Polynômes (à une variable)

Dans tout ce cours $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

I Construction

1) Polynômes

On appelle polynôme à coefficients dans $\mathbb{K}$, en la variable X toute expression formelle du type

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n \ , \ n \in \mathbb{N}.$$

On note $\mathbb{K}[X]$ cet ensemble.

Deux polynômes P et Q dans $\mathbb{K}[X]$ sont dits égaux si et seulement si

$P(X) = \sum_{k=0}^{n} a_k X^k$, $Q(X) = \sum_{k=0}^{m} b_k X^k$ avec

$m = n$ et $\forall k \in \{0, \dots, n\}$ $a_k = b_k$.

Le cas $P(X) = a_0$ est dit polynôme constant

2) L'espace vectoriel des polynômes

Pour $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, $Q(X) = \sum_{k=0}^{m} b_k X^k$, $\lambda \in \mathbb{K}$, on pose

$$\lambda P(X) = \sum_{k=0}^{n} \lambda a_k X^k$$

et $(P+Q)(X) = \sum_{k=0}^{p} (a_k + b_k) X^k$, où $p = \max(m,n)$ et on complète les listes (a_k) et (b_k) par des 0 si nécessaire.

$\mathbb{K}[X]$ devient ainsi un espace vectoriel (cf S2).

3) Degré

Soit $P \in \mathbb{K}[X]$, on appelle degré de P le plus grand entier n tq le coeff. a_n de X^n est non nul.

(Pour $P = 0$, $\deg P = +\infty$).

Prop

$\deg(\lambda P) = \deg P$ (sauf $\lambda = 0 \Rightarrow \deg(\lambda P) = +\infty$).
$\deg(P+Q) \leq \max(\deg P, \deg Q)$.

4) $\mathbb{K}_n[X]$

On note $\mathbb{K}_n[X]$ l'ens. des polynômes $P \in \mathbb{K}[X]$ tq $\deg P \leq n$.

Thm

- $\mathbb{K}_n[X]$ est stable par λ. et par $+$. (c'est un s.e.v. de $\mathbb{K}[X]$)
- La famille $\{1, X, X^2, \dots, X^n\}$ est libre dans $\mathbb{K}_n[X]$, i.e. il n'existe pas de combinaison $\lambda_0 1 + \lambda_1 X + \dots + \lambda_n X^n$ qui donne le polynôme nul, sauf $\lambda_0 = \dots = \lambda_n = 0$.
- Cette famille est génératrice dans $\mathbb{K}_n[X]$, i.e. $\forall P \in \mathbb{K}_n[X]$, il existe $\lambda_0, \dots, \lambda_n \in \mathbb{K}$ tq $P = \lambda_0 1 + \lambda_1 X + \dots + \lambda_n X^n$.

5) L'anneau $\mathbb{K}[X]$.

Pour $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$, on pose $PQ = \sum_{k=0}^{p} c_k X^k$

avec $\boxed{c_k = \sum_{j=0}^{k} a_j b_{k-j}}$ (où on met des 0 si nécessaire aux a_i, b_i).

C'est le produit usuel, naturel, des polynômes :

$$(X^2+X+1)(3X^3-X^2+2) = 3X^5 + (-1+3)X^4 + (3-1)X^3 + (2-1)X^2 + 2X + 2 \text{ etc.}$$

On a $X^n X^m = X^{n+m}$
$1\, P(X) = P(X)$

($\mathbb{K}[X]$ devient alors un anneau commutatif)

Du coup, on peut définir $P^2, \dots, P^n$, pour $P \in \mathbb{K}[X]$.

Notez que l'on a ici aussi :

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

Prop

$$\boxed{\deg(PQ) = \deg P + \deg Q.}$$

Dem

$c_k = \sum_{j=0}^{k} a_j b_{k-j}$. Si $\deg P = p$, $\deg Q = q$ alors $c_k = 0$ pour $k > p+q$

car $a_j b_{k-j} = \begin{cases} a_j \cdot 0 & , \text{ si } 0 \leq j \leq p \Rightarrow k-j > q \\ 0\, b_{k-j} & , \text{ si } j > p \end{cases}$

Ensuite $c_{p+q} = \sum_{j=0}^{p+q} a_j b_{p+q-j} = a_p b_q$ (seul terme non nul) $\neq 0$. ∎

Proposition

- Aucun polynôme P, autre que $P = C \neq 0$, n'est inversible dans $\mathbb{K}[X]$.
- Si $P, Q \in \mathbb{K}[X]$ et $PQ = 0$ alors $P = 0$ ou $Q = 0$
- Si $P, Q, R \in \mathbb{K}[X]$, $P \neq 0$ et si $PR = PQ$, alors $R = Q$.

Dem

- Si $QP = 1 \Rightarrow \deg Q + \deg P = 0 \Rightarrow \deg P = \deg Q = 0$.
- $\deg(PQ) = \deg P + \deg Q$, donc si P et $Q \neq 0 \Rightarrow \deg(PQ) \in \mathbb{N}$, donc $PQ \neq 0$.
- Si $PR = PQ \Rightarrow P(R-Q) = 0 \Rightarrow P = 0$ ou $R - Q = 0$, donc $R - Q = 0$ car $P \neq 0$.

∎

7) Composition de polynômes.

Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q \in \mathbb{K}[X]$, on pose

$$P \circ Q(X) = \sum_{k=0}^{n} a_k Q(X)^k, \quad P \circ Q \in \mathbb{K}[X].$$

Proposition

- $(\lambda P + \mu Q) \circ R = \lambda (P \circ R) + \mu (Q \circ R)$
- $(PQ) \circ R = (P \circ R)(Q \circ R)$

(exercice).

8) Fonctions polynômiales.

On appelle valeur de $P = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{K}[X]$ au point $x \in \mathbb{K}$, le scalaire $P(x) = a_0 + a_1 x + \dots + a_n x^n$.

Proposition

$$(\lambda P + \mu Q)(x) = \lambda P(x) + \mu Q(x)$$
$$(PQ)(x) = P(x)\,Q(x)$$
$$(P \circ Q)(x) = P(Q(x))$$

On appelle racine de $P \in \mathbb{K}[X]$, tout $x \in \mathbb{K}$ tel que $P(x) = 0$.

On appelle fonction polynomiale associée à $P \in \mathbb{K}[X]$, la fonction f, définie sur $\mathbb{K}$, telle que $f(x) = P(x)$, $\forall x \in \mathbb{K}$.

II Dérivation

1) Dérivée première

Soit $P = a_0 + a_1 X + \dots + a_n X^n$, on pose $P' = a_1 + 2a_2 X + \dots + n a_n X^{n-1}$.

$$P = \sum_{k=0}^{n} a_k X^k \Rightarrow P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{k=0}^{n-1} (k+1) a_{k+1} X^k.$$

__Prop__

$$\boxed{\begin{array}{l}\text{Si } P \text{ est constant} \Rightarrow P' = 0 \\ \text{Si } P \text{ est non constant, alors } \deg P' = (\deg P) - 1.\end{array}}$$

__Prop__

$$\boxed{\begin{array}{l}(\lambda P + \mu Q)' = \lambda P' + \mu Q' \\ (PQ)' = P'Q + PQ'\end{array}}$$

__Dem__

Le 1er est ok.

$$(PQ)' = \sum_{k=0}^{r} (k+1) c_{k+1} X^k \Rightarrow (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j}.$$

$$P' = \sum_{k=0}^{n} (k+1) a_{k+1} X^k, \quad Q' = \sum_{\ell=0}^{m} (\ell+1) b_{\ell+1} X^\ell$$

$$P'Q + PQ' \Rightarrow \text{coef } d_k = \sum_{j=0}^{k} (j+1) a_{j+1} b_{k-j} + a_j (k-j+1) b_{k-j+1}$$

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

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

$\square$

__Corollaire__

$$\boxed{\begin{array}{l}(P_1 \cdots P_n)' = \sum_{i=1}^{n} P_1 \cdots P_{i-1} P_i' P_{i+1} \cdots P_n \\ (P^n)' = n P' P^{n-1}.\end{array}}$$

Prop

$$\boxed{(P \circ Q)' = Q' \cdot P' \circ Q.}$$

Dem

$P \circ Q = \sum_{k=0}^{n} a_k Q^k \Rightarrow (P \circ Q)' = \sum_{k=0}^{n} a_k (Q^k)' = \sum_{k=1}^{n} k a_k Q' Q^{k-1}$

$\Rightarrow (P \circ Q)' = Q' \sum_{k=1}^{n} k a_k Q^{k-1} = Q' P'(Q).$ ☐

2) Dérivées d'ordre supérieur.

$P^{(n)}$ etc ...

Prop

$$\boxed{\begin{aligned}(\lambda P + \mu Q)^{(n)} &= \lambda P^{(n)} + \mu Q^{(n)} \\ (PQ)^{(n)} &= \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\end{aligned}}$$

Théorème (Formule de Taylor pour les polynômes)

$\forall P \in \mathbb{K}[X], \forall a \in \mathbb{K}, (n = \deg P)$

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

Dem

Si $P = 0$ ✓.

1) $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k$.

En effet : $P(X) = \sum_{j=0}^{n} a_j X^j \Rightarrow P^{(k)}(X) = \sum_{j=k}^{n} j(j-1)\cdots(j-k+1)\, a_j X^{j-k}$

$$P^{(k)}(0) = k!\, a_k \Rightarrow \boxed{a_k = \frac{P^{(k)}(0)}{k!}}$$

$Q(X) = P(X+a)$ est un polynôme en X aussi, et $Q^{(k)}(X) = P^{(k)}(X+a)$

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

$$P(X+a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} X^k \Rightarrow P(X) = P(X-a+a) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k.$$ ☒

III Arithmétique des polynômes

1) Divisibilité

Un polynôme $P \in \mathbb{K}[X]$ est <u>unitaire</u> si son coeff. dominant est 1.

On dit que $A \in \mathbb{K}[X]$ <u>divise</u> $B \in \mathbb{K}[X]$ si il existe $U \in \mathbb{K}[X]$ tq $B = AU$. On note ça $A \mid B$. On dit que B est un <u>multiple</u> de A.

On note $\mathrm{Div}(A)$ l'ens. des diviseurs de A et $\mathrm{Mult}(A)$ l'ens. des multiples de A.

Exemple : $(X+1) \mid (X^3+X^2+X+1)$ car $X^3+X^2+X+1 = (X+1)(X^2+1)$.

$(X-1) \mid (X^n-1)$ car $X^n - 1 = (X-1)(X^{n-1}+\cdots+X+1)$.

Pour tout $A \in \mathbb{K}[X]$ on a $A \mid 0$.

Les polynômes constants et les λA divisent toujours A.

Si $A = \lambda C$ et $B = \mu D$ alors $A | B \iff C | D$.

Prop

$$\boxed{\begin{array}{l} \text{Si } A|B \text{ et } B|C \Rightarrow A|C \\ \text{Si } A|B \text{ et } B|A \Rightarrow A = \lambda B. \end{array}}$$

Prop

$A|B$ et $B \neq 0 \Rightarrow \deg A \leq \deg B$

$A|B$ et $\deg A = \deg B \Rightarrow A = \lambda B$

$A|B$ et $A|C \Rightarrow A | B+C$

$A|B$ et $C|D \Rightarrow AC | BD$

$A|B \Rightarrow A^n | B^n$

2) Division euclidienne

Thm

Pour tous $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, il existe un unique couple $Q, R \in \mathbb{K}[X]$ tq

$$A = BQ + R \quad \text{avec } \deg R < \deg B.$$

Q est le quotient de la division euclidienne, R est le reste.

Dem

Unicité : Si on a (Q_1, R_1) et (Q_2, R_2) ainsi $\Rightarrow$

$A = Q_1 B + R_1 = Q_2 B + R_2$ avec $\deg R_1, \deg R_2 < \deg B$.

$\Rightarrow B(Q_1 - Q_2) = R_2 - R_1 \Rightarrow B \mid R_2 - R_1$ ce qui est impossible, sauf $R_1 - R_2 = 0$.

Ainsi $R_1 = R_2$. Ensuite $B(Q_1 - Q_2) = 0$ et $B \neq 0 \Rightarrow Q_1 - Q_2 = 0$. ✓

Existence

Soit $p = \deg B$ et b son coeff. dominant. On va montrer par recurrence que pour tout $n \geqslant p$ on a :

$\forall A \in \mathbb{K}_{n-1}[X]$, $\exists (Q, R) \in \mathbb{K}[X]^2$ tq $A = BQ + R$ avec $\deg R < \deg B$.

Pour $n = p$, on prend $Q = 0$ et $R = A$.

Supposons la propriété vraie pour un $n \geqslant p$. Soit $A \in \mathbb{K}_n[X]$, alors

$A = aX^n + \tilde{A}$ avec $\tilde{A} \in \mathbb{K}_{n-1}[X]$.

On a $\frac{a}{b} B X^{n-p} = aX^n + \tilde{B}$ avec $\deg \tilde{B} < n$. Donc

$A = \frac{a}{b} B X^{n-p} + \tilde{A} - \tilde{B}$.

Comme $\deg \tilde{A} - \tilde{B} < n$ on applique l'hyp. de recurrence :

$\tilde{A} - \tilde{B} = \tilde{Q} B + \tilde{R}$ avec $\deg \tilde{R} < p$.

$\Rightarrow A = B\left(\frac{a}{b} X^{n-p} + \tilde{Q}\right) + \tilde{R}$. ∎

Méthode pratique : la division de polynômes :

$$
\begin{array}{rrrrr|l}
X^4 & -3X^3 & +2X^2 & +X & -1 & X^2-X+1 \\
\cline{6-6}
X^4 & -X^3 & +X^2 & & & X^2 \\
\cline{1-3}
 & -2X^3 & +X^2 & +X & -1 & -2X \\
 & -2X^3 & +2X^2 & -2X & & \\
\cline{2-5}
 & & -X^2 & +3X & -1 & -1 \\
 & & -X^2 & +X & -1 & \\
\cline{3-5}
 & & & 2X & &
\end{array}
$$

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

$$
\begin{array}{rrrrrr|l}
X^5 & -X^4 & & -2X^2 & -3X & +1 & X^2+2 \\
\cline{7-7}
X^5 & & +2X^3 & & & & X^3-X^2-2X \\
\cline{1-6}
 & -X^4 & -2X^3 & -2X^2 & -3X & +1 & \\
 & -X^4 & & -2X^2 & & & \\
\cline{2-6}
 & & -2X^3 & & -3X & +1 & \\
 & & -2X^3 & & -4X & & \\
\cline{3-6}
 & & & & X & +1 &
\end{array}
$$

$$X^5-X^4-2X^2-3X+1 = (X^3-X^2-2X)(X^2+2) + X+1.$$

Prop

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. On a $B \mid A \iff$ le reste est 0.

Prop.

a est racine de P si et seulement si $X-a$ divise P.

Dem

$P = (X-a)Q + R$ avec $\deg R < 1$ donc R est un pol. constant.

$P = (X-a)Q + \lambda$

$P(a) = \lambda \Rightarrow R = P(a)$.

Ainsi $(X-a) \mid P \iff P(a) = 0$. $\blacksquare$

$P = X^3 + X^2 - 3X + 1$. On voit que 1 est racine.

$$
\begin{array}{r|l}
X^3 + X^2 - 3X + 1 & X - 1 \\
\cline{2-2}
X^3 - X^2 & X^2 + 2X - 1 \\
\cline{1-1}
2X^2 - 3X + 1 & \\
2X^2 - 2X & \\
\cline{1-1}
-X + 1 & \\
-X + 1 & \\
\cline{1-1}
0 &
\end{array}
$$

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

3) pgcd et ppcm de 2 polynômes.

$\mathrm{Div}(A,B) := \mathrm{Div}(A) \cap \mathrm{Div}(B)$.

Prop

$$\boxed{\text{Si } A = BQ + R \text{ alors } \mathrm{Div}(A,B) = \mathrm{Div}(B,R).}$$

(idem que dans $\mathbb{Z}$).

Thm
Si $A, B \in \mathbb{K}[X]$, il existe un unique polynôme $D \in \mathbb{K}[X]$, unitaire ou nul tq $\mathrm{Div}(A,B) = \mathrm{Div}(D)$.

Dem

Unicité : Si D_1, D_2 ... alors $\mathrm{Div}(D_1) = \mathrm{Div}(D_2) \Rightarrow D_1 | D_2$ et $D_2 | D_1$
$\Rightarrow$ ils sont multiples l'un de l'autre par un scalaire. Mais comme ils sont unitaires $\Rightarrow D_1 = D_2$.

Existence Si $A = B = 0$, alors $D = 0$ convient.
Quitte à échanger A et B on peut supposer $B \neq 0$.

Alors, comme dans $\mathbb{Z}$, algo. d'Euclide :

$A_0 = A$, $A_1 = B$, $A_0 = A_1 Q_1 + A_2 \Rightarrow \mathrm{div}(A_0, A_1) = \mathrm{div}(A_1, A_2)$ avec $\deg A_2 < \deg A_1$

etc ... $A_{m-1} = A_m Q_m + 0$.

$$\mathrm{Div}(A,B) = \mathrm{Div}(A_0, A_1) = \dots = \mathrm{Div}(A_m, 0) = \mathrm{Div}(A_m).$$ (On prend le pol. unit. multiple de A_m)

Ce polynôme est appelé pgcd(A, B) ou $A \wedge B$.

$\mathrm{pgcd}(X^3 + X^2 - 2,\ X^3 + X - 2)$

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

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

$$X^2 - X = \tfrac{1}{2} X (2X - 2) + 0.$$

$\Rightarrow \mathrm{pgcd} = X - 1.$

Théorème (Bezout)

> Si $D = \mathrm{pgcd}(A, B)$, alors $\exists\, (U, V) \in K[X]^2$ tq
> $$D = AU + BV.$$

Idem que pour $\mathbb{Z}$, à partir de l'algo. d'Euclide.

Reprenons l'exemple :

$X^2 - X = A - B$

$2X - 2 = B - (X+1)(X^2-X) = B - (X+1)(A-B) = (X+2)B - (X+1)A.$

$D = \frac{1}{2}(X+2)B - \frac{1}{2}(X+1)A.$

<u>Prop</u>

$\mathrm{pgcd}(A,B) = \mathrm{pgcd}(B,A)$

Si $A | B$ alors $\mathrm{pgcd}(A,B) = \lambda A$.

$P | A$ et $P | B \iff P | \mathrm{pgcd}(A,B)$

$\mathrm{pgcd}(AC, BC) = \mathrm{pgcd}(A,B)\, C$, si C est unitaire

$\mathrm{Mul}(A,B) = \mathrm{Mul}(A) \cap \mathrm{Mul}(B).$

<u>Thm</u>

$\exists !$ pol. unitaire M tq $\mathrm{Mul}(A,B) = \mathrm{Mul}(M)$.

<u>Dem</u>

<u>Unicité</u> : $\mathrm{Mul}(M_1) = \mathrm{Mul}(M_2) \Rightarrow M_1 | M_2$ et $M_2 | M_1$ etc...

<u>Existence</u> : Si $A = 0$ ou $B = 0 \Rightarrow M = 0$.

Si $A, B \neq 0$, alors $\mathrm{Mul}(A,B)$ est non trivial car $\exists AB$.

Soit $M \in \mathrm{Mul}(A,B)$, de deg minimal et unitaire.

Alors $\mathrm{Mul}(M) \subset \mathrm{Mul}(A,B)$ clairement.

Soit $N \in \mathrm{Mul}(A,B)$, $N = MQ + R$, $\deg R < \deg M$.

A / N et $A / M \Rightarrow A | R$; de même $B | R \Rightarrow R \in \mathrm{Mul}(A,B)$

Mais M était censé être de deg minimal dans $\text{Mul}(A,B) \Rightarrow R=0$

Donc $M \mid N$ et donc $N \in \text{Mul}(M)$.

On a montré $\text{Mul}(M) = \text{Mul}(A,B)$.

$\boxed{\text{B}}$

$M = \text{ppcm}(A,B) = A \vee B$.

<u>Prop:</u>

$\text{ppcm}(A,B) = \text{ppcm}(B,A)$

Si $A \mid B$ alors $\text{ppcm}(A,B) = \lambda B$

$A \mid P$ et $B \mid P \Leftrightarrow \text{ppcm}(A,B) \mid P$.

Si C est unitaire $\Rightarrow \text{ppcm}(AC, BC) = \text{ppcm}(A,B) \times C$.

<u>Thm</u>

$$\text{ppcm}(A,B) \times \text{pgcd}(A,B) = \lambda AB.$$

4) <u>Polynômes premiers entre eux</u>

A et B <u>premiers entre eux</u> si $A \wedge B = 1$.

<u>Thm</u> (Bezout)

A, B premiers entre eux $\Leftrightarrow \exists\, U, V \in \mathbb{K}[X]$ tq $AU + BV = 1$.

<u>Prop</u>

$A \wedge B = 1$ et $A \wedge C = 1 \Rightarrow A \wedge (BC) = 1$

$A \wedge P_i = 1, i = 1, \dots, n \Rightarrow A \wedge (P_1 \cdots P_n) = 1$.

$A \wedge B = 1 \Rightarrow A^n \wedge B^m = 1$.

Thm (Gauss)

$$\boxed{A \mid BC \text{ et } A \wedge B = 1 \Rightarrow A \mid C.}$$

Thm

$$\boxed{A \mid C,\ B \mid C \text{ et } A \wedge B = 1 \Rightarrow AB \mid C.}$$

Si $P_1, \dots, P_n$ sont 2 à 2 premiers entre eux et $P_i \mid A\ \forall i$, alors $P_1 \cdots P_n \mid A$.

Si $a_1, \dots, a_n$ racines distinctes de P, alors

$(X-a_1) \cdots (X-a_n) \mid P$.

5) Décomposition en facteurs irréductibles.

$P \in \mathbb{K}[X]$ est irreductible dans $\mathbb{K}[X]$ si ses seuls diviseurs sont les diviseurs triviaux $(\lambda 1, \mu P)$.

Sinon il est composé (sauf si P est constant).

- $X-a$ est irreductible $\forall \mathbb{K}$.
- X^2+1 est irreductible dans $\mathbb{R}[X]$, pas dans $\mathbb{C}[X]$.

Prop

Si P irred et si $P \nmid A \Rightarrow P \wedge A = 1$.

Si P est irred et $P \mid AB \Rightarrow P \mid A$ ou $P \mid B$.

Thm (Décomp. des pol. en facteurs irred).

Soit $A \in \mathbb{K}[X]$, non constant, alors $\exists \lambda \in \mathbb{K}^*$, $N \in \mathbb{N}^*$, $P_1, \dots, P_N$ irreductibles dans $\mathbb{K}[X]$, unitaires 2 à 2 $\neq$, il existe $\alpha_1, \dots, \alpha_n \in \mathbb{N}^*$ tq $A = \lambda P_1^{\alpha_1} \dots P_n^{\alpha_n}$. Cette décomp. est unique à l'ordre des facteurs près.

idem que $\mathbb{Z}$.

IV Racines d'un polynôme.

1) Racines et degré

On a vu que si $a_1, \dots, a_n$ racines $\neq$ de P alors $(X-a_1)\dots(X-a_n) \mid P$.

Prop

Un pol. ne peut pas avoir plus de racines que son degré.

Corollaire

Si $P \in \mathbb{K}_n[X]$ possède au moins $n+1$ racines, alors $P=0$.

Soit $P, Q \in \mathbb{K}_n[X]$ tels que P et Q prennent la même valeur en $n+1$ points. Alors $P-Q \in \mathbb{K}_n[X]$ et s'annule en $n+1$ points. Donc $P=Q$.

2) Multiplicité des racines.

a racine de P est dit de multiplicité $\alpha \in \mathbb{N}^*$ si
$$(X-a)^{\alpha} \mid P \text{ et } (X-a)^{\alpha+1} \nmid P.$$

C'est le plus grand α tq $(X-a)^\alpha \mid P$.

Si $a_1, \dots, a_n$ racines $\neq$, de multiplicité $\alpha_1, \dots, \alpha_n$, alors $(X-a_1)^{\alpha_1} \dots (X-a_n)^{\alpha_n} \mid P$.

La somme des multiplicités des racines ne peut excéder $\deg P$.

3) Multiplicité et dérivation.

Thm

Si a est racine de mult. α pour P, alors a est racine de mult. $\alpha-1$ pour P'

(Dans le cas $\alpha=1$, comprendre a n'est pas racine de P').

Dem

$P = (X-a)^\alpha Q$ avec $Q(a) \neq 0$.

$P' = \alpha (X-a)^{\alpha-1} Q + (X-a)^\alpha Q' = (X-a)^{\alpha-1} \tilde{Q}$.

$\tilde{Q}(a) = \alpha Q(a) \neq 0 \Rightarrow a$ est de mult. $\alpha-1$ pour P. ∎

Thm

Il y a equiv. entre

1) a est racine d'ordre α de P

2) $P(a) = P'(a) = \dots = P^{(\alpha-1)}(a) = 0$ et $P^{(\alpha)}(a) \neq 0$.

V Polynômes scindés

1) Définition

Un polynôme non constant $P \in \mathbb{K}[X]$ est dit <u>scindé</u> dans $\mathbb{K}[X]$ si on peut écrire $P(X) = \lambda(X-x_1)\cdots(X-x_n)$, avec $\lambda \in \mathbb{K}^*$, $x_1, \dots, x_n \in \mathbb{K}$.

Dans ce cas, λ est le coeff dominant de P, n est le degré et $x_1, \dots, x_n$ sont les racines de P.

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

X^2+1 n'est pas scindé dans $\mathbb{R}[X]$ car n'a pas de racine dans $\mathbb{R}$.

Thm

Il y a équivalence entre

i) P est scindé dans $\mathbb{K}[X]$

ii) La somme des multiplicité des racines de P vaut $\deg P$.

2) Le cas $\mathbb{C}[X]$

Thm (d'Alembert-Gauss)

Tout pol. non constant de $\mathbb{C}[X]$ admet au moins une racine.

Admis.

Corollaire

Les pol. irred. de $\mathbb{C}[X]$ sont ceux de deg 1.

Théorème

Soit $P \in \mathbb{C}[X]$ non constant, alors il existe $\lambda \in \mathbb{K}^*$, $N \in \mathbb{N}^*$, $a_1, \dots, a_N \in \mathbb{C}$

2 à 2 distincts, $\alpha_1, \dots, \alpha_N \in \mathbb{N}^*$ tq
$P(X) = \lambda (X - a_1)^{\alpha_1} \dots (X - a_N)^{\alpha_N}$.

Cette décomp. est unique, à l'ordre des facteurs près.

Corollaire

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.

Proposition

Si $A, B \in \mathbb{C}[X]$, il y a équivalence entre
i) $A | B$
ii) les racines de A sont racines de B, leur mult. dans A est $\leq$ à leur mult. ds B.

Prop

Si $A, B \in \mathbb{C}[X]$, il y a équiv. entre
i) $A \wedge B = 1$
ii) A et B n'ont pas de racine commune.

3) Le cas $\mathbb{R}[X]$.

Prop

Les pol. irred. de $\mathbb{R}[X]$ sont :

- les pol. de deg 1.
- les pol. de deg. 2 avec $\Delta < 0$.

Dem

Ils sont clairement irreductibles.

Inversement si P est irred. dans $\mathbb{R}[X]$, P est non constant, donc il admet une racine $a \in \mathbb{C}$. Si $a \in \mathbb{R}$ alors $(X-a) \mid P \Rightarrow P = \lambda(X-a)$.

Si $a \in \mathbb{C}\setminus\mathbb{R}$, alors $\bar{a}$ est aussi racine de P car :

$$P(X) = \sum_{k=0}^{n} \alpha_k X^k,\ P(a) = \sum \alpha_k a^k = 0 \Rightarrow \overline{P(a)} = \sum \bar{\alpha}_k \overline{a^k} = \sum \alpha_k \bar{a}^k = 0$$

$$\Rightarrow (X-a)(X-\bar{a}) \mid P \Rightarrow \underbrace{(X^2 - 2\,\mathrm{Re}\,a + |a|^2)}_{\in \mathbb{R}[X]} \mid P. \Rightarrow \text{etc....}$$

(B)

D'où le thm de décomp. en irred. dans $\mathbb{R}[X]$:

$$\boxed{P(X) = \lambda \prod_{k=1}^{N} (X-a_i)^{\alpha_i} \prod_{\ell=1}^{n} (X^2 + p_\ell X + q_\ell)^{\beta_\ell} \quad \text{avec } p_\ell^2 - 4q_\ell < 0\ \forall \ell.}$$

Factoriser $X^5 - 1$ dans $\mathbb{R}[X]$.

4) Relations coefficients - racines

Thm

$$(X-x_1)\cdots(X-x_n) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_0, \text{ avec}$$

$$\sigma_1 = \sum_{j=1}^{n} x_j,\ \sigma_2 = \sum_{1 \le j_1 < j_2 \le n} x_{j_1} x_{j_2},\ \cdots,\ \sigma_k = \sum_{1 \le j_1 < \cdots < j_k \le n} x_{j_1} \cdots x_{j_k},$$

$$\sigma_n = x_1 \cdots x_n.$$

Dem

Le terme en X^{n-k} est obtenu par des produits de $n-k$ termes en X et de k termes en $-x_i$. $\square$

Les solutions du système $\begin{cases} x_1 + x_2 = \sigma_1 \\ x_1 x_2 = \sigma_2 \end{cases}$ sont les racines de $X^2 - \sigma_1 X + \sigma_2$