \in \mathbb{C}$ 2 à 2 $\neq$
$\exists\, m_1, \ldots, m_r \in \mathbb{N}^*$
$\exists\, \lambda \in \mathbb{C}^*$

$$P = \lambda \cdot \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$$

b) Cette écriture est unique à l'ordre près des facteurs

Démo : a) facto. simultanée avec $Z_{\mathbb{C}}(P)$ + d'Alembert-Gauss

b) $\{\alpha_i\} = Z_{\mathbb{C}}(P)$ $\quad m_i = m_{\alpha_i}(P)$

4) Factorisation dans $\mathbb{R}[X]$

a) Rappel : racines complexes de polynômes réels

Lemme !!! : $\alpha \in \mathbb{C}$, $P \in \mathbb{R}[X]$

Alors . $P(\alpha) = 0 \Rightarrow P(\bar{\alpha}) = 0$

. $m_\alpha(P) = m_{\bar{\alpha}}(P)$: zéro

b) Irréductibles dans $\mathbb{R}[X]$

Théorème : Les irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1
- les polynômes aX^2+bX+c avec $b^2-4ac<0$

démo :

deg 1 → ok c'est irréductible

deg 2 et $\Delta<0$ → c'est irr car $\emptyset$ racine

ce sont les seuls

Soit $P\in\mathbb{R}[X]$ irr. de degré ≥ 2

alors : soit $\alpha\in\mathbb{C}$ tq $P(\alpha)=0$

d'après D'Alembert-Gauss :

on a $\alpha\notin\mathbb{R}$

on a $P(\bar{\alpha})=0$

donc $\underbrace{(X-\alpha)(X-\bar{\alpha})}_{\in\mathbb{R}[X]}$ divise P dans $\mathbb{C}[X]$

Écrivons la DE de P par $(X-\alpha)(X-\bar{\alpha})$ dans $\mathbb{R}[X]$

noté $\Pi\in\mathbb{R}[X]$

On a $P=\Pi\cdot Q+R$ avec $\deg R\leq 1$ (*)

C'est la DE de P par Π dans $\mathbb{R}[X]$

La relation (*) est encore vrai dans $\mathbb{C}[X]$

$$\begin{cases} P=\Pi\cdot Q+R \\ \deg R\leq 1 \end{cases} \rightarrow \text{sont aussi dans } \mathbb{C}[X]$$

Or $\Pi\mid P$ dans $\mathbb{C}[X]$

car $P(\alpha)=P(\bar{\alpha})=0$ par facto. simultanée

donc $R = 0$
donc $\Pi \mid P$ dans $\mathbb{R}[X]$

Or P est irréductible donc $\exists \lambda \in \mathbb{R}^* : P = \lambda \cdot \Pi$

donc $\deg P = 2$ et aussi $\Delta_P < 0$

c) Décomposition en irréductibles dans $\mathbb{R}[X]$

Théorème

Soit $P \in \mathbb{R}[X]$ non constant.
Alors P s'écrit de façon unique à l'ordre près :

$$P = \lambda \prod_{i=1}^{s} (X - \alpha_i)^{m_i} \cdot \prod_{j=1}^{t} (X^2 + b_j X + c_j)^{m_j}$$

où $\alpha_i \in \mathbb{R}$ 2 à 2 $\neq$
$m_i \in \mathbb{N}^*$
où $(b_j, c_j) \in \mathbb{R}^2$ 2 à 2 distincts tq $b_j^2 - 4c_j < 0$
$m_j \in \mathbb{N}^*$