Pour lu: entretiens avec les enseignants
12h - 14h30

Pour ma: 13.1, 13.2
24.22, 24.28



# Compléments sur les polynômes

## Je me souviens

1. Que sont les polynômes ?
2. Quelles sont les opérations sur les polynômes ?

les polynômes.

$E = \{(u_n)_n \text{ tq } u_n \text{ nulle à partir d'un certain rang}\}$

dans $E$, il y a $(0,1,0,1,0,0,0,0\ldots)$
$(3,5,0,0,0\ldots)$

On définit des opérations sur ces suites

- $+$ (terme à terme) ) ev.
- $\cdot$ (terme à terme) )
- $\times$ $w_n = \sum_{k=0}^{n} u_k v_{n-k}$ $\forall n$ ] algèbre.

anneau

Notation: On pose $(1,0,\ldots) = 1$
$(0,1,0\ldots) = X$

etc $(0 \ldots, \underset{\uparrow}{1}, 0 \ldots) = X^n$
$n$

derivata, primitivazione.

composizione ...

$$P \circ (X+1) = P(X+1)$$

3. Que désigne $\mathbb{K}_n[X]$ ?

ens des pol de degré $\leq n$

$\mathrm{Vect}(1, X, \dots, X^n)$

4. Énoncer le théorème de la division euclidienne dans $\mathbb{K}[X]$.

Soit $A, B \in \mathbb{K}[X]$ $\quad B \neq 0$

div eucl de $A$ par $B$

$\exists ! (Q, R)$ tq $\quad$ Si $B$ de deg $\mu$

$A = BQ + R \quad R \in \mathbb{K}_{\mu-1}[X]$

$(\deg R < \deg B)$

5. Qu'est-ce que la fonction polynomiale associée à $P$ ?

$\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$

$t \longmapsto P(t) = \sum_{k=0}^{n} a_k t^k$

$t^k$ : $t \times \dots \times t$ dans $\mathbb{K}$ ($k$ fois)

Rmq : Si $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$ ....

6. Parlons de racines d'un polynôme.

$\alpha$ racine de $P$

$\Leftrightarrow \quad \tilde{P}(\alpha) = 0$

$\Leftrightarrow \quad (X-\alpha) \mid P$

savoir d'un point de vue à l'autre.

$\alpha$ racine d'ordre au moins $k$ de $P$ — $k$ entier

$\Leftrightarrow \quad \tilde{P}(\alpha) = \dots = \tilde{P}^{(k-1)}(\alpha) = 0$

$\Leftrightarrow \quad (X-\alpha)^k \mid P$

7. Qu'est-ce qu'un polynôme scindé ?

$P$ scindé $\Leftrightarrow$ $P$ peut s'écrire $\lambda \prod_{k=1}^{n} (X-\alpha_k)$

ex : $X^2+X+1$ non scindé dans $\mathbb{R}[X]$

$X^2-1$ est scindé dans $\mathbb{R}[X]$

8. Relations coefficients-racines.

sous-groupe absorbant

9. Quels sont les idéaux de $\mathbb{K}[X]$ ?

Ce sont les $A\mathbb{K}[X]$ où $A \in \mathbb{K}[X]$

(multiples de $A$)

$\{P \in \mathbb{K}[X] \mid A \mid P\}$

- $A\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$ car
  - $A\mathbb{K}[X] \subset \mathbb{K}[X]$
  - $0 \in A\mathbb{K}[X]$
  - $A\mathbb{K}[X]$ est stable par + et passage à l'opposé :
  - Soit $P \in A\mathbb{K}[X]$ et $Q \in \mathbb{K}[X]$
    Alors $A \mid P$ donc $A \mid PQ$
    donc $PQ \in A\mathbb{K}[X]$.
- Soit $I$ idéal de $\mathbb{K}[X]$

1er cas : $I = \{0\} = 0.\mathbb{K}[X]$

2e cas : On note $A$ polynôme unitaire, de degré minimal, dans $\mathbb{K}[X]$.

Mq $I = A\mathbb{K}[X]$.

$\supset$ $A \in I$ et $I$ absorbant

donc $A\mathbb{K}[X] \subset I$

(c) Soit $P \in I$

On effectue la div. eucl. de $P$ par $A$. Donc

$\exists ! (Q, R)$ tq

$P = AQ + R$

où $R = 0$ ou $\deg R < \deg A$

Mais $AQ \in I$

$P \in I$

donc $R \in I$

donc $R = 0$

car $\deg A$ est minimal

donc $P = AQ$

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

Le programme se limite au cas où le corps de base $\mathbb{K}$ est un sous-corps de $\mathbb{C}$. Typiquement $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$.

# 1 PGCD de deux polynômes

## 1.1 Définition du PGCD par les idéaux

**Lemme.** Soit $A, B \in \mathbb{K}[X]$. Alors :

$$(A) + (B) = A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV,\ U, V \in \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$.

**Définition.** Soit $A, B \in \mathbb{K}[X]$ non tous les deux nuls. Alors il existe un unique polynôme unitaire $D$, appelé **PGCD de $A$ et $B$**, tel que :

$$(A) + (B) = (D) \text{ i.e. } A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

**Notation.**

- On note $A \wedge B$ le PGCD de $A$ et $B$.
- La relation $AU + BV = A \wedge B$ s'appelle **relation de Bézout**.

**Proposition.** Soit $A, B$ deux polynômes non nuls. Les diviseurs communs à $A$ et $B$ sont les diviseurs de $A \wedge B$.

**Remarque.** *On retrouve la définition de première année : $A \wedge B$ est le polynôme unitaire, de plus grand degré, qui divise à la fois $A$ et $B$.*

Même preuve que dans $\mathbb{Z}$.

## 1.2 Algorithme d'Euclide

**Proposition.** Soit $A, B \in \mathbb{K}[X]$, supposés non nuls. En notant $R$ le reste de la division euclidienne de $A$ par $B$, on a :

$$A \wedge B = B \wedge R$$

Preuve : On note $D = A \wedge B$

On effectue la div. eucl. de $A$ par $B$ :

$A = BQ + R$ où $\deg R < \deg B$

Comme $D = A \wedge B$, $\exists U, V$ tq

$AU + BV = D$

Mq $D = B \wedge R$ ie $(B)+(R) = (D)$.

⊃ $D = AU + BV$

$= (BQ + R)U + BV$

$= B(QU + V) + RU$

$\in (B) + (R)$

⊂ Soit $P \in (B) + (R)$

ie $\exists T, S$ tq $P = BT + RS$

donc $P = BT + (A - BQ)S$

$= AS + B(T - QS)$

$\in (A) + (B) = (D)$

degré strictement ↓

$A \wedge B = B \wedge R$

**Corollaire.** En itérant l'utilisant de cette propriété, le degré du second polynôme est strictement décroissant, donc les itérations se terminent avec un reste nul. Le PGCD de $A$ et $B$ est alors le dernier reste non nul obtenu.

$A \wedge B = B \wedge R_1$

$= R_1 \wedge R_2$

...

$= R_n \wedge 0 = R_n$

car $(R_n) + (0) = (R_n)$

**Corollaire.** L'analyse de l'algorithme d'Euclide permet de construire un couple $(U, V)$ de polynômes satisfaisant la relation de Bézout.

## 1.3 Polynômes premiers entre eux

**Définition.** On dit que $A$ et $B$ sont premiers entre eux lorsque $A \wedge B = 1$.

**Remarque.** *Deux polynômes sont premiers entre eux lorsque les seuls diviseurs communs sont les polynômes constants.*

**Théorème de Bézout.**

Deux polynômes $A$ et $B$ sont premiers entre eux si et seulement s'il existe des polynômes $U$ et $V$ tels que :

$$AU + BV = 1$$

**Proposition.** Soit $A, B$ deux polynômes non nuls, $D$ un polynôme unitaire.

$$D = A \wedge B \iff \exists A_1, B_1 \in \mathbb{K}[X], \begin{cases} A = A_1 D \text{ et } B = B_1 D \\ A_1 \text{ et } B_1 \text{ sont premiers entre eux} \end{cases}$$

## 2 Un peu d'arithmétique des polynômes

**Lemme de Gauss.**

Soit $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$.

**Corollaire.** Si $A \mid C$, $B \mid C$ et $A \wedge B = 1$, alors $AB \mid C$.

**Corollaire.** Si $A \wedge C = 1$ et $B \wedge C = 1$, alors $AB \wedge C = 1$.

Preuve: On suppose $A \mid BC$ ie $\exists P$ tq $BC = AP$

et $A \wedge B = 1$ ie $\exists U, V$ tq $AU + BV = 1$

donc $AUC + BCV = C$

ie $AUC + APV = C$

donc $A(UC + PV) = C$

donc $A \mid C$

Corollaire : On suppose $A \mid C$ et $B \mid C$ et $A \wedge B = 1$

$\exists P, Q$ tq $AP = C = BQ$

donc $AP = BQ$ donc $A \mid BQ$

or $A \wedge B = 1$ donc $A \mid Q$ (Gauss)

donc $\exists R$ tq $Q = AR$

puis $C = BAR$ donc $AB \mid C$

$\mathbb{K} = \mathbb{Q}$ $\mathbb{Z}/7\mathbb{Z}$

# 3 Polynômes irréductibles, décomposition en facteurs irréductibles

## 3.1 Définition

**Définition.** Un polynôme $P$ est dit **irréductible** s'il est non constant, et que ses seuls diviseurs sont les polynômes constants et les polynômes associés à $P$, i.e. les $\lambda P$ où $\lambda \neq 0$.

**Analogie.** *Les polynômes irréductibles sont aux polynômes ce que les nombre premiers sont aux entiers.*

## 3.2 Propriétés

**Proposition.** Un polynôme $P$ est irréductible si et seulement s'il n'existe pas de factorisation $P = AB$ où $0 < \deg(A) < \deg(P)$.

**Proposition.** Soit $P$ irréductible, et $Q$ quelconque. Alors soit $P \wedge Q = 1$, soit $P \mid Q$.

(il y a que ces 2 options)

## 3.3 Exemples

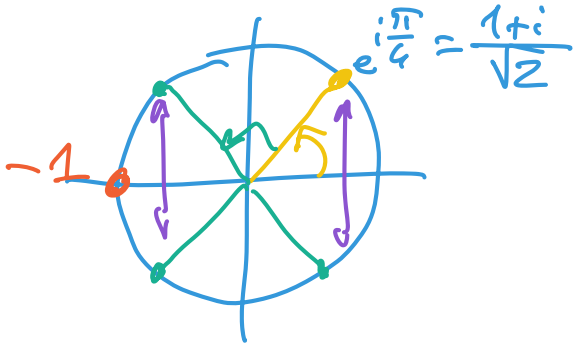
**Remarque.** *L'étude générale des polynômes irréductibles n'est pas au probramme. Seuls la description des irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$ est à connaître.*
*La description des irréductibles de $\mathbb{Q}[X]$ est, par exemple, très délicate.*

**Proposition.**

- Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré 1.
- Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1, et ceux de degré 2 à discriminant $< 0$.

**Remarque.** $X^4 + 1$ *n'a pas de racine réelle, mais ce n'est pas un irréductible de* $\mathbb{R}[X]$.

↳ $X^4 + 1 = X^4 - (-1)$




les racines 4e de $(-1)$ sont $e^{i\frac{\pi}{4}}$, $ie^{i\frac{\pi}{4}}$, $-e^{i\frac{\pi}{4}}$, $-ie^{i\frac{\pi}{4}}$

$\alpha$ $\beta$ $\overline{\beta}$ $\overline{\alpha}$

$$(X^4+1) = (X-\alpha)(X-\bar{\alpha})(X-\beta)(X-\bar{\beta})$$

$$= (X^2 - 2\mathrm{Re}\,\alpha\, X + |\alpha|^2)$$

$$(X^2 - 2\mathrm{Re}\,\beta\, X + |\beta|^2)$$

$$= (X^2 - \sqrt{2}\,X + 1)(X^2 + \sqrt{2}\,X + 1)$$

irréductibles de $\mathbb{R}[X]$

## 3.4 Décomposition en facteurs irréductibles

**Théorème.**

Tout polynôme $P$ non constant se décompose de façon unique (à l'ordre des facteurs près) sous la forme :

$$P = \lambda \prod_{i=1}^{k} P_i^{m_i}$$

où les $P_i$ sont irréductibles unitaires, les $m_i$ dans $\mathbb{N}^*$ et $\lambda$ le coefficient dominant de $P$.

**Remarque.** *Cette décomposition s'écrit :*

- *sur* $\mathbb{C}[X]$ *:* $P = \lambda \prod_{i=1}^{k} (X - a_i)^{m_i}$
- *sur* $\mathbb{R}[X]$ *:* $P = \lambda \prod_{i=1}^{k} (X - a_i)^{m_i} \prod_{j=1}^{\ell} (X^2 + b_j X + c_j)^{n_j}$ *où* $b_j^2 - 4c_j < 0$.

## 3.5 Utilisation de la décomposition en facteurs irréductibles pour le calcul du PGCD

**Proposition.** Soit $P, Q$ deux polynômes non nuls, que l'on décompose en facteurs irréductibles :

$$P = \lambda \prod_{i=1}^{k} P_i^{m_i} \text{ et } Q = \mu \prod_{i=1}^{k} P_i^{n_i}$$

Les $P_i$ sont supposés irréductibles, unitaires, deux à deux distincts et les $m_i, n_i$ sont des entiers éventuellement nuls. Alors :

$$\text{pgcd}(P, Q) = \prod_{i=1}^{k} P_i^{\text{Min}(m_i, n_i)}$$

**Proposition.** Soit $P, Q$ deux polynômes non nuls, que l'on décompose en facteurs irréductibles. Alors $P$ et $Q$ sont premiers entre eux si et seulement s'il n'ont aucun facteur irréductible commun.

## 4.6 Rappel : relations coefficients-racines