

Démonstration kholle 20

I Division euclidienne

Propriété :

Soit $(A, B) \in (\mathbb{K}[X])^2$ avec $B \neq 0$

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

Démonstration :

Unicité :

Si $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$

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

$$B(Q_1 - Q_2) = R_2 - R_1$$

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

$$\text{donc } \deg(B) + \deg(Q_1 - Q_2) < \deg(B)$$

$$\text{or } \deg(B) \in \mathbb{N} \text{ car } B \neq 0 \text{ donc } \deg(Q_1 - Q_2) < 0$$

$$\text{donc } Q_1 - Q_2 = 0 \text{ donc } Q_1 = Q_2 \text{ et } R_1 = R_2$$

Existence :

$$Q, R \leftarrow 0, A$$

Tant que $\deg(R) \geq \deg(B)$:

Soit sX^d le monome tel que $sX^d B$ ont le même terme de plus haut degré que R :

$$Q, R \leftarrow Q + sX^d, R - sX^d B$$

Renvoyer Q, R

Notons Q_k et R_k les valeurs de Q et R après k itérations

Terminaison : $\deg(R_k)$ décroît strictement dans $\mathbb{N} \cup \{-\infty\}$

Correction Montrons que qu'après chaque itérations on a bien $A = BQ_k + R_k$

Initialisation : $k = 0, Q_0 = 0, R_0 = A$

$$A = B \times 0 + A$$

Hérédité Soit $k \in \mathbb{N}^*$ tel que la propriété soit vraie au rang k-1. Si on effectue une k-ième itération :

$$\deg(R_{k-1}) \geq \deg(B)$$

prenons $d = \deg(R_{k-1}) - \deg(B) \in \mathbb{N}$ et $s = \frac{\text{dom}(R_{k-1})}{\text{dom}(B)}$ a un sens car $\text{dom}(B) \in \mathbb{K}^*$

$$\text{Alors : } Q_k = Q_{k-1} + sX^d \text{ et } R_k = R_{k-1} - sX^d B$$

$$\text{donc } BQ_k + R_k = BQ_{k-1} + R_{k-1} = A$$

Conclusion : Soit k_0 le nombre total d'itérations, on renvoie (Q_{k_0}, R_{k_0})

Par principe de récurrence : $A = BQ_{k_0} + R_{k_0}$

Puisque l'on effectue plus d'itération supplémentaire $\deg(R_{k_0}) < \deg(B)$

II Factorisation d'une racine; un polynôme n'a pas plus de racines distincts que son degré

Propriété :

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

1) Le reste de la division euclidienne de P par $X - \alpha$ est $P(\alpha)$

2) $P(\alpha) = 0 \iff (X - \alpha) | P$

Démonstration :

$$1) P = (X - \alpha)Q + R$$

Avec $Q \in \mathbb{K}[X], R \in \mathbb{K}[X]$

et $\deg(R) < \deg(X - \alpha) = 1$ donc R est constant

substitutions α à X :

$$P(\alpha) = R(\alpha) = R \text{ car } R \text{ constante}$$

$$2) (X - \alpha) | P \iff R = 0$$

Propriété :

Soit $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$. Alors P possède au plus n racines.

Démonstration : récurrence sur n

Initialisation : $n=0$, $P \in \mathbb{K}^*$ aucune racine .

Hérédité : Soit $n \in \mathbb{N}^*$ tel que la propriété est vraie au rang $n-1$

Soit $P \in \mathbb{K}[X]$ de degré n :

- si P n'a pas de racine : il n'en a pas plus de n

- si P a au moins une racine $c \in \mathbb{K}$, soit $Q \in \mathbb{K}[X]$ tel que :

$$\forall x \in \mathbb{K}, P(x) = (x - c)Q(x)$$

$$\text{alors } \deg(Q) = n - 1$$

Q a donc au plus $n-1$ racines

On a pour $x \in \mathbb{K}$:

$$P(x) = 0 \iff (x - c) \text{ ou } Q(x) = 0$$

P possède au plus une racine de plus que Q donc au plus n au total

III Factorisation simultanée de plusieurs racines distinctes ; cas où il y a autant de racines que le degré (polynôme scindé simple)

Propriété:

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

Soit $(\alpha_1, \dots, \alpha_r)$ des racines deux à deux distinctes de P . Alors :

$$(X - \alpha_1) \dots (X - \alpha_r) | P$$

c'est-à-dire: $\exists Q \in \mathbb{K}[X], P = (X - \alpha_1) \dots (X - \alpha_r)Q$

Démonstration : soit la division euclidienne :

$$P = (X - \alpha_1) \dots (X - \alpha_r)Q + R \text{ avec } (Q, R) \in \mathbb{K}[X]$$

$$\text{et } \deg(R) < \deg((X - \alpha_1) \dots (X - \alpha_r)) = r$$

Pour $k \in \llbracket 1, r \rrbracket$:

$$R(\alpha_k) = P(\alpha_k) = 0 \text{ donc } R \text{ possède au moins } r \text{ racines or } \deg(R) < r \text{ donc } R = 0$$

Corollaire :

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

On suppose qu'il possède d racines distinctes 2 à 2 $\alpha_1, \dots, \alpha_d$ alors :

$$P = \text{dom}(P) \prod_{k=1}^d (X - \alpha_k)$$

Démonstration : Comme les racines sont 2 à 2 distincts :

$$\exists Q \in \mathbb{K}[X], P = (X - \alpha_1) \dots (X - \alpha_d)Q$$

$$\text{de degré } d = \underbrace{1 + \dots + 1}_{d \text{ termes}} + \deg(Q) \quad \deg(Q) = 0 \text{ donc } Q = \lambda \in \mathbb{K}^*$$

$$\text{coefficient dominant : } \text{dom}(P) = \lambda$$

IV Interpolation de Lagrange

Propriété :

Soit $n \in \mathbb{N}^*$, et $(a_1, \dots, a_n) \in \mathbb{K}^n$ deux à deux distincts.

La famille des polynômes associée à (a_1, \dots, a_n) est (L_1, \dots, L_n) où :

$$L_k = \prod_{i=1, i \neq k}^n \frac{X - a_i}{a_k - a_i}$$

$$1) \forall k \in \llbracket 1, n \rrbracket, \deg(L_k) = n - 1$$

$$2) \forall (k, j) \in \llbracket 1, n \rrbracket^2, L_k(a_j) = \delta_{k,j}$$

3) (L_1, \dots, L_n) est une base de $\mathbb{K}_{n-1}[X]$ Plus précisément :

$$\forall P \in \mathbb{K}_{n-1}[X], P = \sum_{k=1}^n P(a_k) L_k$$

Démonstration :

1) Il y a $n-1$ facteur de degré 1

$$2) L_k(a_j) = \prod_{i=1, i \neq k}^n \frac{a_j - a_i}{a_k - a_i}$$

si $j \neq k$, i peut prendre la valeur j et donne un facteur nul $L_k(a_j) = 0$

si $j = k$: tous les facteurs valent 1 $L_k(a_j) = 1$

3) C'est bien une famille de $\mathbb{K}_{n-1}[X]$

Montrons que tout $P \in \mathbb{K}_{n-1}[X]$ est combinaison linéaire de (L_1, \dots, L_n) de façon unique

Soit $P \in \mathbb{K}_{n-1}[X]$

analyse : si $P = \sum_{k=1}^n \lambda_k L_k$ avec $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$

Pour $j \in [[1, n]]$:

$$P(a_j) = \sum_{k=1}^n \lambda_k L_k(a_j)$$

$$P(a_j) = \sum_{k=1}^n \lambda_k \delta_{k,j}$$

$$P(a_j) = \lambda_j$$

unicité des candidats $(\lambda_1, \dots, \lambda_n)$

Synthèse : Pour $Q = P - \sum_{k=1}^n P(\alpha_k) L_k$

d'une part : $P, L_1, \dots, L_n \in \mathbb{K}_{n-1}[X]$ donc $Q \in \mathbb{K}_{n-1}[X]$

d'autre part : pour $j \in [[1, n]]$:

$$Q(a_j) = P(a_j) - \underbrace{\sum_{k=1}^n P(a_k) L_k(a_j)}_{=P(a_j)}$$

$$Q(a_j) = 0$$

Ainsi $\deg(Q) < n$ et Q possède au moins n racines distinctes donc $Q = 0$, $P = \sum_{k=1}^n P(\alpha_k) L_k$

V Dérivée de PQ

Propriété :

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

Démonstration :

coeff de X^k dans P : a_k

coeff de X^k dans Q : b_k

coeff de X^k dans PQ : $\sum_{j=0}^k a_j b_{k-j}$

coeff de X^k dans $(PQ)'$: $(k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j}$

coeff de X^k dans P' : $(k+1)a_{k+1}$

coeff de X^k dans Q' : $(k+1)b_{k+1}$

coeff de X^k dans $P'Q$: $\sum_{j=0}^k (j+1)a_{j+1}b_{k-j}$

coeff de X^k dans PQ' : $\sum_{j=0}^k a_j(k-j+1)b_{k-j+1} = \sum_{j=0}^{k+1} a_j(k-j+1)b_{k-j+1}$

Pour $P'Q$:

$$\sum_{j=0}^k (j+1)a_{j+1}b_{k-j} = \sum_{j=1}^{k+1} j a_j b_{k+1-j} = \sum_{j=0}^{k+1} j a_j b_{k+1-j}$$

coeff de X^k dans $P'Q + PQ'$: $\sum_{j=0}^{k+1} (j+k-j+1)a_j b_{k+1-j} = (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j}$

VI Formule de Taylor

Propriété :

Soit $a \in \mathbb{K}$:

$$\forall n \in \mathbb{N}, \forall P \in \mathbb{K}_n[X], P = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Démonstration :

Récurrence sur n :

Initialisation : Soit $P \in \mathbb{K}_0[X] = \mathbb{K}$

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

Hérédité Soit $n \in \mathbb{N}$ tel que la formule soit vraie au rang n :

Soit $P \in \mathbb{K}_{n+1}[X]$

$P' \in \mathbb{K}_n[X]$ donc par hypothèse de récurrence :

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

Posons :

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

Alors :

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

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

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

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

$$Q' = 0 \text{ donc } Q \in \mathbb{K}$$

$$\text{or } Q(a) = P(a) - \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!} 0^k$$

$$Q(a) = P(a) - P(a) = 0 \text{ donc } Q = 0 \text{ l'hypothèse est vérifiée au rang } n+1$$

VII Caractérisation différentielle de la multiplicité

Propriété :

Soit $P \in \mathbb{K}[X] \setminus \{0\}$, $\alpha \in \mathbb{K}$, $n \in \mathbb{N}$ Les propositions suivantes sont équivalentes :

1) α est racine de P de multiplicité m

2) $P^{(k)}(\alpha) = 0$ pour $k < m$ et $P^{(m)}(\alpha) \neq 0$

Démonstration :

1 \Rightarrow 2 : Soit $Q \in \mathbb{K}[X]$ tel que :

$$P = (X - \alpha)^m Q \text{ et } Q(\alpha) \neq 0$$

Soit $k \in [[0, m]]$, par la formule de Leibniz :

$$P^{(k)} = \sum_{j=0}^k \binom{k}{j} ((X - \alpha)^m)^{(k-j)} Q^{(j)}$$

$$P^{(k)} = \sum_{j=0}^k \binom{k}{j} \frac{m!}{(m-k+j)!} (X - \alpha)^{m-k+j} Q^{(j)} \text{ car } (k-j) \in [[0, k]] \subset [[0, m]] \text{ donc } m - (k-j) = m - k + j \in \mathbb{N}$$

$$\text{donc } P^{(k)} = \sum_{j=0}^k \binom{k}{j} \frac{m!}{(m-k+j)!} 0^{m-k+j} Q^{(j)}(\alpha)$$

si $k < m$: $k-j$ varie entre 0 et k donc :

$$\forall j \in [[0, k]], m - (k-j) \in \mathbb{N}^*$$

$$P^{(k)}(\alpha) = 0$$

si $k = m$:

$$P^{(m)}(\alpha) = \sum_{j=0}^m \binom{m}{j} \frac{m!}{j!} 0^j Q^{(j)}(\alpha)$$

$$P^{(m)}(\alpha) = m! Q(\alpha) \neq 0 \text{ car } Q(\alpha) \neq 0$$

2 \Rightarrow 1 on a : $P^{(k)}(\alpha) = 0$ si $k < m$ et $P^{(m)}(\alpha) \neq 0$

Formule de Taylor $d = \deg(P)$:

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

on a $0 \leq m \leq d$ car si $m > d$, $P^{(m)} = 0$ donc $P^{(m)}(\alpha) = 0$

On a donc :

$$P = \sum_{k=m}^d \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$$

$$P = (X - \alpha)^m \underbrace{\sum_{k=m}^d \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^{k-m}}_{Q \in \mathbb{K}[X]}$$

enfin :

$$Q(\alpha) = \sum_{k=m}^d \frac{P^{(k)}(\alpha)}{k!} 0^{k-m}$$

$$Q(\alpha) = \frac{P^{(m)}(\alpha)}{m!} \neq 0$$