# Polynômes

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

## I. Generalites

### 1/ Définitions et exemples

**Déf 1:**
On appelle polynôme à coefficients dans $\mathbb{K}$ toute expression de la forme

$$P(X) = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n$$

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 coéfficients 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 polynomes 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 ssi tous ses coéff sont nuls.

**NB :** Soit $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{K}[X]$

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

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

## Déf 3 : (degré)

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

Soit $P(x) = a_0 + a_1 X + \cdots + a_n x^n$

supp $\boxed{P(x) \neq 0}$.

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

**Notation :** $\deg(P)$ ou $d^\circ(P)$

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

**NB :**

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

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

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

**Réflexe 1 :**

1/ $\deg(P) = -\infty \iff P = 0$

2/ $\deg(P) = 0 \iff (\exists\, c \in \mathbb{K}^* / \underbrace{P(x) = c}_{\text{cste non nul}})$

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

4/ $\deg(P)=2 \iff \left(\begin{array}{l}\exists(a,b,c)\in \mathbb{K}\times\mathbb{K}\times\mathbb{K}^* \text{ tel que} \\ P(X)=a+bX+cX^2\end{array}\right)$

5/ Soit $n\in\mathbb{N}$

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

---

**Réflexe 2 :**

1/ $\deg(P)\leq 0 \iff (\exists c\in\mathbb{K} \,/\, P(X)=c)$

2/ $\deg(P)\leq 1 \iff (\exists (a,b)\in\mathbb{K}^2 \,/\, P(X)=a+bX)$

3/ $\deg(P)\leq 2 \iff (\exists (a,b,c)\in\mathbb{K}^3 \,/\, P(X)=a+bX+cX^2$

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

---

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

$P(X)=a_0+a_1X+\dots+a_nX^n$ (où $a_n\neq 0$)

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

En effet :

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

---

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

1/ $P(X)=0 \iff \forall k\in\mathbb{N},\ a_k=0$

2/ $P(X)=Q(X) \iff \forall k\in\mathbb{N},\ a_k=b_k$.

---

**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 $cd(P)=1$, on dit que $P(x)$ est un polynôme unitaire

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

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

$\mathbb{K}_n[X]$ : L'ensemble des polynômes de degrés $\leq n$

<< Attention : non pas $=n$ >>

Ex

1/ $X^2-3X+1\in\mathbb{R}_2[X]$ et $\in\mathbb{C}_2[X]$.

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/ Operations 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 $Q(X)=\sum_{k=0}^{+\infty} b_k X^k$

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

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

**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 :**

$$P(X)=a_0+a_1X+a_2X^2,\ Q(X)=b_0+b_1X$$

1/ Avec le lycée, on a :

$$P(X)Q(X)=a_0b_0+(a_0b_1+a_1b_0)X+(a_2b_0+a_1b_1)X^2+a_2b_1X^3$$

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 $= k$

$c_0 = a_0 b_0$ ; $c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 \cancel{b_2} + a_1 b_1 + a_2 b_0 = a_1 b_1 + a_2 b_0$

$c_3 = a_0 \cancel{b_3} + a_1 \cancel{b_2} + a_2 b_1 + \cancel{a_3} b_0 = a_2 b_1$.

$c_4 = a_0 \cancel{b_4} + a_1 \cancel{b_3} + a_2 \cancel{b_2} + \cancel{a_3} b_1 + \cancel{a_4} b_0 = 0$

4c : $P(X)Q(X) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + (a_1 b_1 + a_2 b_0)X^2 + a_2 b_1 X^3$

On retrouve le m̂ résultat.

---

**Ex d'appli :**

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

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

---

## 3) Propriétés du degré.

**Prop 1 :**

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

2) Si $\deg(P) \neq \deg(Q)$ alors
$\deg(P+Q) = \max(d^\circ(P), d^\circ(Q))$

---

**Ex :** $P(X) = 2 + X + X^2$ ; $Q(X) = 3 + X + 2X^2$

$R(X) = 2 + 3X - X^2$ ; $T(X) = 2 + 3X + X^2 - X^3$.

1/ $\underbrace{\deg(P+Q)}_{2} \underset{=}{<} \underbrace{\max(\deg(P), \deg(Q))}_{2}$.

2/ $\underbrace{\deg(P+R)}_{1} \underset{<}{\leq} \underbrace{\max(\deg(P), \deg(R))}_{2}$

3/ $\underbrace{\deg(P+T)}_{3} \underset{=}{\leq} \underbrace{\max(\deg(P), \deg(T))}_{3}$.

---

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

1/ $\begin{pmatrix} \deg(P) \leq n \\ \deg(Q) \leq n \end{pmatrix} \Rightarrow d^\circ(P+Q) \leq n$

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

---

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

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

**Conventions :**

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

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

---

**Démo :**

1/ Si $(P = 0$ ou $Q = 0)$
l'égalité est vraie : $d^\circ(P \cdot Q) = d^\circ(P) + d^\circ(Q) = -\infty$
vu la convention.

2/ Si $(P \neq 0$ et $Q \neq 0)$.
On a $d^\circ(P) = r \in \mathbb{N}$, $d^\circ(Q) = s \in \mathbb{N}$.
On a :
$$P(X) = \sum_{k=0}^{+\infty} a_k X^k \quad \text{où} \quad \begin{cases} a_r \neq 0 \\ \forall k \geq r+1, a_k = 0 \end{cases}$$

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

On veut montrer que $\boxed{d^\circ(P(X)\,Q(X)) = d^\circ(P) + d^\circ(Q) = r+s}$

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

$$\begin{cases} a) \quad C_{r+s} \neq 0 \\ b) \quad \forall n \geq r+s+1 \text{ , } C_n = 0 \end{cases}$$

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

$$\begin{aligned} C_{r+s} &= \sum_{k=0}^{r+s} a_k b_{r+s-k} \\ &= \sum_{k=r+1}^{r+s} \underbrace{a_k}_{=0} b_{r+s-k} + \sum_{k=0}^{r} a_k b_{r+s-k} \\ &= \sum_{k=0}^{r} a_k b_{r+s-k} \qquad (\text{Car } \forall k \geq r+1,\ a_k = 0) \\ &= \sum_{k=0}^{r-1} a_k \underbrace{b_{r+s-k}}_{=0} + a_r b_s \end{aligned}$$

Or : $r+s-k \geq s+1 \iff k \leq r-1$

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

---

b) Soit $n \geq r+s+1$ Mq $C_n = 0$

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

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

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

Car : $k \leq r \Rightarrow n-k \geq n-r \geq s+1$ | $n \geq r+s+1$ ; $\forall k \geq s+1 , b_k = 0$

Ainsi : $\boxed{C_n = 0}$ □

---

## Corollaire 4

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

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

---

## Démo

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

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

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

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

□

---

## 4/ 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/ $(\alpha.P)\times Q = P\times(\alpha.Q) = \alpha.(P\times Q)$

**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 .

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

**Prop 3 :**

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

## 5/ Fonction polynomiale

**Déf :** soit $P(X)=\sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.
La fonction polynomiale associée à $P$ est notée $\widetilde{P}$ et est définie de $\mathbb{K}$ vers $\mathbb{K}$ par :

$$\widetilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$$
$$x \longmapsto \widetilde{P}(x)=\sum_{k=0}^{n} a_k x^k$$

**NB$_1$ :**

1/ $\widetilde{P}$ se lit "P tilde"
2/ si $P(X)=2X+1$
"$P(1)$" n'est à présent pas défini par contre $\widetilde{P}(1)=3$

**NB$_2$ :** Dorénavant, on confondra polynôme $P$ avec sa fonction polynomiale $\widetilde{P}$.
Ainsi pour $\alpha \in \mathbb{K}$, on écrira $P(\alpha)$ pour désigner $\widetilde{P}(\alpha)$.

**Par exemple :** soit $n \in \mathbb{N}^*$. Posons $P(X) = X^n - 1$

$$\forall k \in \mathbb{Z},\ P\left(e^{\frac{2k\pi i}{n}}\right) = 0$$

## 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)

$d°(P') = -\infty$

**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 $n \in \mathbb{N}$ ; $P, Q \in \mathbb{K}[X]$.

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

(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 :

$$(X^n)^{(k)} = n \cdots (n-k+1) X^{n-k}$$

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

2/ $(X^n)^{(n)} = n!$

3/ $\forall k > n \;;\quad (X^n)^{(k)} = 0$

**NB :** Il faut savoir retrouver $(X^n)^{(k)} = \cdots\cdots$

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

1/ $$\left((X+a)^n\right)^{(k)} = \frac{n!}{(n-k)!} (X+a)^{n-k}$$

2/ $$\left((a-X)^n\right)^{(k)} = (-1)^k \frac{n!}{(n-k)!} (a-X)^{n-k}$$

3/ $$\left((a+bX)^n\right)^{(k)} = b^k \frac{n!}{(n-k)!} (a+bX)^{n-k}$$

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

1) $P(X) = a_0 + \cdots + a_n X^n \Longrightarrow P^{(n)}(X) = a_n \cdot n!$

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

**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

**Déf 1 :** Soient $A$ et $B \in \mathbb{K}[X]$.
On dit que $A$ *divise* $B$ si et ssi

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

**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 $(X^2-1) = (X-1).(X+1)$

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 $X^n-1 = \prod_{k=0}^{n-1}(X-e^{2k\pi i/n})$

---

## Prop2

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

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

i) $\lambda / A$.

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

3/ $(A/B$ et $B/C) \Rightarrow A/C$

4/ $\begin{pmatrix} A/B \\ A/C \end{pmatrix} \Rightarrow A/(B \pm C)$

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

où $\lambda_1,\dots,\lambda_n \in \mathbb{K}$.

6/ $\begin{pmatrix} A/B \\ C/D \end{pmatrix} \Rightarrow AC/BD$

7/ $A/B \Rightarrow \forall k\in\mathbb{N},\ A^k/B^k$

8/ $\forall k\in[\![1,n]\!],\ A_k/B_k \Rightarrow \prod_{k=1}^{n}A_k / \prod_{k=1}^{n}B_k$

Notation : $[\![1,n]\!]=\{1,2,\dots,n\}$

---

**Prop3 :** Soient $B\in\mathbb{K}[X]\setminus\{0\}$ et $A\in\mathbb{K}[X]$.

$A/B \Rightarrow \deg(A)\leq\deg(B)$.

---

NB : Il faut que B soit non nul :

on a $X/0$ mais $d^\circ(X)=1 \not\leq d^\circ(0)=-\infty$

---

Démo de prop 3 :

Supp $A/B$ et $B\neq 0$

$\Rightarrow \exists Q\in\mathbb{K}[X] /\ B=A.Q$.

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

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

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

---

**Prop4 :** Soient $A$ et $B\in\mathbb{K}[X]\setminus\{0\}$

Les assertions suivantes sont équivalentes:

1/ $A/B$ et $B/A$

2/ $\exists\lambda\in\mathbb{K}^*\ B=\lambda A$

3/ $\exists\mu\in\mathbb{K}^*, A=\mu B$

---

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

**1) $\Rightarrow$ 2)**

Supp $A/B$ et $B/A$

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

$\Rightarrow d°(B) = d°(Q) + d°(A)$ $(\Omega)$

D'autre par

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

$\Rightarrow d°(A) = d°(B)$.

et $(\Omega) \Rightarrow d°(Q) = 0$ càd polynôme cst non nul

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

Ainsi $\boxed{B = \lambda A}$ □

**2) $\Rightarrow$ 3)**

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

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

**3) $\Rightarrow$ 1)**

supp que $A = \mu B$ où $\mu \in \mathbb{K}^*$.

Alors $\begin{cases} A = \mu B \\ B = \frac{1}{\mu} A \end{cases} \Rightarrow \begin{cases} A/B \\ B/A \end{cases}$. □

---

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

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

$A/B$ et $B/A$

---

**Notation :** $A \equiv B$

**Exo :** M que $\equiv$ est une relation d'équivalence sur $\mathbb{K}[X] \setminus \{0\}$

---

## 2/ Division euclidienne :

**Prop 1 : (Thm de la div eucli)**

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

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

1/ $A = BQ + R$

2/ $d°(R) < d°(B)$

**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 :**

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

**Exemples :** Déterminer le reste de la div euclidienne de $X^{2020}$ par :

1/ $(X-1)$

2/ $(X^2-1)$

3/ $(X-i)$

4/ $(X-1)^2$

5/ $(X+1)(X-1)^2$

6/ $(X^2+1)$

**Sol :**

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

On a : $d°(R) < d°(X-1)$

Déterminons le reste $R(X)$ :

$d°(R) < 1 \iff d°(R) \leq 0$

$\iff \exists c \in \mathbb{K}, R(X) = c$

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

Pour $X=1$ on obtient $1=c$

C/c : Le reste de la div euclid de $X^{2020}$ par $(X-1)$ est 1.

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

$d°(R) < d°(X^2-1) = 2$

On a $d°(R) \leq 1 \iff R(X) = a + bX$

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

$X^{2020} = (X^2-1)Q(X) + a + bX$. On prend pour $X = 1$ et $X = -1$.

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

C/c $\boxed{\text{Le reste de la div euclid de } X^{2020} \text{ par } (X^2-1) \text{ est } R(X) = 1.}$

4/ $X^{2020} = (X-1)^2 Q(X) + R(X)$

avec $d°(R) < d°((X-1)^2) = 2$

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

Ainsi $X^{2020} = (X-1)^2 Q(X) + a + bX$ $(\Omega)$

$X=1$ dans $(\Omega) \Rightarrow a+b=1$

On a besoin d'une autre équation.

En dérivant, on obtient :

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

$X=1 \Rightarrow 2020 = b$

d'où $a = -2019$

C/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 $\begin{cases} a = 1 \\ b = 0 \end{cases}$ ; « égalité de deux complexes »

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

---

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

$B / A \iff R = 0$

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

---

**Ex d'appli :**

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

---

**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 $b \in \mathbb{R}$.

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

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

$\Rightarrow a + bi = 0$

$\Rightarrow (a = 0$ et $b = 0)$ ; « Nombre complexe nul »

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

càd $(X^2+1) / P(X)$.

---

## III – Racines d'un polynome :

### 1/ Généralités

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

**Exemple :** (à retenir)
$n \geq 2$ et $P(X) = X^n - 1$.
Les racines complexes de $(X^n - 1)$ sont exactement les racines $n^{ème}$ de l'unité.
en effet :
Soit $a \in \mathbb{C}$.
$$P(a) = 0 \iff a^n = 1$$
$$\iff a \in \mathbb{U}_n$$
où $\mathbb{U}_n$ est l'ensemble des racines nème 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 $P(a)$.

**Démo :** $P(X) = (X - a)Q(X) + R(X)$.
où $d°(R) < 1$. Posons $R(X) = C$.
$$P(X) = (X - a)Q(X) + C$$
pour $X = a \Rightarrow C = P(a)$

**Corollaire 3 :**
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
$$P(a) = 0 \iff (X - a) / P.$$

**Démo :** $P(a) = 0 \iff$ (Le reste de la div euclid de $P$ par $(X-a)$ est nul)
$$\iff (X - a) / P.$$

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 évidement $7, 8, 9$.

1) Pour la racine $9$

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 $8$ :

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 $7$ :

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

$7$ est dite racine de multiplicité $1$ de $P$.

En général, on a la déf suivante :

**Déf 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

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

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/ $(X-a)^m / P$

**Exemple introductif :**

$P(X) = (X-1)^2$, on a $m=2$ est 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/

On a : $\begin{cases} P(X) = (X-a)^m Q(X) \\ \text{avec } Q(a) \neq 0 \end{cases}$

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

$$P^{(k)}(X) = \left((X-a)^m Q(X)\right)^{(k)}$$
$$= \sum_{i=0}^{k} C_k^i \left((X-a)^m\right)^{(i)} Q(X)^{(k-i)}$$

$$\left((X-a)^m\right)^{(i)} = \frac{m!}{(m-i)!}(X-a)^{m-i}$$

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

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

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

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

Càd si $i \leq m-1$.

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

2) $\Rightarrow$ 1) Par récurrence sur $m \geq 1$.

---

**Prop 5 :**

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

$$(X-a)^m / P \iff \left(\forall\, 0 \leq k \leq m-1,\ P^{(k)}(a) = 0\right)$$

---

**Démo :**

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

Réflexe à avoir :

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

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

---

**Ex :** Déterminons le reste de la div euclidi de $X^{2020}$ par $(X-1)^3$

---

**Sol :**

$$X^{2020} = \underbrace{(X-1)^3 Q(X)}_{\text{noté } T(X)} + \left(a + bX + cX^2\right)$$

On a $T(X) = (X-1)^3 Q(X)$

$$\Longrightarrow \quad T(1) = T'(1) = T''(1) = 0$$

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

C/C : Le reste voulu est $\boxed{R(x) = \sim\sim\sim}$ □

Exo (TD)

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

Mque $X^2 \,/\, \left((X+1)^n - nX - 1\right)$

Solution

Notons $P(X) = (X+1)^n - nX - 1$

On veut M.que $X^2 / P$.

On a : $X^2 / P \Longleftrightarrow \left(P(0) = 0 \text{ et } P'(0) = 0\right)$

i) On a $P(0) = 1 - 1 = 0$

ii) $P'(X) = n(X+1)^{n-1} - n$

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

D'où $\boxed{X^2 / P}$ □

## 3| Nombre de racines d'un polynôme.

**Prop 1 :** Soient $P(X) \in \mathbb{K}[X]$ et $x_1 \neq x_2 \in \mathbb{K}$.

$$\left(P(x_1) = P(x_2) = 0\right) \Longleftrightarrow (X - x_1)(X - x_2) / P(X)$$

**Démo :**

$(\Leftarrow)$ évident.

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

Mque $(X - x_1)(X - x_2) / P(X)$

On a : $P(x_1) = 0 \Rightarrow \exists Q \in \mathbb{R}[X] \; ; \; P(X) = (X - x_1) Q(X)$

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

$\Rightarrow Q(x_2) = 0$ (car $x_1 \neq x_2$)

$\Rightarrow \exists T(X) \in \mathbb{K}[X] \; , \; Q(X) = (X - x_2) \cdot T(X)$.

D'où $P(X) = (X - x_1)(X - x_2) T(X)$.

Alors $(X - x_1)(X - x_2) / P(X)$.

En général, on a la prop suivante :

**Prop 2 :** soit $n \geq 2$. Soient $x_1, \dots, x_n \in \mathbb{K}$ distincts deux à deux on a :

$$\left(P(x_1) = \dots = P(x_n) = 0\right) \Longleftrightarrow \left((X - x_1) \dots (X - x_n) / P(X)\right)$$

**Démo :** ($\Leftarrow$) 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 mque
$P(a)=0$ et $P(b)=0$

**Exercice :**
Mque : $(X^2-3X+2) \mid T(X)$ où
$T(X) = X^4 - 3X^3 + 3X^2 - 3X + 2$.

**Sol :** Mque $(X-1)(X-2) \mid T(X)$
Il suffit de mque $T(1)=0$ et $T(2)=0$ car $1 \neq 2$

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

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

**Démo :** Posons $P(X) = \sum_{k=0}^{n} a_k X^k$, les $a_k \in \mathbb{R}$.
On a :

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

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

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

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

Attention ! Si $P \notin \mathbb{R}[X]$, c'est FAUX
C-exemple :
$P(X) = X - i$
$i$ 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 $\omega$ alors il a $\omega$ et $\bar{\omega}$ comme racines.

**Ex d'appli :**

Redémontrons que :

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

**Sol :** On a :

$$(x^2+1) / T(x) \underset{i \neq -i}{\Longleftrightarrow} (x-i)(x+i) / T(x)$$
$$\Longleftrightarrow T(i) = 0 \text{ et } T(-i) = 0$$
$$\Longleftrightarrow T(i) = 0$$

car $\bar{i} = -i$ et $T$ à coeff réels,

et on a $T(i) = 0$

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

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

**Démo :**

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

Soient $x_1, \dots, x_s$, les $s$ racines distinctes de $P$.

Il s'agit de mque $s \leq n$

On a $(X - x_1) \dots (X - x_s) / P(X)$

$$\Rightarrow d^\circ(\underbrace{(X-x_1)\cdots(X-x_p)}_{=p}) \leq \underbrace{d^\circ(P(X))}_{\leq n}$$

d'où $p \leq n$

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

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

Alors $\boxed{P = 0}$

**Démo :** En bref (Par l'absurde)

Supp que $P \neq 0$

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

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

**Réflexes**

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

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'applic (Extrait CNC)

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

Soient $x_0, x_1, \dots, x_n$ des réels 2 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 $\phi(P) = (0, 0, \dots, 0)$

Mque : $P = 0$

## Solution :

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

Mque : $P = 0$

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

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

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

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

Par suite $\boxed{P = 0}$ $\square$

## Corollaire 5

Un polynôme ayant une infinité de racines est nul.

### Ex d'appli : (TD)

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

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

Mque $U = 0$ et $V = 0$

## 4/ Cas des racines complexes :

**Prop 1 (Théorème de d'Alembert-Gauss)**

Tout polynôme de degré $\geq 1$ admet au moins une racine complexe.

**Démo :** hors programme

**Corollaire 2 :**

Tout polynôme de degré $\geq 1$ est divisible par un polynôme complexe de degré 1.

Démo :

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 $\geq 1$ et n'a aucune racine réelle.

# IV Polynômes irréductibles.

## 1/ Généralité :

Def 1 :

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

$P$ est dit irréductible dans $\mathbb{K}[X]$ si et ssi :

1/ $d°(P) \geq 1$

2/ Les seuls diviseurs de $P$ dans $\mathbb{K}[X]$ sont ses associés et les polynômes constants non nuls.

NB$_1$ :

2/ Veut dire que ses seuls diviseurs sont de la forme $(\lambda P)$ et $\mu$ où $\lambda$ et $\mu \in \mathbb{K}^*$.

NB$_2$ :

Pour tout $\lambda \in \mathbb{K}$, $\lambda$ n'est pas irréductibles.

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 $\underbrace{(x-1)}_{\in \mathbb{C}[X]} / (x^2-1)$

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 :

$$P(X) = aX^2 + bX + c \quad (a,b,c) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}.$$

$\Delta < 0$.

$\Rightarrow$ 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 $\geq 2$ 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 $d^\circ(P) \geq 2$

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

$\Longrightarrow (x-\alpha) / P(x)$.

2) et 3) 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 $P \in \mathbb{R}[X]$.

$\longrightarrow$ Si $d°(P) \leq 0$ ; $P$ n'est pas irréductible dans $\mathbb{R}[X]$.

$\longrightarrow$ Si $d°(P) = 1$ : $P$ est irréductible dans $\mathbb{R}[X]$ (déjà vu)

$\longrightarrow$ Si $d°(P) = 2$ ;

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

$\longrightarrow$ Si $\Delta \geq 0$ :

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

car $P$ possède une racine réelle $\alpha$

et donc $(X-\alpha) / P$.

3| si $d°(P) \geq 3$.

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 $(X-\alpha) \ / \ P(X)$.

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

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

on a $\begin{cases} P(\alpha) = 0 \\ P(\bar{\alpha}) = 0 \end{cases}$ car $P$ à coeff réels.

or $\alpha \neq \bar{\alpha}$. (Car $\alpha \notin \mathbb{R}$)

$\boxed{\begin{matrix} \bar{z} = z \Leftrightarrow z \in \mathbb{R} \\ \bar{z} \neq z \Leftrightarrow z \notin \mathbb{R} \end{matrix}}$

Rappel

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

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

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

---

3| 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/ $X^3 - 1$ :

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

a/ Dans $\mathbb{R}$.

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

b/ Dans $\mathbb{C}$.

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

**Rapel :**

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

Soit $n \geq 2$. On a :

1) Les racines complexes de $(X^n - 1)$ sont les racines nème de l'unité ; càd :

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

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

à retenir

D'une manière générale, on a :

**Prop 1 :**

1/ Tout polynôme $P \in \mathbb{K}[X]$, de degré $\geq 1$ s'écrit sous la forme :

$$P = \lambda P_1 \cdots P_r$$

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

---

NB : $\lambda = cd(P)$.

NB$_1$ : Décomposition dans $\mathbb{C}$.

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

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

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

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

$a_1, \ldots, a_s$ les racines de $P$ 2 à 2 distincts entre eux.

$m_i$ étant la multiplicité de la racine $a_i$.

**$NB_2$ : 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 $\lambda = cd(P)$, $d^\circ(P) = \sum_{l=1}^{s} m_i + \sum_{k=1}^{r} 2n_k$.
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

**Déf 1** Un polynôme $P \in \mathbb{K}[X]$ est dit scindé dans $\mathbb{K}$ si et ssi :

1/ $\deg(P) \geq 1$.
2/ $P$ s'écrit comme produit de polynômes de degrés 1 et à coéfficients dans $\mathbb{K}$.

**Exemples rapides :**

1/ $(X^2 - 1) = (X-1)(X+1)$
$(X^2 - 1)$ est scindé dans $\mathbb{R}$ et dans $\mathbb{C}$.

2/ $X^2 + 1 = (X - i)(X + i)$
$(X^2 + 1)$ est scindé dans $\mathbb{C}$ mais pas dans $\mathbb{R}$.

**Prop 2 :**

Dans $\mathbb{C}$, tout polynôme de degré $\geq 1$ est scindé.

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

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

1/ $P$ s'écrit sous la forme :

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

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

2/ $P$ s'écrit aussi sous la forme

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

où : $\begin{cases} \lambda \text{ et les } a_i \in \mathbb{K}. \\ d^\circ(P) = \sum_{i=1}^{s} m_i \\ a_1, \dots, a_s \text{ sont les racines de } P \text{ distinctes } 2 \text{ à } 2 \end{cases}$

$m_i$ = la multiplicité de la racine $a_i$.

## 2/ Relations de Viète entre les racines et les coeff d'un polynôme scindé

**Lemme :**

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

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

**Démo :** par récurrence sur $n \geq 1$ (À faire).

**Prop 1 :**

Soit $n \geq 1$

Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ de degré $n$, scindé dans $\mathbb{K}$.

Soient $x_1, \ldots, x_n$ ses racines, non forcement distincts 2 à 2. On a :

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

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

**Démo :**

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

d'après le Lemme, on a alors.

$P(X) = a_0 + \cdots + a_{n-1} X^{n-1} + a_n X^n$.

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

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

$\frac{1}{(-1)^n} = (-1)^n$ 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)** $x_1, x_2$ 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 :** $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$.

$\sigma_3 = x_1x_2x_3$.

**Q)** $x_1, x_2, x_3$ 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 :** $\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$

$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$.

$\sigma_4 = x_1x_2x_3x_4$.

**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 :

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

NB :

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

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

2) Pour $k=n$.

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

## VI 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 :**

Posons $P(X) = \displaystyle\sum_{k=0}^{+\infty} a_k X^k$, soit $n\in\mathbb{N}$.

On a $P^{(n)}(X) = \displaystyle\sum_{k=n}^{+\infty} k(k-1)\cdots(k-n+1) a_k X^{k-n}$

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

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

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.

$$P(X+a)=\sum_{k=0}^{+\infty}\frac{P^{(k)}(a)}{k!}X^k \qquad \text{CQFD}$$

## 2) Composition de polynômes.

Déf 1 :

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

$$(P\circ Q)(X)\overset{\text{déf}}{=}\sum_{k=0}^{+\infty}a_k\,(Q(X))^k.$$

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

$$P(X)=a_0+a_1X+\cdots+a_nX^n \quad (a_n\neq 0).$$

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 $a \neq 0$.

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

## 3) Polynôme d'interpolation de Lagrange

**Notation :** $n \in \mathbb{N}^*$, $a_0, \dots, a_n \in \mathbb{K}$, distincts 2 à 2. Pour $k \in [\![0,n]\!]$, 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 $k \in [\![0,n]\!]$, $L_k(X)$ est un polynôme de degré $n$.

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

## 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 :

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

## 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

$$\forall k \in [\![0,n]\!], P(a_k) = y_k$$

2) Ce polynôme $P$ est exactement :

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

## Démo

### 1) i) Unicité

Soient $P$ et $Q \in \mathbb{K}_n[X]$ 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 $P = Q$ ; càd M.que $P - Q = 0$

On a $P$ et $Q \in \mathbb{K}_n[X]$ alors $(P-Q) \in \mathbb{K}_n[X]$

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

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

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

D'où $\boxed{P - Q = 0}$ $\square$

### ii) Existence

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

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

Car $\forall 0 \leq j \leq n,\ L_j(X) \in \mathbb{K}_n[X]$ $(\deg(L_j(X)) = n \leq n)$

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

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

$$\boxed{\begin{array}{l} L_j(a_k) = 0 \text{ si } j \neq k \\ L_j(a_k) = 1 \text{ si } j = k \end{array}}$$

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

$= y_k L_k(a_k)$ (car $\forall j \neq k, L_j(a_k) = 0$)

$= y_k$ $\square$ ($L_k(a_k) = 1$)

NB : On verra plus loin une démo plus rapide

NB : (à montrer)

Les polynômes $T \in \mathbb{K}[X]$ vérifiant :
$\forall i \in [\![0,n]\!], T(a_i) = y_i$.
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 $Q \in \mathbb{K}[X]$, 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 $A | B$ alors

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

ii) $A$ est un pgcd de $A$ et $B$.

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

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

3/ On a L'algorithme d'Euclide qui est analogue à celui pour les entiers.
Il donne un pgcd.

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

5/ Si D est un pgcd de A et B, alors il existe U et $V \in \mathbb{K}[X]$ tels que :

$$AU + BV = D.$$

---

## 2/ PPCM de deux polynômes non nuls.

---

**Déf 1 :** Soient $P$ et $Q \in \mathbb{K}[X] \setminus \{0\}$.
Le ppcm 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) :**

1/ $(2X) \vee (3X^2) = X^2$.

2/ $A / B \Longrightarrow A \vee B = \dfrac{B}{cd/B}$.

3/ $\begin{cases} P/A \\ Q/A \end{cases} \Longrightarrow P \vee Q / A$

4/ $(A \wedge B) \cdot (A \vee B) \equiv AB$
associé !

Pause : Soient $\lambda$ et $\mu$ deux polynômes constants non nuls
1/ On a $\lambda / \mu$
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 $(A_1 \wedge \ldots \wedge A_n)$, le pgcd de $A_1, \ldots, A_n$.
C'est défini d'une manière récurrente.

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

Exemple express.
Concernant l'arith des entiers que vaut

$$\underbrace{\underbrace{6 \wedge 26}_{2} \wedge 16}_{2} \wedge 8$$

$$\underbrace{2 \wedge 16}_{2} \wedge 8$$

$$2 \wedge 8$$

Rep : c'est 2.

**Vocabulaire :**

Dans l'arithmetique des entiers.
si $a_1 \wedge \dots \wedge a_n = 1$, on dit que $a_1, \dots, a_n$ sont premiers entre eux dans leurs 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/ $\begin{pmatrix} A_1, \dots, A_n \text{ premier} \\ \text{entr eux 2 à 2} \end{pmatrix} \Rightarrow \begin{pmatrix} A_1, \dots, A_n \text{ premiers entre} \\ \text{eux dans leur ensembles} \end{pmatrix}$

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/ $A \wedge B = 1 \Leftrightarrow \exists U, V \in \mathbb{K}[X], AU + BV = 1$

2/ $A_1 \wedge \dots \wedge A_n = 1 \Leftrightarrow \exists U_1, \dots, U_n \in \mathbb{K}[X], \sum_{i=1}^{n} A_i U_i = 1$

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

**Démo :** $(X-a)-(X-b)=(b-a)$

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

Bezout $\Rightarrow (X-a) \wedge (X-b) = 1$

**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 :**

$$P/1 \iff P \equiv 1 \iff \exists \lambda \in \mathbb{K}^*, P = \lambda.1.$$
$$\iff P \in \mathbb{K}^*$$

**Prop :**

Les éléments inversibles de l'anneau $(\mathbb{K}[X], +, \times)$.
sont les polynômes constants non nuls.

C.à.d $U(\mathbb{K}[X]) = \mathbb{K}^*$

**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 : $P/Q \iff \forall i \in [\![1,n]\!], m_i \leq r_i$