

Polynômes

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$

I. Généralités

1) Définitions et exemples

Def 1:

On appelle polynôme à coefficients dans $\mathbb{K}$ toute expression de la forme

$$P(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

où $n \in \mathbb{N}$, $a_0, \dots, a_n \in \mathbb{K}$

Convention : $x^0 = 1$

Vocabulaire et notation :

1) x : l'indéterminée

2) $a_0, \dots, a_n$: les coefficients de P .

3) Le polynôme $P(x)$ se note P

4) i) Si $\mathbb{K} = \mathbb{R}$, le polynôme $P(x)$ est dit à coeff réels.

ii) Si $\mathbb{K} = \mathbb{C}$: $P(x)$ est dit à coeff complexes

5) $\mathbb{K}[x]$ désignera l'ensemble des polynômes à coeff ds $\mathbb{K}$.

Exemples: 1) $x^2 + x - 1 \in \mathbb{R}[x]$ et $\in \mathbb{C}[x]$

2) $(2x^3 + (1+i)x^2 + x) \in \mathbb{C}[x]$ et $\notin \mathbb{R}[x]$

Déf 2: Polynôme nul

Un polynôme est dit **nul** si et si tous ses coeff sont nuls.

NB: Soit $P(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{K}[x]$

1) $P(x) = 0 \Leftrightarrow (\forall 0 \leq i \leq n, a_i = 0)$

2) $P(x) \neq 0 \Leftrightarrow (\exists 0 \leq i \leq n, a_i \neq 0)$

Déf 3: (degré)

Soit $n \in \mathbb{N}$.

Soit $P(x) = a_0 + a_1x + \dots + a_nx^n$

Supp $P(x) \neq 0$.

Si $a_n \neq 0$, on dit que l'entier n est le **degré** de $P(x)$.

Notation: $\deg(P)$ ou $d^o(P)$

Convention: $\deg(0) = -\infty$

NB:

1) $\forall P \in \mathbb{K}[x] / \{0\}, \deg(P) \in \mathbb{N}$.

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

3) $\forall P \in \mathbb{K}[x], \deg(P) \in \mathbb{N} \cup \{-\infty\}$

Prop 1:

1) $\deg(P) = -\infty \Leftrightarrow P = 0$ cste non nul

2) $\deg(P) = 0 \Leftrightarrow (\exists c \in \mathbb{K}^* / P(x) = c)$

3) $\deg(P) = 1 \Leftrightarrow (\exists (a, b) \in \mathbb{K} \times \mathbb{K}^* / P(x) = a + bx)$

4) $\deg(P) = 2 \Leftrightarrow \left(\begin{array}{l} \exists (a, b, c) \in \mathbb{K} \times \mathbb{K} \times \mathbb{K}^* \text{ tel que} \\ P(x) = a + bx + cx^2 \end{array} \right)$

5) Soit $n \in \mathbb{N}$
 $\deg(P) = n \Leftrightarrow \left(\begin{array}{l} \exists (a_0, \dots, a_n) \in \mathbb{K}^{n+1} \text{ avec } a_n \neq 0 \text{ tq} \\ P(x) = \sum_{i=0}^n a_i x^i \end{array} \right)$

Réflexe 2 :

1) $\deg(P) \leq 0 \Leftrightarrow (\exists c \in \mathbb{K} / P(x) = c)$

2) $\deg(P) \leq 1 \Leftrightarrow (\exists (a, b) \in \mathbb{K}^2 / P(x) = a + bx)$

3) $\deg(P) \leq 2 \Leftrightarrow (\exists (a, b, c) \in \mathbb{K}^3 / P(x) = a + bx + cx^2)$

4) $\deg(P) \leq n \Leftrightarrow \exists (a_0, \dots, a_n) \in \mathbb{K}^{n+1} / P(x) = \sum_{k=0}^n a_k x^k$

R/R : Supp $\deg(P) = n \in \mathbb{N}$ tq

$P(x) = a_0 + a_1 x + \dots + a_n x^n$ (où $a_n \neq 0$)

On écrit : $P(x) = \sum_{k=0}^{+\infty} a_k x^k$

Eneffet :

$\forall k \geq n+1, a_k = 0$

NB : Soient $P(x) = \sum_{k=0}^{+\infty} a_k x^k$ et $Q(x) = \sum_{k=0}^{+\infty} b_k x^k$

1) $P(x) = 0 \Leftrightarrow \forall k \in \mathbb{N}, a_k = 0$

2) $P(x) = Q(x) \Leftrightarrow \forall k \in \mathbb{N}, a_k = b_k$

Vocabulaire 1 :

Supp $\deg(P) = n$ et $P(x) = \sum_{k=0}^n a_k x^k$
 où $a_n \neq 0$

1) a_n s'appelle **coeff dominant** de $P(x)$

2) On le note **cd(P)**

3) a_k = le coeff en x^k de $P(x)$

Vocabulaire 2 :

Si $\text{cd}(P) = 1$, on dit que $P(x)$ est un polynôme unitaire

Reflexe : Si $P \neq 0$ alors $\frac{P(x)}{\text{cd}(P)}$ est unitaire

Notation : Soit $n \in \mathbb{N}$.

$\mathbb{K}_n[x]$: l'ensemble des polynômes de degré $\leq n$

⟨ Attention : non pas $= n$ ⟩

Ex

1) $x^2 - 3x + 1 \in \mathbb{R}_2[x]$ et $\in \mathbb{Q}_2[x]$.

2) $x^2 - 3x + 1 \in \mathbb{K}_{2021}[x]$.

Prop 4 :

1) $P \in \mathbb{K}_0[x] \Leftrightarrow \exists c \in \mathbb{K}, P(x) = c$

2) $P \in \mathbb{K}_1[x] \Leftrightarrow \exists (a, b) \in \mathbb{K}^2, P(x) = a + bx$

3) $P \in \mathbb{K}_2[x] \Leftrightarrow \exists (a, b, c) \in \mathbb{K}^3, P(x) = a + bx + cx^2$

4) $P \in \mathbb{K}_n[x] \Leftrightarrow \left(\begin{array}{l} \exists (a_0, \dots, a_n) \in \mathbb{K}^{n+1} \text{ tel que } \\ P(x) = \sum_{k=0}^n a_k x^k \end{array} \right)$

NB : $\forall n \in \mathbb{N}, 0 \in \mathbb{K}_n[x]$.

en effet $\deg(0) = -\infty \leq n$

2) Opérations sur les polynômes.

a) Combinaisons linéaires de deux polynômes.

Déf : Soit $P(x) = \sum_{k=0}^{+\infty} a_k x^k$ et $Q(x) = \sum_{k=0}^{+\infty} b_k x^k$
deux polynômes de $\mathbb{K}[X]$.

1) Somme : $P(x) + Q(x) = \sum_{k=0}^{+\infty} (a_k + b_k) x^k$

2) Multiplication par un scalaire $\alpha \in \mathbb{K}$:
 $\alpha P(x) = \sum_{k=0}^{+\infty} \alpha a_k x^k$

3) Combinaison linéaire
 $\forall \alpha, \beta \in \mathbb{K}, \alpha P(x) + \beta Q(x) = \sum_{k=0}^{+\infty} (\alpha a_k + \beta b_k) x^k$

3) Produit de deux polynômes.

Définitions :

Soient $P(x) = \sum_{k=0}^{+\infty} a_k x^k$ et $Q(x) = \sum_{k=0}^{+\infty} b_k x^k$

$P(x) \cdot Q(x) = \sum_{k=0}^{+\infty} c_k x^k$

où $c_k = \sum_{i=0}^k a_i b_{k-i}, \forall k \in \mathbb{N}$

NB :

$c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i+j=k} a_i b_j = \sum_{i=0}^k a_{k-i} b_i$

Exemple illustratif :

$P(x) = a_0 + a_1 x + a_2 x^2, Q(x) = b_0 + b_1 x$

1) Avec le lycée. On a :

$P(x)Q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_1 b_1 + a_2 b_0)x^2 + a_2 b_1 x^3$

2) Retrouvons ceci avec déf :

On a $P(x) = \sum_{k=0}^{+\infty} a_k x^k$ avec $a_k = 0 (\forall k \geq 3)$

$Q(x) = \sum_{k=0}^{+\infty} b_k x^k$ avec $b_k = 0 (\forall k \geq 2)$

$$P(x)Q(x) = \sum_{k=0}^{+\infty} C_k x^k \quad \text{où} \quad C_k = \sum_{i=0}^k a_i b_{k-i}$$

↑ ↑
somme = k

$$C_0 = a_0 b_0 ; \quad C_1 = a_0 b_1 + a_1 b_0$$

$$C_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = a_1 b_1 + a_2 b_0$$

$$C_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = a_2 b_1$$

$$C_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 0$$

¶c: $P(x)Q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_1 b_1 + a_2 b_0)x^2 + a_2 b_1 x^3$
On retrouve le m résultat.

Ex d'appli:

Via le bin de Newton et en considérant le coeff en x^p
de: $(x+1)^{m+n} = (x+1)^m \cdot (x+1)^n$

¶que: $C_{m+n}^p = \sum_{k=0}^p C_n^k C_m^{p-k}$

3) Propriétés du degré:

Prop 1:

1) $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$

2) Si $\deg(P) \neq \deg(Q)$ alors

$$\deg(P+Q) = \max(\deg(P), \deg(Q))$$

Ex: $P(x) = 2 + x + x^2$; $Q(x) = 3 + x + 2x^2$
 $R(x) = 2 + 3x - x^2$; $T(x) = 2 + 3x + x^2 - x^3$

$$\underline{1)} \deg(P+Q) \leq \max(\deg(P), \deg(Q)).$$

$$\underline{2)} \deg(P+R) \leq \max(\deg(P), \deg(R))$$

$$\underline{3)} \deg(P+T) \leq \max(\deg(P), \deg(T)).$$

Corollaire 2 $n \in \mathbb{N}$.

$$\underline{1)} \left(\begin{array}{l} \deg(P) \leq n \\ \deg(Q) \leq n \end{array} \right) \Rightarrow d^0(P+Q) \leq n$$

$$\underline{2)} \forall P, Q \in K_n[X], \forall \alpha, \beta \in K, (\alpha P + \beta Q) \in K_n[X].$$

Prop 3: Soient P et $Q \in K[X]$. On a:

$$\deg(P \cdot Q) = \deg(P) + \deg(Q)$$

Conventions:

$$\underline{1)} (\forall n \in \mathbb{N}, -\infty \leq n) \text{ et } (-\infty \leq -\infty)$$

$$\underline{2)} (-\infty) + (-\infty) = -\infty ; (\forall n \in \mathbb{N}, -\infty + n = -\infty)$$

Démonstration:

$$\underline{1)} \text{ Si } (P=0 \text{ ou } Q=0)$$

$$\text{l'égalité est vraie: } d^0(P \cdot Q) = d^0(P) + d^0(Q) = -\infty$$

Vu la convention.

$$\underline{2)} \text{ Si } (P \neq 0 \text{ et } Q \neq 0).$$

$$\text{on a } d^0(P) = r \in \mathbb{N}, d^0(Q) = s \in \mathbb{N}.$$

On a:

$$P(x) = \sum_{k=0}^{+\infty} a_k x^k \quad \text{ou} \quad \begin{cases} a_r \neq 0 \\ \forall k \geq r+1, a_k = 0 \end{cases}$$

$$Q(X) = \sum_{k=0}^{+\infty} b_k X^k, \text{ où } \begin{cases} b_0 \neq 0 \\ \forall k \geq r+1, b_k = 0 \end{cases}$$

On veut montrer que $d^o(P(X)Q(X)) = d^o(P) + d^o(Q) = r + s$

Posons $P(X)Q(X) = \sum_{n=0}^{+\infty} c_n X^n$ où $c_n = \sum_{k=0}^n a_k b_{n-k}$.

Il s'agit de montrer que.

$$\begin{cases} a) c_{r+s} \neq 0 \\ b) \forall n \geq r+s+1, c_n = 0 \end{cases}$$

a) On montrera que $c_{r+s} = a_r b_s \neq 0$.

$$\begin{aligned} c_{r+s} &= \sum_{k=0}^{r+s} a_k b_{r+s-k} \\ &= \sum_{k=r+1}^{r+s} a_k b_{r+s-k} + \sum_{k=0}^r a_k b_{r+s-k} \\ &= \sum_{k=0}^r a_k b_{r+s-k} \quad (\text{car } \forall k \geq r+1, a_k = 0) \\ &= \sum_{k=0}^{r-1} a_k b_{r+s-k} + a_r b_s \end{aligned}$$

$$\text{Or: } r+s-k \geq s+1 \Leftrightarrow k \leq r-1$$

Ainsi $c_{r+s} = a_r b_s \neq 0$ CQFD

b) Soit $n \geq r+s+1$ Mg $c_n = 0$

$$c_n = \sum_{k=0}^n a_k b_{n-k}$$

$$\forall k \geq r+1, a_k = 0$$

$$= \sum_{k=r+1}^n a_k b_{n-k} + \sum_{k=0}^r a_k b_{n-k}$$

$\swarrow \rightarrow = 0$ $\swarrow \rightarrow = 0$

Car: $k \leq r \Rightarrow n-k \geq n-r \geq r+1$

$$n \geq r+s+1$$

$$\forall k \geq r+1, b_k = 0$$

Ainsi: $C_n = 0$ $\square$

Corollaire 4

Soient P et $Q \in K[X]$ on a:

$$PQ=0 \Leftrightarrow (P=0 \text{ ou } Q=0)$$

Demo

$$PQ=0 \Leftrightarrow \deg(PQ) = -\infty$$

$$\Leftrightarrow \deg(P) + \deg(Q) = -\infty$$

$$\Leftrightarrow \deg(P) = -\infty \text{ ou } \deg(Q) = -\infty$$

$$\Leftrightarrow P=0 \text{ ou } Q=0$$

$\square$

4.1 Autres propriétés :

Prop 1 : $\alpha \in \mathbb{K} ; P, Q, R \in \mathbb{K}[X]$

1) $P + Q = Q + P$ et $P \times Q = Q \times P$

2) $P + 0 = P$ et $P \times 1 = P$

3) $(P + Q) + R = P + (Q + R)$

4) $(P \times Q) \times R = P \times (Q \times R)$

5) $P + (-P) = 0$

6) $P \times (Q + R) = P \times Q + P \times R$

7) $(\alpha \cdot P) \times Q = P \times (\alpha \cdot Q) = \alpha \cdot (P \times Q)$

Prop 2 : (Binôme de Newton)

Soient $n \in \mathbb{N} ; P, Q \in \mathbb{K}[X]$ on a :

$$(P + Q)^n = \sum_{k=0}^n C_n^k P^k Q^{n-k}$$

Demo : Pareille à celle des complexes.

NB : On a aussi l'égalité de Bernouilli :

$$P^n - Q^n = (P - Q) \cdot \sum_{i=0}^{n-1} P^i Q^{n-1-i}$$

Prop 3 :



- 1) $(\mathbb{K}[X], +)$ est un **groupe commutatif**.
- 2) $(\mathbb{K}[X], +, \cdot)$ est un **anneau commutatif**.
- 3) $(\mathbb{K}[X], +, \cdot)$ est un anneau **intègre**.

51 Fonction polynomiale

Def : Soit $P(x) = \sum_{k=0}^n a_k x^k \in \mathbb{K}[X]$.

La **fonction polynomiale** associée à P est notée $\tilde{P}$ et est définie de $\mathbb{K}$ vers $\mathbb{K}$ par :

$$\begin{aligned} \tilde{P} : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\longmapsto \tilde{P}(x) = \sum_{k=0}^n a_k x^k \end{aligned}$$

NB₁ :

1) $\tilde{P}$ se lit " **$\tilde{P}$ tilde**"

2) Si $P(X) = 2X + 1$

" $P(1)$ " n'est à présent pas défini par contre $\tilde{P}(1) = 3$

NB₂ : Dorénavant, on confondra polynôme P avec sa fonction polynomiale $\tilde{P}$.

Ainsi pour $\alpha \in \mathbb{K}$, on écrira $P(\alpha)$ pour désigner $\tilde{P}(\alpha)$.

Par exemple : soit $n \in \mathbb{N}^*$. Posons $P(x) = x^n - 1$
 $\forall k \in \mathbb{Z}, P(e^{\frac{2k\pi i}{n}}) = 0$

6) Dérivées successives d'un polynôme.

Déf 1 : Soit $P = \sum_{k=0}^{+\infty} a_k x^k \in \mathbb{K}[X]$.

Le polynôme dérivé de P est

$$P'(x) = \sum_{k=1}^{+\infty} k a_k x^{k-1}$$

NB : On a aussi :

$$P'(x) = \sum_{k=0}^{+\infty} (k+1) a_{k+1} x^k$$

Exemples express :

P	P'	$\deg(P)$	$\deg(P')$
$2 + 3x^2$	$6x$	2	1
2	0	0	$-\infty$
0	0	$-\infty$	$-\infty$

Prop 2 :

$\deg(P') = \deg(P) - 1$ si P n'est pas constant.

NB :

Si $P \in \mathbb{K}_0[X]$ (ie P polynôme constant)

$$d^0(P') = -\infty$$

Def: (Dérivées successives d'un polynôme)

Elles sont définies comme pour les fonctions. $P^{(0)} = P$

$$\forall n \in \mathbb{N}, (P^{(n)})' = P^{(n+1)}$$

Prop 4: Soient P et $Q \in \mathbb{K}[X]$, on a:

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

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

3) $\forall \lambda \in \mathbb{K}, (\lambda P)' = \lambda P'$

4) En général:

$$\left(\sum_{i=1}^n \lambda_i P_i \right)^{(k)} = \sum_{i=1}^n \lambda_i P_i^{(k)}$$

Prop 5: Soient $n \in \mathbb{N}, P, Q \in \mathbb{K}[X]$.

$$(PQ)^{(n)} = \sum_{k=0}^n C_n^k P^{(k)} Q^{(n-k)} \quad (\text{Formule de Leibniz})$$

NB: On a aussi

1) $(PQ)^{(n)} = \sum_{k=0}^n C_n^k P^{(n-k)} Q^{(k)}$

2) $(PQ)^{(n)} = \sum_{i+j=n} C_n^i P^{(i)} Q^{(j)}$

Prop 6:

1) $\forall n \in \mathbb{N}, \forall 0 \leq k \leq n$ on a:

$$(x^n)^{(k)} = n \dots (n-k+1) x^{n-k}$$

$$(x^n)^{(k)} = \frac{n!}{(n-k)!} x^{n-k}$$

2) $(x^n)^{(n)} = n!$

3) $\forall k > n, (x^n)^{(k)} = 0$

NB: Il faut savoir retrouver $(x^n)^{(k)} = \dots$

Prop 7: Soient $n \in \mathbb{N}, 0 \leq k \leq n$ et $a \in \mathbb{K}$ on a:

1) $((x+a)^n)^{(k)} = \frac{n!}{(n-k)!} (x+a)^{n-k}$

2) $((a-x)^n)^{(k)} = (-1)^k \frac{n!}{(n-k)!} (a-x)^{n-k}$

3) $(a+bx)^n)^{(k)} = b^k \frac{n!}{(n-k)!} (a+bx)^{n-k}$

Coroll 8: Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$.

1) $P(x) = a_0 + \dots + a_n x^n \Rightarrow P^{(n)}(x) = a_n \cdot n!$

2) $\deg(P) \leq n \Rightarrow (\forall k \geq n+1, P^{(k)} = 0)$

Prop 9 :

Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$.

Les assertions suivantes sont équivalentes :

1 $P^{(n+1)} = 0$

2 $\exists a_0, \dots, a_n \in \mathbb{K}^{n+1}, P = a_0 + \dots + a_n X^n$

3 $P \in \mathbb{K}_n[X]$.

II Arithmétique dans $\mathbb{K}[X]$.

1) Divisibilité

Def 1 : Soient A et $B \in \mathbb{K}[X]$.

On dit que A **divise** B si et si

$\exists C \in \mathbb{K}[X] ; B = AC$

Notation A/B .

Vocab : Supp que A/B .

1 B est un **multiple** de A .

2 A est un **diviseur** de B .

Exemples immédiats.

1) $(x-1) / (x^2-1)$ car $(x^2-1) = (x-1) \cdot (x+1)$

2) Dans $\mathbb{R}[X]$:

1, 2020, (x^2+1) sont des diviseurs de (x^2+1) .

3) Dans $\mathbb{C}[X]$

3 (x^2+1) , $(x+i)$ et $(x-i)$ divisent (x^2+1) .

4) Dans $\mathbb{R}[X]$ Les polynômes suivants sont des diviseurs de (x^n-1) : $(x-1)$ et $(1+x+\dots+x^{n-1})$

Car: $x^n-1 = (x-1)(1+x+\dots+x^{n-1})$

5) Dans $\mathbb{C}[X]$ Les $(x - e^{\frac{2k\pi i}{n}})$

où $0 \leq k \leq n-1$ divisent (x^n-1)

Car $x^n-1 = \prod_{k=0}^{n-1} (x - e^{\frac{2k\pi i}{n}})$

Prop 2

1) $\forall A \in \mathbb{K}[X], A/0$

2) $\forall A \in \mathbb{K}[X], \forall \lambda \in \mathbb{K}^*$ on a:

i) λ / A .

ii) $(\lambda A) / A$ et $A / (\lambda A)$.

3) $(A/B \text{ et } B/C) \Rightarrow A/C$

4) $\left(\begin{matrix} A/B \\ A/C \end{matrix} \right) \Rightarrow A/(B \pm C)$

$$\underline{51} \quad (\forall 1 \leq k \leq n, A/B_k) \Rightarrow A / \left(\sum_{k=1}^n \lambda_k B_k \right)$$

où $\lambda_1, \dots, \lambda_n \in K$.

$$\underline{61} \quad \begin{pmatrix} A/B \\ C/D \end{pmatrix} \Rightarrow AC/BD$$

$$\underline{71} \quad A/B \Rightarrow \forall k \in \mathbb{N}, A^k/B^k$$

$$\underline{81} \quad \forall k \in \llbracket 1, n \rrbracket, A_k/B_k \Rightarrow \prod_{k=1}^n A_k / \prod_{k=1}^n B_k$$

Notation : $\llbracket 1, n \rrbracket = \{1, 2, \dots, n\}$

Prop 3 : Soient $B \in K[X] \setminus \{0\}$ et $A \in K[X]$.
 $A/B \Rightarrow \deg(A) \leq \deg(B)$.

NB : Il faut que B soit non nul :
 on a $x/0$ mais $d^0(x) = 1 \neq d^0(0) = -\infty$

Dém de prop 3 :

Supp A/B et $B \neq 0$

$$\Rightarrow \exists Q \in K[X] / B = A \cdot Q$$

$$\Rightarrow d^0(B) = d^0(A) + d^0(Q)$$

Or $Q \neq 0$ car $B = AQ$ et $B \neq 0$

d'où $d^0(Q) \geq 0$ ($\in \mathbb{N}$) Alors $\deg(A) \leq \deg(B)$.

Prop 4 : Soient A et $B \in K[X] \setminus \{0\}$
 Les assertions suivantes sont équivalentes :

11 A/B et B/A

21 $\exists \lambda \in K^* B = \lambda A$

31 $\exists \mu \in K^*, A = \mu B$

Dém9: On montrera que $(1) \Rightarrow (2)$; $(2) \Rightarrow (3)$ et $(3) \Rightarrow (1)$

1) $\Rightarrow$ 2)

Supp A/B et B/A

On a $A/B \Rightarrow \exists Q \in K[X], B = QA$

$$\Rightarrow d^0(B) = d^0(Q) + d^0(A) \quad (\Omega)$$

D'autre part

On a $\begin{pmatrix} A/B \\ B/A \end{pmatrix}$, donc $\begin{pmatrix} d^0(A) \leq d^0(B) \\ d^0(B) \leq d^0(A) \end{pmatrix}$

$$\Rightarrow d^0(A) = d^0(B)$$

et $(\Omega) \Rightarrow d^0(Q) = 0$ car d polynôme est non nul

$$\Rightarrow \exists \lambda \in K^* / Q = \lambda$$

Ainsi $B = \lambda A$ $\square$

2) $\Rightarrow$ 3)

Supp $B = \lambda A$ avec $\lambda \in K^*$

On a $A = \mu B$ où $\mu = \frac{1}{\lambda} \in K^*$

3) $\Rightarrow$ 1)

Supp que $A = \mu B$ où $\mu \in K^*$.

$$\text{Alors } \begin{cases} A = \mu B \\ B = \frac{1}{\mu} A \end{cases} \Rightarrow \begin{cases} A/B \\ B/A \end{cases} \quad \square$$

Déf 5: Soient A et $B \in K[X] \setminus \{0\}$.

On dit que A et B sont **associés** si et ssi :

$$A/B \text{ et } B/A$$

Notation: $A \equiv B$

Exo: Montrer que $\equiv$ est une relation d'équivalence

sur $K[X] \setminus \{0\}$

2) Division euclidienne :

Prop 1 (Thm de la div eucli)

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$.

Il existe un unique $(Q, R) \in (\mathbb{K}[X])^2$ tq :

$$\begin{array}{|l} \underline{1)} \quad A = BQ + R \\ \underline{2)} \quad d^0(R) < d^0(B) \end{array}$$

Vocab :

1) On dit qu'on a effectué la division euclidienne de A par B .

2) Q (resp R) s'appelle le quotient (resp reste) de la div euclidienne de A par B .

Exemple :

Effectuer la div euclidienne de $(x^4 + x - 1)$ par $(x^2 + 1)$.

Réponse :

$$x^4 + x - 1 = (x^2 + 1) \underbrace{(x^2 - 1)}_{\text{quoti}} + \underbrace{x}_{\text{reste}}$$

Exemples : Déterminer le reste de la div euclidienne de x^{2020} par :

1) $(x-1)$

4) $(x-1)^2$

2) (x^2-1)

5) $(x+1)(x-1)^2$

3) $(x-i)$

6) (x^2+1)

Sol :

1) $x^{2020} = (x-1)Q(x) + R(x)$

On a : $d^0(R) < d^0(x-1)$

Déterminons le reste $R(x)$:

$$d^0(R) < 1 \Leftrightarrow d^0(R) \leq 0$$

$$\Leftrightarrow \exists c \in \mathbb{K}, R(x) = c$$

$$\text{On a : } x^{2020} = (x-1)Q(x) + c$$

Pour $x=1$ on obtient $1=c$

$\%c$: le reste de la div euclid de x^{2020} par $(x-1)$ est 1.

$$\underline{2)} \quad x^{2020} = (x^2-1)Q(x) + R(x)$$

$$d^0(R) < d^0(x^2-1) = 2$$

$$\text{On a } d^0(R) \leq 1 \Leftrightarrow R(x) = a + bx$$

$$x^{2020} = (x^2-1)Q(x) + R(x)$$

$$x^{2020} = (x^2-1)Q(x) + a + bx, \text{ On prend par } x=1 \text{ et } x=-1.$$

$$\text{On a : } \begin{cases} a+b=1 \\ a-b=1 \end{cases} \Rightarrow \begin{cases} a=1 \\ b=0 \end{cases}$$

$\%c$: le reste de la div euclid de x^{2020} par (x^2-1) est $R(x)=1$.

$$\underline{4)} \quad x^{2020} = (x-1)^2 Q(x) + R(x)$$

$$\text{avec } d^0(R) < d^0((x-1)^2) = 2$$

$\Rightarrow$ le reste $R(x) = a + bx$; où a et $b \in \mathbb{R}$.

$$\text{Ainsi } x^{2020} = (x-1)^2 Q(x) + a + bx \quad \textcircled{2}$$

$$x=1 \text{ dans } \textcircled{2} \Rightarrow a+b=1$$

On a besoin d'une autre équation.

En dérivant, on obtient :

$$2020 x^{2019} = 2(x-1)Q(x) + (x-1)^2 Q'(x) + b$$

$$x=1 \Rightarrow 2020 = b$$

$$\text{d'où } a = -2019$$

$\%c$: $(-2019 + 2020x)$ est le reste de la div euclid de x^{2020} par $(x-1)^2$.

6) $X^{2020} = (X^2 + 1)Q(X) + (a + bX)$ où a et $b \in \mathbb{R}$.

Pour $X = i$, $1 = a + bi$

d'où $\begin{cases} a = 1 \\ b = 0 \end{cases}$; (l'égalité de deux complexes) $\Rightarrow$

c/c : $R(X) = 1$

Prop 2 : Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$

$B \mid A \iff R = 0$

où R est le reste de la div euclidienne de A par B .

Ex d'appli :

Mque $(X^2 + 1) \mid (X^4 + X^3 - X^2 + X - 2)$

Sol :

Il suffit de mque le reste de la div euclid de $P(X)$ par $(X^2 + 1)$ est nul.

On a : $P(X) = (X^2 + 1)Q(X) + a + bX$; où a et $b \in \mathbb{R}$.

$X = i \Rightarrow P(i) = \underbrace{(i^2 + 1)}_{=0} Q(i) + a + bi$

$\Rightarrow i^4 + i^3 - i^2 + i - 2 = a + bi$

$\Rightarrow a + bi = 0$

$\Rightarrow (a = 0 \text{ et } b = 0)$; (Nombre complexe nul) $\Rightarrow$

Ainsi le reste de la div de $P(X)$ par $(X^2 + 1)$ est nul.

càd $(X^2 + 1) \mid P(X)$.

III - Racines d'un polynome :

1) Généralités :

Def 1 : Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
 a est dit racine de P si et si $P(a) = 0$.

Exemple : (à retenir)

$n \geq 2$ et $P(x) = x^n - 1$.

Les racines complexes de $(x^n - 1)$ sont exactement les racines $n^{\text{ème}}$ de l'unité.

en effet :

Soit $a \in \mathbb{C}$.

$$P(a) = 0 \Leftrightarrow a^n = 1$$

$$\Leftrightarrow a \in U_n$$

où U_n est l'ensemble des racines $n^{\text{ème}}$ de l'unité.

Prop 2 : Soient $P(x) \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
le reste de la division euclidienne de $P(x)$ par $(x - a)$ est $P(a)$.

Dém : $P(x) = (x - a)Q(x) + R(x)$.

où $\deg(R) < 1$. Posons $R(x) = c$.

$$P(x) = (x - a)Q(x) + c$$

$$\text{pour } x = a \Rightarrow c = P(a)$$

Corollaire 3 :

Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

$$P(a) = 0 \Leftrightarrow (x - a) \mid P.$$

Dém : $P(a) = 0 \Leftrightarrow \left(\begin{array}{l} \text{Le reste de la div euclid de } P \text{ par } (x - a) \\ \text{est nul} \end{array} \right)$
 $\Leftrightarrow (x - a) \mid P.$

Vocabulaire :

On dit racine de P , ou zéro de P

2) Multiplicité d'une racine :

Exemple introductif :

$$P(x) = (x-7)(x-8)^2(x-9)^3 \in \mathbb{R}[x].$$

Les racines de P sont évidemment 7, 8, 9.

1) Pour la racine 9

$$\text{On a } \begin{cases} (x-9)^3 / P \\ (x-9)^{3+1} \nmid P \end{cases}$$

On dit que 9 est une racine de multiplicité 3.

2) Pour la racine 8 :

$$\text{On a } \begin{cases} (x-8)^2 / P \\ (x-8)^{2+1} \nmid P \end{cases}$$

8 est une racine de multiplicité 2 de P .

3) Pour la racine 7 :

$$\text{On a } (x-7)^1 / P \text{ et } (x-7)^{1+1} \nmid P$$

7 est dite racine de multiplicité 1 de P .

En général, on a la bcf suivante :

Def 1 Soit a une racine du poly P .

Soit $m \in \mathbb{N}^*$.

On dit que a est une racine de multiplicité m de P si et ssi.

$$(x-a)^m / P \text{ et } (x-a)^{m+1} \nmid P.$$

$$\text{Réflexe : } T(a) = 0 \iff T(x) = (x-a)Q(x).$$

Vocab :

a racine de multiplicité m de P .

1) Si $m=1$ a est dit racine simple

2) Si $m=2$ " " " double.

3) Si $m=3$ " " " triple

4) Si $m \geq 2$ " " " multiple

Prop 2 :

Soient $P \in \mathbb{K}$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

Les propositions suivantes sont équivalentes :

1) a racine de multiplicité m de P .

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

NB : Si la multiplicité $m \geq r$, on dit que a est une racine de multiplicité au moins r .

Prop 3 : Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $m \in \mathbb{N}^*$.

Les prop suivantes sont équivalentes :

1) a racine de multiplicité au moins m .

2) $(X-a)^m \mid P$

Exemple introductif :

$P(X) = (X-1)^2$, on a $m=2$ et la multiplicité de 1,

et on a aussi
$$\begin{cases} P^{(0)}(1) = 0 ; P^{(1)}(1) = 0 \\ P^{(2)}(1) \neq 0 \end{cases}$$

En général, on a :

Prop 4 : Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$.

Les propositions suivantes sont équivalentes :

1) a racine de multiplicité m de P .

2)
$$\begin{cases} P(a) = \dots = P^{(m-1)}(a) = 0 \\ P^{(m)}(a) \neq 0 \end{cases}$$

⚠ Avertissement :

Supp $P(x) = \sum_{k=0}^n a_k x^k$

$P(0) \neq 0$ mais $P(0) = a_0$

Supp $T(x) = \sum_{k=0}^n a_k (x-b)^k$

$T(b) \neq 0$ mais $T(b) = a_0$.

Démo prop 4 :

1) $\Rightarrow$ 2)
$$\begin{cases} P(x) = (x-a)^m Q(x) \\ \text{avec } Q(a) \neq 0 \end{cases}$$

On a :

i) Soit $0 \leq k \leq m-1$ Mque $P^{(k)}(a) = 0$

$$\begin{aligned} P^{(k)}(x) &= ((x-a)^m Q(x))^{(k)} \\ &= \sum_{i=0}^k C_k^i ((x-a)^m)^{(i)} Q(x)^{(k-i)} \end{aligned}$$

$$((x-a)^m)^{(i)} = \frac{m!}{(m-i)!} (x-a)^{m-i}$$

Or $\forall 0 \leq i \leq k$, on a $i \leq m-1$ car $k \leq m-1$.

$\Rightarrow \forall 0 \leq i \leq k$, $m-i \geq 1$.

$\Rightarrow \forall 0 \leq i \leq k$ $(x-a)^{m-i}$ s'annule en a .

Ainsi $P^{(k)}(a) = 0$

ii) $P^{(m)}(a) \neq 0$?

$$P^{(m)}(x) = ((x-a)^m Q(x))^{(m)} \\ = \sum_{i=0}^m C_m^i ((x-a)^m)^{(i)} Q^{(m-i)}(x)$$

$$((x-a)^m)^{(i)} = \frac{m!}{(m-i)!} (x-a)^{m-i}$$

Ainsi $((x-a)^m)^{(i)}$ s'annule en a si $m-i \geq 1$

Càd si $i \leq m-1$.

$$\text{Ainsi } P^{(m)}(a) = m! \cdot Q^{(0)}(a) = m! Q(a) \neq 0$$

21 $\Rightarrow$ 11 Par récurrence sur $m \geq 1$.

Prop 5:

$m \in \mathbb{N}^*$, $a \in K$ et $P \in K[x]$ on a:

$$(x-a)^m \mid P \iff (\forall 0 \leq k \leq m-1, P^{(k)}(a) = 0)$$

Dém:

$(\Rightarrow)$ vu $(\Leftarrow)$ récurrence sur $m \in \mathbb{N}^*$

Réflexe à avoir:

Si $T(x) = (x-a)^m Q(x)$ alors

$$T(a) = T^{(1)}(a) = \dots = T^{(m-1)}(a) = 0$$

Ex : Déterminons le reste de la div euclidienne de x^{2020} par $(x-1)^3$

Sol :

$$x^{2020} = \underbrace{(x-1)^3 Q(x)}_{\text{noté } T(x)} + (a + bx + cx^2)$$

$$\text{On a } T(x) = (x-1)^3 Q(x)$$

$$\Rightarrow T(1) = T'(1) = T''(1) = 0$$

$$\text{Ainsi } \begin{cases} 1 = a + b + c \\ 2020 = b + 2c \\ 2020 \times 2019 = 2c \end{cases} \quad \text{; Alors } \begin{cases} a = \text{---} \\ b = \text{---} \\ c = \text{---} \end{cases}$$

C/c : 2 tests voulu et

$$R(x) = \text{---}$$

□

Exo (TD)

Soit $n \in \mathbb{N}^*$

Montrer $x^2 \mid ((x+1)^n - nx - 1)$

Solution

Notons $P(x) = (x+1)^n - nx - 1$

On veut M. qm. $x^2 \mid P$.

On a : $x^2 \mid P \Leftrightarrow (P(0) = 0 \text{ et } P'(0) = 0)$

$$\text{i) On a } P(0) = 1 - 1 = 0$$

$$\text{ii) } P'(x) = n(x+1)^{n-1} - n$$

$$\Rightarrow P'(0) = n - n = 0$$

d'où

$$x^2 \mid P$$

□

3) Nombre de racines d'un polynôme.

Prop 1:

Soient $P(x) \in K[x]$ et $x_1 \neq x_2 \in K$.

$$(P(x_1) = P(x_2) = 0) \Leftrightarrow (x - x_1)(x - x_2) \mid P(x)$$

Démo:

$(\Leftarrow)$ évident.

$(\Rightarrow)$ Supposons que $P(x_1) = P(x_2) = 0$

Montrons que $(x - x_1)(x - x_2) \mid P(x)$

On a : $P(x_1) = 0 \Rightarrow \exists Q \in K[x] ; P(x) = (x - x_1) Q(x)$

$$\text{et } P(x_2) = 0 \Rightarrow 0 = \underbrace{(x_2 - x_1)}_{\neq 0} Q(x_2)$$

$$\Rightarrow Q(x_2) = 0 \quad (\text{car } x_1 \neq x_2)$$

$$\Rightarrow \exists T(x) \in K[x] , Q(x) = (x - x_2) \cdot T(x).$$

$$\text{D'où } P(x) = (x - x_1)(x - x_2) T(x).$$

Alors $(x - x_1)(x - x_2) \mid P(x)$.

En général, on a la prop suivante:

Prop 2: soit $n \geq 2$ - soient $x_1, \dots, x_n \in K$ distincts deux à deux on a :

$$(P(x_1) = \dots = P(x_n) = 0) \Leftrightarrow (x - x_1) \dots (x - x_n) \mid P(x)$$

Dém. ($\Leftarrow$) évident.

($\Rightarrow$) Via prop 1 et récurrence.

Réflexe : Pour montrer que :

$(x-a)(x-b) \mid P(x)$ où $a \neq b$ il suffit de mgue
 $P(a) = 0$ et $P(b) = 0$

Exercice :

Mgue : $(x^2 - 3x + 2) \mid T(x)$ où
 $T(x) = x^4 - 3x^3 + 3x^2 - 3x + 2$.

Sol : Mgue $(x-1)(x-2) \mid T(x)$

Il suffit de mgue $T(1) = 0$ et $T(2) = 0$ car $1 \neq 2$

N.B : $(x_1, \dots, x_n \text{ distincts 2 à 2}) \Leftrightarrow (\forall i \neq j, x_i \neq x_j)$

Prop 3 : Soient $P \in \mathbb{R}[X]$ et $w \in \mathbb{C}$.
 w racine de $P \Leftrightarrow \bar{w}$ racine de P .

Dém. : Posons $P(x) = \sum_{k=0}^n a_k x^k$, $\forall a_k \in \mathbb{R}$.

$$P(w) = 0 \Leftrightarrow \sum_{k=0}^n a_k w^k = 0$$

$$\Leftrightarrow \sum_{k=0}^n \bar{a}_k \bar{w}^k = 0$$

$$\Leftrightarrow \sum_{k=0}^n a_k (\bar{w})^k = 0 \quad (\bar{a}_k = a_k)$$

$$\Leftrightarrow P(\bar{w}) = 0$$

Attention ! Si $P \notin \mathbb{R}[X]$, c'est FAUX

C - ex. :

$$P(x) = x - i$$

i racine de $P(x)$

$\bar{i} = -i$ n'est pas racine de $P(x)$

Réflexe :

Soit P polyn à coeff réels.
Si P possède une racine complexe w
alors il a w et $\bar{w}$ comme racines.

Ex d'appli :

Redémontrons que :

$(x^2+1) \mid T(x)$ où $T(x) = x^4 + x^3 - x^2 + x - 2$.

Sol : on a :

$$\begin{aligned}(x^2+1) \mid T(x) &\Leftrightarrow (x-i)(x+i) \mid T(x) \\ &\Leftrightarrow_{i \neq -i} T(i) = 0 \text{ et } T(-i) = 0 \\ &\Leftrightarrow T(i) = 0\end{aligned}$$

car $\bar{i} = -i$ et T à coeff réels,
et on a $T(i) = 0$

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

Si $\begin{pmatrix} P \neq 0 \\ d^o(P) \leq n \end{pmatrix}$ alors P admet au plus n racines
distinctes :

Dém :

Supp que $\begin{cases} P \neq 0 \\ d^o(P) \leq n \end{cases}$

Soient $x_1, \dots, x_p$, Les p racines distinctes de P .

Il s'agit de mqr $p \leq n$

On a $(x-x_1) \dots (x-x_p) \mid P(x)$

$$\Rightarrow d^0((x-x_1)\dots(x-x_p)) \leq d^0(P(x))$$

$\underbrace{\hspace{10em}}_{=A} \qquad \underbrace{\hspace{10em}}_{\leq n}$

d'où $A \leq n$

Prop 4: Soit $n \in \mathbb{N}^*$

Si $\begin{cases} \text{1/ } d^0(P) \leq n \\ \text{2/ } P \text{ possède } (n+1) \text{ racines distinctes.} \end{cases}$

Alors $P=0$

Dém: En bref (Par l'absurde)

Supp que $P \neq 0$

puisque $d^0(P) \leq n$, alors P possède au plus n racines distinctes.

Ce qui contredit le fait qu'il y a $(n+1)$ racines distinctes, d'où $P=0$.

Reflexes

1/ Si $\begin{cases} d^0(P) \leq 2 \\ P(1) = P(7) = P(-1) = 0 \end{cases}$

Alors $P=0$

2/ Si $\begin{cases} P \in \mathbb{R}_1[X] \\ P(1) = P(-1) = 0 \end{cases}$ alors $P=0$

Ex d'appli (Extrait CNC)

Soit $n \in \mathbb{N}^*$.

Soient $x_0, x_1, \dots, x_n$ des réels $2 \text{ à } 2$ distincts.

Considérons l'application :

$$\phi : \mathbb{R}_n[x] \longrightarrow \mathbb{R}^{n+1}$$

$$P \longmapsto (P(x_0), P(x_1), \dots, P(x_n))$$

Soit $P \in \mathbb{R}_n[x]$ tel que $\phi(P) = (0, 0, \dots, 0)$

Montrer : $P = 0$

Solution :

Soit $P \in \mathbb{R}_n[x]$ tel que $\phi(P) = (0, 0, \dots, 0)$

Montrer : $P = 0$

$$\text{On a } \phi(P) = (0, \dots, 0)$$

$$\Rightarrow (P(x_0), \dots, P(x_n)) = (0, \dots, 0)$$

$$\Rightarrow P(x_0) = 0, \dots, P(x_n) = 0$$

$$\text{D'où } \begin{cases} P \text{ admet } (n+1) \text{ racines distinctes} \\ \deg(P) \leq n \end{cases}$$

Par suite $P = 0$ $\square$

Corollaire 5

Un polynôme ayant une infinité de racines est nul.

Ex d'appli : (TD)

Soient U et $V \in \mathbb{R}[X]$ vérifiant :

$$\forall x > 0, U(x) \cos(x) + V(x) \sin(x) = 0$$

Montrer $U = 0$ et $V = 0$

4/ Cas des racines complexes :

Prop 1 (Théorème de d'Alembert - Gauss)

Tout polynôme de degré ≥ 1 admet au moins une racine complexe.

Dém : hors programme

Corollaire 2 :

Tout polynôme de degré ≥ 1 est divisible par un polynôme complexe de degré 1.

Dém:

D'Alembert - Gauss $\Rightarrow \exists \alpha \in \mathbb{C}, P(\alpha) = 0$
 $\Rightarrow (x - \alpha) / P(x)$

NB: C'est faux dans $\mathbb{R}$.

$(x^2 + 1)^{2020}$ de degré ≥ 1 et n'a aucune racine réelle.

IV Polynômes irréductibles.

1) Généralité:

Def 1:

Soit $P \in K[x]$.

P est dit irréductible dans $K[x]$ si et ssi :

1) $\deg(P) \geq 1$

2) Les seuls diviseurs de P dans $K[x]$ sont ses associés et les polynômes constants non nuls.

NB₁:

2) Veut dire que ses seuls diviseurs sont de la forme (λP) et μ où λ et $\mu \in K^*$.

NB₂:

Pour tout $\lambda \in K$, λ n'est pas irréductible.

Exemples express.

1) $(x^2 - 1)$ est-il irréductible dans $\mathbb{R}[x]$? $\mathbb{C}[x]$?

Rep: non car $\underbrace{(x-1)}_{\in \mathbb{R}[x]} / (x^2-1)$ et $\underbrace{(x-1)}_{\in \mathbb{Q}[x]} / (x^2-1)$

2) (x^2+1) est-il irréductible dans $\mathbb{R}[X]$? $\mathbb{C}[X]$?

Rep:

a) Dans $\mathbb{R}[X]$, oui.

Dans $\mathbb{C}[X]$, non car $(x-i) / (x^2+1)$.

3) En général, tout polynôme réel de degré 2 à discriminant $\Delta < 0$ est irréductible dans $\mathbb{R}$.

Démo:

$$P(x) = ax^2 + bx + c \quad (a, b, c) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}$$

$$\Delta < 0$$

$\Rightarrow$ $\text{supp } P(x)$ n'est pas irréductible dans $\mathbb{R}$.

Alors $[\exists (\alpha, \beta) \in \mathbb{R}^* \times \mathbb{R} : (\alpha x + \beta) / P(x)]$

$\Rightarrow \frac{-\beta}{\alpha}$ est une racine réelle de $P(x)$

Ce qui est absurde, car $\Delta < 0$

Prop 2:

1) Dans $\mathbb{C}[X]$, tous les polynômes de degré ≥ 2 ne sont pas irréductibles.

2) Dans $\mathbb{K}[X]$, tous les polynômes de degré 1 sont irréductibles.

3) Dans $\mathbb{R}[X]$, tous les polynômes de degré 2 à discriminant < 0 sont irréductibles.

Démo:

1) Soit $P \in \mathbb{C}[X]$ avec $d^0(P) \geq 2$

$\xRightarrow{\text{D-G}} \exists \alpha \in \mathbb{C} \mid P(\alpha) = 0$

$$\Rightarrow (x - \alpha) \mid P(x).$$

21 et 31 OK

2°) Les polynômes irréductibles dans $\mathbb{R}$ et dans $\mathbb{C}$.

⚡! Prop 1: Dans $\mathbb{C}$, les polynômes irréductibles sont les polynômes de degré 1.

Démo: (OK)

⚡! Prop 2: Dans $\mathbb{R}$, les polynômes irréductibles sont les polynômes de degré 1 et ceux de degré 2 à discriminant < 0 .

Démo:

Soit $P \in \mathbb{R}[x]$.

→ Si $\deg(P) \leq 0$; P n'est pas irréductible dans $\mathbb{R}[x]$.

→ Si $\deg(P) = 1$: P est irréductible dans $\mathbb{R}[x]$ (déjà vu)

→ Si $\deg(P) = 2$:

→ Si $\Delta < 0$, P est irréductible dans $\mathbb{R}[x]$

→ Si $\Delta \geq 0$:

P n'est pas irréductible dans $\mathbb{R}[x]$

Car P possède une racine réelle α
et donc $(x - \alpha) \mid P$.

31 si $d^{\circ}(P) \geq 3$.

On montrera que P n'est pas irréductible dans $\mathbb{R}[X]$.

$$D-G \Rightarrow \exists \alpha \in \mathbb{C} / P(\alpha) = 0$$

Cas 1 : Si $\alpha \in \mathbb{R}$.

on a $(X - \alpha) \in \mathbb{R}[X]$ et $(X - \alpha) \mid P(X)$.

P n'est pas irréductible ds $\mathbb{R}$.

Cas 2 : Si $\alpha \notin \mathbb{R}$. ($(X - \alpha) \notin \mathbb{R}[X]$)

$$\text{on a } \begin{cases} P(\alpha) = 0 \\ P(\bar{\alpha}) = 0 \end{cases}$$

car P à coeff réels.

$$\text{or } \alpha \neq \bar{\alpha} \text{ (car } \alpha \notin \mathbb{R})$$

$$\begin{aligned} \bar{\bar{z}} &= z \Leftrightarrow z \in \mathbb{R} \\ \bar{z} &\neq z \Leftrightarrow z \notin \mathbb{R} \end{aligned}$$

Rappel

$$\text{d'où } (X - \alpha)(X - \bar{\alpha}) \mid P(X)$$

$$\Rightarrow \begin{cases} (X^2 - (\alpha + \bar{\alpha})X + |\alpha|^2) \mid P(X) \\ \text{et} \\ (X^2 - 2\operatorname{Re}(\alpha)X + |\alpha|^2) \in \mathbb{R}[X]. \end{cases}$$

D'où $P(X)$ n'est pas irréductible ds $\mathbb{R}$.

31 Décomposition d'un polynôme en produit de facteurs irréductibles.

Vocab. On parle aussi de « factorisation ».

Ex : Décomposer chacun des polynômes suivants en prod de fact irréductibles, dans $\mathbb{R}$ et dans $\mathbb{C}$: $x^3 \pm 1$; $x^4 \pm 1$; $x^6 \pm 1$.

Sol :

1) $x^3 - 1$:

a) Dans $\mathbb{R}$.

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

b) Dans $\mathbb{C}$.

$$(x^3 - 1) = (x - 1)(x - j)(x - j^2) \text{ où } j = e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2}$$

$$x^n - 1 = (x - 1) \sum_{k=0}^{n-1} x^k = (x - 1)(1 + x + \dots + x^{n-1})$$

Rappel :

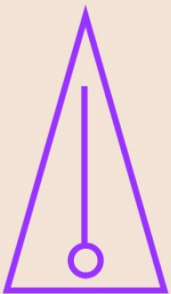
$$\bar{j} = j^2 = \frac{1}{j} \quad , \quad \mathbb{L}_3 = \{1, j, j^2\}.$$

Soit $n \geq 2$. On a :

1) Les racines complexes de $(X^n - 1)$ sont les racines n-èmes de l'unité ; c-à-d :

les $e^{\frac{2k\pi i}{n}}$, avec $0 \leq k \leq n-1$.

$$2) \quad X^n - 1 = \prod_{k=0}^{n-1} (X - x_k) \quad , \text{ où } x_k = e^{\frac{2k\pi i}{n}}$$



à
retenir

D'une manière générale, on a :

Prop 1 :

1) Tout polynôme $P \in \mathbb{K}[x]$, de degré ≥ 1 , s'écrit sous la forme :

$$P = \lambda P_1 \cdots P_n$$

où $\lambda \in \mathbb{K}^*$ et les P_i unitaires et irréductibles dans $\mathbb{K}[x]$

NB : $\lambda = \text{cd}(P)$.

NB₁ : Décomposition dans $\mathbb{C}$.

1)
$$P(x) = \lambda \prod_{k=1}^n (x - x_k)$$

où $\begin{cases} \lambda = \text{cd}(P) \\ n = \deg(P) \\ x_1, \dots, x_n \text{ les racines de } P, \text{ non forcément distinctes 2 à 2.} \end{cases}$

2)
$$P(x) = \lambda \prod_{i=1}^s (x - a_i)^{m_i}$$

où $\lambda = \text{cd}(P)$, $\deg(P) = \sum_{i=1}^s m_i$

$a_1, \dots, a_s$ les racines de P 2a et distincts entre eux.

m_i étant la multiplicité de la racine a_i .

NB₂ : Décomposition dans $\mathbb{R}$.

$$P(x) = \lambda \prod_{i=1}^s (x - x_i)^{m_i} \cdot \prod_{k=1}^r (x^2 + b_k x + c_k)^{n_k}$$

où $\lambda = \text{cd}(P)$, $\text{deg}(P) = \sum_{i=1}^s m_i + \sum_{k=1}^r 2n_k$.

Les x_i sont les racines réelles de P distinctes 2 à 2

$$\forall k, b_k^2 - 4c_k < 0.$$

V Polynômes scindés

1) Généralités.

Def 1 Un polynôme $P \in K[x]$ est dit **scinde** dans K si et ssi :

1) $\text{deg}(P) \geq 1$.

2) P s'écrit comme produit de polynômes de degrés 1 et à coefficients dans K .

Exemples rapides :

1) $(x^2 - 1) = (x - 1)(x + 1)$

$(x^2 - 1)$ est scinde dans $\mathbb{R}$ et dans $\mathbb{C}$.

2) $x^2 + 1 = (x - i)(x + i)$

$(x^2 + 1)$ est scinde dans $\mathbb{C}$ mais pas dans $\mathbb{R}$.

Prop 2 :

Dans $\mathbb{C}$, tout polynôme de degré ≥ 1 est scinde.

Dém : Repose sur le thm de d'Alembert - Gauss.

NB : Soit $P \in \mathbb{K}[X]$ scinde dans $\mathbb{K}$.

1) P s'écrit sous la forme :

$$P(X) = \lambda \prod_{k=1}^n (X - x_k).$$

où $\left\{ \begin{array}{l} \lambda \text{ et les } x_k \in \mathbb{K}. \\ d^0(P) = n \\ x_1, \dots, x_n \text{ les racines de } P, \text{ non forcément distincts} \\ 2 \text{ à } 2. \end{array} \right.$

2) P s'écrit aussi sous la forme

$$P(X) = \lambda \prod_{i=1}^p (X - a_i)^{m_i}$$

où $\left\{ \begin{array}{l} \lambda \text{ et les } a_i \in \mathbb{K}. \\ d^0(P) = \sum_{i=1}^p m_i \\ a_1, \dots, a_p \text{ sont les racines de } P \text{ distinctes } 2 \text{ à } 2 \end{array} \right.$

m_i = la multiplicité de la racine a_i .

2.7 Relations de Viète entre les racines et les coeff d'un polynôme scinde

Lemme :

Soit $n \geq 1$. Soient $x_1, \dots, x_n \in \mathbb{K}$

$$\prod_{k=1}^n (X - x_k) = X^n - \left(\sum_{k=1}^n x_k \right) X^{n-1} + \dots + (-1)^n \left(\prod_{k=1}^n x_k \right).$$

Dém : par récurrence sur $n \geq 1$ (à faire).

Prop 1 :

Soit $n \geq 1$

Soit $P(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$ de degré n , scindé dans K .

Soient $x_1, \dots, x_n$ ses racines, non forcément distinctes

à 2 on a :

$$\text{1) } \sum_{k=1}^n x_k = \frac{-a_{n-1}}{a_n}$$

$$\text{2) } \prod_{k=1}^n x_k = \frac{(-1)^n a_0}{a_n}$$

Dém. :

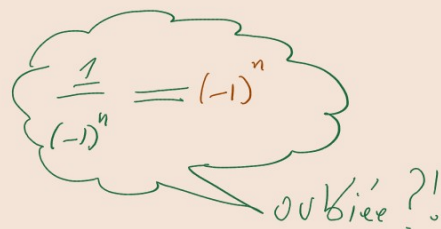
On a $P(x) = a_n \prod_{k=1}^n (x - x_k)$.

d'après le lemme, on a alors.

$$P(x) = a_0 + \dots + a_{n-1}x^{n-1} + a_nx^n$$

$$P(x) = a_n \left(x^n - \left(\sum_{k=1}^n x_k \right) x^{n-1} + \dots + (-1)^n \left(\prod_{k=1}^n x_k \right) \right)$$

$$\Rightarrow \begin{cases} -a_n \sum_{k=1}^n x_k = a_{n-1} \\ a_n (-1)^n \left(\prod_{k=1}^n x_k \right) = a_0 \end{cases}$$


$$\frac{1}{(-1)^n} = (-1)^n$$

oubliée?!

D'où la conclusion.

Exemple :

$P(x) = ax^2 + bx + c$, $a \neq 0$, et x_1 et x_2 ses racines.

Au lycée : On avait vu que $\begin{cases} x_1 + x_2 = -\frac{b}{a} \\ x_1 x_2 = \frac{c}{a} \end{cases}$

Via la Prop 1 :

En posant $\begin{cases} a = a_2 \\ b = a_1 \\ c = a_0 \end{cases}$, on a :

$$\begin{cases} x_1 + x_2 = -\frac{a_1}{a_2} = -\frac{b}{a} \\ x_1 x_2 = (-1)^2 \frac{a_0}{a_2} = \frac{c}{a} \end{cases}$$

Q) $x_1, x_2 \text{ et } x_3 \in \mathbb{K}$

$$\sigma_2 = \sum_{1 \leq i_1 < i_2 \leq 3} x_{i_1} x_{i_2} = ?$$

$$\sigma_3 = \sum_{1 \leq i_1 < i_2 < i_3 \leq 3} x_{i_1} x_{i_2} x_{i_3} = ?$$

Rep: $\sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$
 $\sigma_3 = x_1 x_2 x_3$

Q) $x_1, x_2, x_3 \text{ et } x_4 \in \mathbb{K}$

$$\sigma_2 = \sum_{1 \leq i_1 < i_2 \leq 4} x_{i_1} x_{i_2} = ?$$

$$\sigma_3 = \sum_{1 \leq i_1 < i_2 < i_3 \leq 4} x_{i_1} x_{i_2} x_{i_3} = ?$$

$$\sigma_4 = \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq 4} x_{i_1} x_{i_2} x_{i_3} x_{i_4} = ?$$

Rep: $\sigma_2 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$
 $\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4$
 $\sigma_4 = x_1 x_2 x_3 x_4$

Prop 2: Formule de Viète (cas général)

$$P \in \mathbb{K}[X], \deg(P) = n \geq 1.$$

$$P(X) = a_0 + \dots + a_n X^n.$$

$x_1, \dots, x_n$ Les racines de P (non forcément distinctes

2 à 2) On a :

$$\forall 1 \leq k \leq n; \underbrace{\sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \dots x_{i_k}}_{= \sigma_k} = \frac{(-1)^k a_{n-k}}{a_n}$$

NB :

Pour $k=1$ et $k=n$, on retrouve la (Prop 1) :

$$1) \sum_{1 \leq i_1 \leq n} x_{i_1} = \frac{(-1)^1 a_{n-1}}{a_n} = \frac{-a_{n-1}}{a_n}$$

2) Pour $k=n$.

$$x_1 \dots x_n = \frac{(-1)^n a_0}{a_n}$$

VII Formule de Taylor polynomiale Composition polynomiale

1) Formule de Taylor.

Prop 1

Soit $P \in \mathbb{K}[x]$, on a :

$$P(x) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} x^k.$$

Démo :

$$\text{Posons } P(x) = \sum_{k=0}^{+\infty} a_k x^k$$

Soit $n \in \mathbb{N}$.

$$\text{on a } P^{(n)}(x) = \sum_{k=n}^{+\infty} k(k-1)\dots(k-n+1) a_k x^{k-n}$$

$$\Rightarrow P^{(n)}(0) = n! a_n \quad (\text{c'est le 1er terme})$$

$$\text{d'où } (\forall n \in \mathbb{N}, a_n = \frac{P^{(n)}(0)}{n!})$$

Ainsi

$$P(x) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(0)}{k!} x^k$$

Corollaire 2 : Soient $P \in \mathbb{K}[x]$ et $a \in \mathbb{K}$, on a :

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

Démo :

Pour montrer que : $P(x) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (x-a)^k$.

Il suffit de montrer que :

$$P(x+a) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} x^k \quad (*)$$

Posons alors $T(x) = P(x+a)$.

D'après prop 1 :

$$T(x) = \sum_{k=0}^{+\infty} \frac{T^{(k)}(0)}{k!} (x)^k.$$

D'autre part on a : $T(x) = P(x+a)$

$$T^{(k)}(x) = P^{(k)}(x+a)$$

$$T^{(k)}(0) = P^{(k)}(a).$$

En l'injectant, dans $(*)$ on obtient.

$$P(x+a) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} x^k \quad \underline{\text{CQFD}}$$

2) Composition de polynômes.

Déf 1 :

Soient $P(x) = \sum_{k=0}^{+\infty} a_k x^k$ et $Q(x) \in \mathbb{K}[X]$.

$$(P \circ Q)(x) \stackrel{\text{def}}{=} \sum_{k=0}^{+\infty} a_k (Q(x))^k.$$

Prop 2 :

Soient P et $Q \in \mathbb{K}[X] \setminus \{0\}$.

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

Démo : (en bref).

Notons $n = \deg(P) \in \mathbb{N}$.

$$P(x) = a_0 + a_1 x + \dots + a_n x^n \quad (a_n \neq 0).$$

$$\text{On a : } (P \circ Q)(x) = a_0 + a_1 Q(x) + \dots + a_n Q(x)^n$$

$$\deg(P \circ Q(x)) = \deg(Q(x)^n)$$

$$= n \deg(Q)$$

$$= \deg(P) \times \deg(Q).$$

Exo d'application :

Déterminer tous les polynômes $P \in \mathbb{R}[X]$.

tels que $P(x^2) = (x^2+1)P(x)$ (I).

Solution :

Cas 1 : Si $P=0$, c'est une solution.

Cas 2 : si $P \neq 0$

Notons $n = \deg(P) \in \mathbb{N}$, on a :

$P(x^2) = (x^2+1)P(x)$ implique par passage au degré que : $2n = 2+n \Rightarrow n=2$.

Posons $P(x) = ax^2 + bx + c$ avec $a \neq 0$

On a $P(x^2) = (x^2+1)P(x) \Leftrightarrow$

$$ax^4 + bx^2 + c = ax^4 + bx^3 + (a+c)x^2 + bx + c.$$

$$\Leftrightarrow \begin{cases} a = -c \\ b = 0 \end{cases}$$

$$\Leftrightarrow P(x) = a(x^2-1)$$

Ainsi les sol de (I) sont 0 et $a(x^2-1)$ avec $a \neq 0$.

On a : $S = \{a(x^2-1) / a \in \mathbb{R}\}.$

31 Polynôme d'interpolation de Lagrange

Notation : $n \in \mathbb{N}^*$, $a_0, \dots, a_n \in K$, distincts

2 à 2. Pour $k \in \llbracket 0, n \rrbracket$, on note :

$$L_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^n \left(\frac{x - a_j}{a_k - a_j} \right)$$

Prop 1:

1) Soit $k \in \llbracket 0, n \rrbracket$, $L_k(x)$ est un polynôme de degré n .

$$2) \text{ Soient } k, i \in \llbracket 0, n \rrbracket, \begin{cases} L_k(a_i) = 0 & \text{si } k \neq i \\ L_k(a_i) = 1 & \text{si } k = i \end{cases}$$

Démo :

$$1) L_k(x) = \prod_{\substack{j=0 \\ j \neq k}}^n \left(\frac{x - a_j}{a_k - a_j} \right) = \underbrace{\prod_{\substack{j=0 \\ j \neq k}}^n \left(\frac{1}{a_k - a_j} \right)}_{\text{Constante}} \times \underbrace{\prod_{\substack{j=0 \\ j \neq k}}^n (x - a_j)}_{\text{polynôme de degré } n}$$

2) Les a_j , avec $j \neq k$, sont des racines de $L_k(x)$.

$$\Rightarrow L_k(a_i) = 0 \text{ si } k \neq i$$

Et si $k = i$, on a :

$$L_k(a_i) = L_k(a_k) = \prod_{\substack{j=0 \\ j \neq k}}^n \left(\frac{a_k - a_j}{a_k - a_j} \right) = \prod_{\substack{j=0 \\ j \neq k}}^n 1 = 1$$

Prop 2: Soient $a_0, \dots, a_n \in \mathbb{K}$ distincts 2 à 2.

Soient $y_0, \dots, y_n \in \mathbb{K}$.

1) Il existe un unique polynôme $P \in \mathbb{K}_n[x]$ tel que
 $\forall k \in \llbracket 0, n \rrbracket, P(a_k) = y_k$

2) Ce polynôme P est exactement :

$$P(x) = \sum_{j=0}^n y_j L_j(x)$$

Démo

1) i) Unicité

Soient P et $Q \in K_n[x]$ tels que :

$$\begin{cases} \forall k \in [0, n], P(a_k) = y_k \\ \forall k \in [0, n], Q(a_k) = y_k \end{cases}$$

Montrons que $P = Q$; c'est à dire $P - Q = 0$

On a P et $Q \in K_n[x]$ alors $(P - Q) \in K_n[x]$

Et on a aussi : $(\forall 0 \leq k \leq n, P(a_k) = Q(a_k))$

$$\Rightarrow \begin{cases} \deg(P - Q) \leq n \\ \forall 0 \leq k \leq n, (P - Q)(a_k) = 0 \end{cases}$$

Ainsi : $\begin{cases} \deg(P - Q) \leq n \\ (P - Q) \text{ admet } (n+1) \text{ racines distinctes,} \end{cases}$

D'où

$$\boxed{P - Q = 0}$$



ii) Existence

Vérifions que le polynôme : $P(x) = \sum_{j=0}^n y_j L_j(x)$, convient.

a) $P \in K_n[x]$

Car $\forall 0 \leq j \leq n, L_j(x) \in K_n[x]$ ($\deg(L_j(x)) = n \leq n$)

b) Soit $0 \leq k \leq n$. Montrer $P(a_k) = y_k$

$$\text{On a } P(x) = \sum_{j=0}^n y_j L_j(x)$$

$$\Rightarrow P(a_k) = \sum_{j=0}^n y_j L_j(a_k)$$

$$= y_k L_k(a_k)$$

$$= y_k$$



(Car $\forall j \neq k, L_j(a_k) = 0$)

($L_k(a_k) = 1$)

$$L_j(a_k) = 0 \text{ si } j \neq k$$

$$L_j(a_k) = 1 \text{ si } j = k$$

NB : On verra plus loin une démo plus rapide

NB : (à montrer)

Les polynômes $T \in \mathbb{K}[x]$ vérifiant :

$\forall i \in \llbracket 0, n \rrbracket, T(a_i) = y_i$

sont exactement ceux de la forme :

$$T(x) = P(x) + \left(\prod_{k=0}^n (x - a_k) \right) \cdot Q(x)$$

où $P(x)$ est celui de la prop et $Q \in \mathbb{K}[x]$ quelconque.

VII Arithmétique des polynômes (Partie 2)

1) Pgcd de deux polynômes tous deux non nuls.

Déf 1 : Soient P et $Q \in K[X]$, non tous deux nuls.
Le Pgcd de P et Q , noté $P \wedge Q$, est le polynôme unitaire de plus haut degré appartenant à $D(P) \cap D(Q)$

où $D(P)$ est l'ensemble des diviseurs de P .

NB :

1) Tout polynôme associé à $P \wedge Q$ est dit un pgcd de P et Q .

2) $P \wedge Q$ impose qu'il soit unitaire

Ex rapide :

1) $2x \wedge x^2 = x$

2) $x, 25x$ sont des pgcd de $2x$ et x^2

NB :

1) Si $A \mid B$ alors

i) $A \wedge B = \frac{A}{\text{cd}(A)}$

ii) A est un pgcd de A et B .

21 • $D(A) \cap D(B) = D(A \wedge B)$.

• $\begin{cases} P/A \\ P/B \end{cases} \Leftrightarrow P/(A \wedge B)$

31 On a l'algorithme d'Euclide qui est analogue à celui pour les entiers.
Il donne un pgcd.

41 L'algorithme d'Euclide, tout comme pour les entiers, il donne une relation de Bézout

51 Si D est un pgcd de A et B , alors il existe U et $V \in K[x]$ tels que :

$$AU + BV = D.$$

21 PPCM de deux polynômes non nuls.

Déf 1e Soient P et $Q \in K[x] \setminus \{0\}$.

Le ppem de P et Q , noté $P \vee Q$ est le polynôme unitaire, de plus petit degré parmi les multiples commun à P et à Q .

Exemple (NB):

11 $(2x) \vee (3x^2) = x^2$.

21 $A/B \Rightarrow A \vee B = \frac{B}{\text{cd}/B}$

31 $\begin{cases} P/A \\ Q/A \end{cases} \Rightarrow P \vee Q / A$

41 $(A \wedge B) \cdot (A \vee B) \stackrel{\text{associé}}{=} AB$

Pause: Soient λ et μ deux polynômes constants non nuls

1) On a λ / μ

2) $\lambda \wedge \mu = 1$

Attention: c'est l'arithm des polynômes non des entiers.

3) Pgcd d'un nombre fini de polynômes.

NB₁:

1) $(A_1 \wedge A_2) \wedge A_3 = A_1 \wedge (A_2 \wedge A_3)$.

qu'on note $A_1 \wedge A_2 \wedge A_3$ qui est le pgcd de A_1, A_2 et A_3

2) Pareil aux entiers.

NB₂: On parle ainsi de $(A_1 \wedge \dots \wedge A_n)$ le pgcd de $A_1, \dots, A_n$.
C'est défini d'une manière récurrente.

NB₃: On parle de m du pgcd de plusieurs entiers $a_1, \dots, a_n$ et se note:
 $a_1 \wedge \dots \wedge a_n$ (Pour les entiers).

Exemple express.

Concernant l'arith des entiers que vaut

$$\underline{6 \wedge 26 \wedge 16 \wedge 8.}$$

$$\underline{2 \wedge 16 \wedge 8}$$

$$\underline{2 \wedge 8}$$

Rep. c'est 2.

Vocabulaire:

Dans l'arithmétique des entiers.

Si $a_1 \wedge \dots \wedge a_n = 1$, on dit que $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble.

Voc :

1) Dans l'arithm des polynômes :

Si $A_1 \wedge \dots \wedge A_n = 1$, on dit que les polynômes $A_1, \dots, A_n$ sont **premiers** entre eux dans leur ensemble.

2) $(A_1, \dots, A_n \text{ premier entre eux 2 à 2}) \Rightarrow (A_1, \dots, A_n \text{ premiers entre eux dans leur ensemble})$

Car $A_1 \wedge A_2 \wedge \dots \wedge A_n = 1 \wedge (A_3 \wedge \dots \wedge A_n) = 1$
la réciproque est en générale fausse.

Vocabulaire:

Si $A \wedge B = 1$, on dit que A et B sont **premiers entre eux**.

Prop (Thm de Bezout)

1) $A \wedge B = 1 \Leftrightarrow \exists u, v \in K[X], Au + Bv = 1$

2) $A_1 \wedge \dots \wedge A_n = 1 \Leftrightarrow \exists u_1, \dots, u_n \in K[X], \sum_{i=1}^n A_i u_i = 1$

Prop : $\forall a \neq b, (x-a) \wedge (x-b) = 1$

Démo : $(x-a) - (x-b) = (b-a)$

$$\Rightarrow \frac{1}{b-a} (x-a) - \frac{1}{b-a} (x-b) = 1$$

Bézout $\Rightarrow (x-a) \wedge (x-b) = 1$

Prop :

Si $A \wedge B = 1$ alors $A^m \wedge B^s = 1$

et ce, pour tout $m, s \in \mathbb{N}$.

Corollaire :

Si $a_1, \dots, a_n \in \mathbb{K}$ distincts 2 à 2, alors

$(x-a_1)^{s_1}, \dots, (x-a_n)^{s_n}$ sont 2 à 2 premiers entre eux, et ce pour tout $s_1, \dots, s_n \in \mathbb{N}$.

Démo :

$\forall i \neq j, (x-a_i) \wedge (x-a_j) = 1$ car $a_i \neq a_j$.

$$\Rightarrow (x-a_i)^{s_i} \wedge (x-a_j)^{s_j} = 1$$

Prop : Lemme d'Euclide :
Si $(A/P, B/P, A \wedge B = 1)$ alors AB/P .

Prop (Lemme de Gauss) :
Si $\begin{cases} A/(BC) \\ A \wedge B = 1 \end{cases}$ alors A/C

Question : Quels sont les polynômes divisant 1?
Rep :

$$P/1 \Leftrightarrow P \equiv 1 \Leftrightarrow \exists \lambda \in K^*, P = \lambda \cdot 1 \\ \Leftrightarrow P \in K^*$$

Prop :
Les éléments inversibles de l'anneau $(K[x], +, \cdot)$ sont les polynômes constants non nuls.
Càd $\bigcup (K[x]) = K^*$

NB : $P(x) = \prod_{i=1}^n (x - a_i)^{m_i}$, m_i multiplicité de a_i
 $Q(x) = \prod_{i=1}^n (x - a_i)^{r_i}$, r_i multiplicité de a_i

On a $P/Q \Leftrightarrow \forall i \in [1, n], m_i \leq r_i$

Prop

Deux polynômes de $\mathbb{C}[X]$ sont premiers entre eux si et seulement s'ils n'ont pas de racine commune.

Démo

(En bref)
Supp que $P(x) = \prod_{i=1}^n (x - x_i)$ et $Q(x) = \prod_{i=1}^m (x - y_i)$.

C'est la décomposition de P et de Q .

$$P \wedge Q = 1 \Leftrightarrow (\forall i \in \llbracket 1, n \rrbracket, (x - x_i) \nmid Q)$$

$$\Leftrightarrow (\forall i \in \llbracket 1, n \rrbracket, Q(x_i) \neq 0)$$

$$\Leftrightarrow (P \text{ et } Q \text{ n'ont aucune racine commune})$$



Exemple très classique (à savoir )

Soit $P \in \mathbb{C}[X]$ de degré ≥ 1 .

Montrer que :

Toutes les racines de P sont simples si et seulement si

P et P' sont premiers entre eux.

Solution

Notons $n = \deg(P) \geq 1$, et $\alpha_1, \dots, \alpha_n$ les racines de P .

On a :

$$\left(\text{Toutes les racines de } P \text{ sont simples} \right) \Leftrightarrow \left(\forall 1 \leq i \leq n, P'(\alpha_i) \neq 0 \right)$$

$$\Leftrightarrow \left(\forall 1 \leq i \leq n, \alpha_i \text{ n'est pas une racine de } P' \right)$$

$$\Leftrightarrow P \text{ et } P' \text{ n'ont aucune racine commune}$$

$$\Leftrightarrow P \wedge P' = 1$$



FIN