

# Compléments sur les polynômes

<b>Je me souviens</b>	<b>2</b>
<b>Cours</b>	<b>3</b>
1 PGCD de deux polynômes . . . . .	3
1.1 Définition du PGCD par les idéaux . . . . .	3
1.2 Algorithme d'Euclide . . . . .	3
1.3 Polynômes premiers entre eux . . . . .	3
2 Un peu d'arithmétique des polynômes . . . . .	4
3 Polynômes irréductibles, décomposition en facteurs irréductibles . . . . .	4
3.1 Définition . . . . .	4
3.2 Propriétés . . . . .	4
3.3 Exemples . . . . .	4
3.4 Décomposition en facteurs irréductibles . . . . .	4
3.5 Utilisation de la décomposition en facteurs irréductibles pour le calcul du PGCD . . . . .	5
4 Annexes . . . . .	5
4.1 PPCM de deux polynômes . . . . .	5
4.2 PGCD de plus de deux éléments . . . . .	5
4.3 Annexe : méthode de Horner pour l'évaluation polynomiale . . . . .	6
4.4 Rappel : interpolation de Lagrange . . . . .	6
4.5 Rappel : polynômes scindé . . . . .	7
4.6 Rappel : relations coefficients-racines . . . . .	7
<b>Exercices</b>	<b>8</b>
Exercices et résultats classiques à connaître . . . . .	8
Relations coefficients-racines . . . . .	8
Autour des racines $n$ -ièmes de l'unité . . . . .	8
Exercices du CCINP . . . . .	9
Exercices . . . . .	9
Petits problèmes d'entraînement . . . . .	10

**Je me souviens**

1. Que sont les polynômes ?
2. Quelles sont les opérations sur les polynômes ?
3. Que désigne  $\mathbb{K}_n[X]$  ?
4. Énoncer le théorème de la division euclidienne dans  $\mathbb{K}[X]$ .
5. Qu'est-ce que la fonction polynomiale associée à  $P$  ?
6. Parlons de racines d'un polynôme.
7. Qu'est-ce qu'un polynôme scindé ?
8. Relations coefficients-racines.
9. Quels sont les idéaux de  $\mathbb{K}[X]$  ?

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  $B$ .

### 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 :

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

**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.

**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  $AB \wedge C = 1$ .

## 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 nombres 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  $P \mid Q$ .

### 3.3 Exemples

**Remarque.** L'étude générale des polynômes irréductibles n'est pas au programme. Seule 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  $\mathbb{R}[X]$ .

### 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 :

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

**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 Annexes

### 4.1 PPCM de deux polynômes

**Remarque.** La notion de PPCM est beaucoup moins utilisée que celle de PGCD.

**Définition.** Soit  $A, B$  deux polynômes non nuls. Alors  $I = (A) \cap (B)$  est un idéal de  $\mathbb{K}[X]$ , donc il existe un unique  $M \in \mathbb{K}[X]$  unitaire tel que :

$$(A) \cap (B) = (M)$$

On l'appelle **PPCM de  $A$  et  $B$** , et on le note  $A \vee B$ .

**Proposition.** Avec les mêmes notations, en notant  $D = A \wedge B$ , les deux polynômes  $AB$  et  $MD$  sont associés, c'est-à-dire égaux à un coefficient multiplicatif non nul près.

**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 :

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

### 4.2 PGCD de plus de deux éléments

**Définition.** Soit  $A_1, \dots, A_p \in \mathbb{K}[X]$  des polynômes non nuls. Considérons :

$$\begin{aligned} I &= (A_1) + (A_2) + \dots + (A_p) \\ &= \{A_1 U_1 + A_2 U_2 + \dots + A_p U_p, \\ &\quad U_1, \dots, U_p \in \mathbb{K}[X]\} \end{aligned}$$

Alors  $I$  est un idéal non nul de  $A$ , donc il existe un unique polynôme unitaire  $D$  tel que  $I = (D)$ . On l'appelle le **PGCD** de  $(A_1, \dots, A_p)$ .

**Proposition.** Les diviseurs communs à tous les  $A_i$  sont les diviseurs de  $D$  :

$$(\forall i, P \mid A_i) \iff D \mid \text{pgcd}(A_1, \dots, A_p)$$

**Associativité.**

$$\begin{aligned} \text{pgcd}(A_1, \dots, A_p, A_{p+1}) \\ = \text{pgcd}(\text{pgcd}(A_1, \dots, A_p), A_{p+1}) \end{aligned}$$

**Définition.** Les polynômes  $A_1, \dots, A_p$  sont **premiers entre eux** (dans leur ensemble) lorsque  $\text{pgcd}(A_1, \dots, A_p) = 1$ .

**Théorème de Bézout.**

$A_1, \dots, A_p$  sont **premiers entre eux** si et seulement s'il existe  $U_1, \dots, U_p$  tels que :

$$A_1 U_1 + \dots + A_p U_p = 1$$

**Remarque.** Attention, des polynômes peuvent être premiers entre eux dans leur ensemble, sans être premiers entre eux deux à deux.

**Exemple.** Donner le PGCD de  $(X-2)(X-3)$ ,  $(X-2)(X-5)$  et  $(X-3)(X-5)$ .

### 4.3 Annexe : méthode de Horner pour l'évaluation polynomiale

```
# -*- coding:utf-8 -*-

from numpy.polynomial import Polynomial
X = Polynomial([0, 1])
P = 3*X**6 + 2*X**5 - 8*X**3 + X**2 + 30*X + 11
a = P.coef
print(a)
# [11. 30. 1. -8. 0. 2. 3.]

print(P(-2))
# 147.0

def evaluate(a, t):
    """renvoie la valeur P(t) où P est le polynôme
    dont les coefficients sont dans a"""
    n = len(a)-1
    puiss = 1
    s = a[0]
    for k in range(0,n):
        # en entrée de boucle, puiss est t^k,
        # s est \sum_{i=0}^k a_i t^i
        puiss *= t
        s += a[k+1] * puiss
    return s
```

```
print(evaluate(a,-2))
# 147.0

def evaluate2(a, t):
    """renvoie la valeur P(t) où P est le polynôme
    dont les coefficients sont dans a
    par la méthode de Horner """
    n = len(a)-1
    s = a[n]
    for k in range(0,n):
        # en entrée de boucle, s est
        # a_n t^k + a_{n-1} t^{k-1} + ... + a_{n-k+1} t + a_{n-k}
        # c'est-à-dire \sum_{i=0}^k a_{n-i} t^{k-i}
        s *= t
        s += a[n-k-1]
    return s

print(evaluate2(a,-2))
# 147.0

# avec cette seconde fonction,
# le nombre de multiplications a été divisé par 2.
```

### 4.4 Rappel : interpolation de Lagrange

#### Théorème.

Soit  $\alpha_0, \dots, \alpha_n \in \mathbb{K}$  supposés deux à deux distincts, et  $y_0, \dots, y_n \in \mathbb{K}$ . Il existe un unique polynôme  $P \in \mathbb{K}_n[X]$  tel que :

$$\forall i \in \{0, \dots, n\}, P(\alpha_i) = y_i$$

*Preuve.* On introduit :

$$\begin{aligned} \varphi : \mathbb{K}_n[X] &\rightarrow \mathbb{K}^{n+1} \\ P &\mapsto (P(\alpha_0), \dots, P(\alpha_n)) \end{aligned}$$

- L'évaluation en  $\alpha_i$  est linéaire, donc  $\varphi$  est une application linéaire.
- Si  $P \in \text{Ker } \varphi$ , alors  $P \in \mathbb{K}_n[X]$  et s'annule en  $(n+1)$  points distincts, donc  $P = 0$ . On a montré que  $\varphi$  est injective.
- Comme  $\dim \mathbb{K}_n[X] = n+1 = \dim \mathbb{K}^{n+1}$ , on en déduit que  $\varphi$  est bijective.

□

**Exercice.** Soit  $\alpha_0, \dots, \alpha_n \in \mathbb{K}$  deux à deux distincts.

1. Pour  $i \in \{0, \dots, n\}$ , déterminer l'unique polynôme  $L_i \in \mathbb{K}_n[X]$  tel que :

$$L_i(\alpha_i) = 1 \text{ et } L_i(\alpha_j) = 0 \text{ pour } j \neq i$$

2. Montrer que la famille  $(L_0, \dots, L_n)$  est une base de  $\mathbb{K}_n[X]$ .

3. Donner les coordonnées d'un polynôme  $P \in \mathbb{K}_n[X]$ , dans cette base.

4. En déduire une autre démonstration du théorème précédent.

*Solution.*

1. Il y a une ambiguïté dans la formulation de la question. Est-ce qu'il faut justifier cette unicité ?

$$\boxed{M1} \quad \text{Posons } L_i(X) = \frac{\prod_{\substack{k=1 \\ k \neq i}}^n (X - \alpha_k)}{\prod_{\substack{k=1 \\ k \neq i}}^n (\alpha_i - \alpha_k)}.$$

On remarque que les  $L_i$  conviennent.

$\boxed{M2}$  **Analyse.** Supposons que  $L_i$  convienne. On sait que les  $(\alpha_k)_{0 \leq k \leq n}$  sont  $n$  racines distinctes de  $L_i$  de degré  $\leq n$ , donc il existe  $\lambda \in \mathbb{K}$  tel que :

$$L_i(X) = \lambda \prod_{\substack{k=1 \\ k \neq i}}^n (X - \alpha_k)$$

Et comme  $L_i(\alpha_i) = 1$ , c'est que :

$$\lambda = \frac{1}{\prod_{\substack{k=1 \\ k \neq i}}^n (\alpha_i - \alpha_k)}$$

Cela justifie l'unicité sous réserve d'existence, et donne l'expression (potentielle) de  $L_i(X)$ .

**Synthèse.** Posons  $L_i(X) = \frac{\prod_{\substack{k=1 \\ k \neq i}}^n (X - \alpha_k)}{\prod_{\substack{k=1 \\ k \neq i}}^n (\alpha_i - \alpha_k)}$ .

Ils sont bien de degré  $\leq n$ , et satisfont la propriété  $L_i(\alpha_j) = \delta_{ij}$ .

2. • Montrons que  $(L_0, \dots, L_n)$  est libre.  
Soit  $\lambda_0, \dots, \lambda_n \in \mathbb{K}$  tels que :

$$\underbrace{\lambda_0 L_0 + \dots + \lambda_n L_n}_0 = 0$$

En évaluant ce polynôme en  $\alpha_j$ , on obtient :

$$\begin{aligned} 0 &= \sum_{i=0}^n \lambda_i L_i(\alpha_j) \\ &= \sum_{i=0}^n \lambda_i \delta_{ij} \\ &= \lambda_j \end{aligned}$$

ce qui est vrai pour tout  $j$ , ce qui montre la liberté.

- Comme  $(L_0, \dots, L_n)$  est une famille libre à  $n+1$  éléments dans  $\mathbb{K}_n[X]$  de dimension  $n+1$ , c'est une base.

3. Soit  $P \in \mathbb{K}_n[X]$ . On cherche  $\lambda_0, \dots, \lambda_n \in \mathbb{K}$  tels que :

$$P = \sum_{i=0}^n \lambda_i L_i$$

En évaluant ce polynôme en  $\alpha_j$ , on obtient :

$$P(\alpha_j) = \lambda_j$$

de sorte que :

$$P = \sum_{i=0}^n P(\alpha_i) L_i$$

**Remarque.** On a en particulier :

$$1 = \sum_{i=0}^n L_i$$

4. On sait que l'application qui, à un vecteur d'un e.v. de dimension finie, associe ses coordonnées dans une base fixée, est un isomorphisme. □

## 4.5 Rappel : polynômes scindé

**Définition.** Un polynôme  $P$  est dit **scindé** lorsque tous les polynômes irréductibles qui figurent dans sa décomposition sont de degré 1 :

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

**Proposition.**  $P$  est scindé si et seulement si le nombre de ses racines, comptées avec multiplicité, est égal à  $\deg(P)$ .

### Théorème de d'Alembert-Gauss.

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

**Proposition.** Dans  $\mathbb{C}[X]$ ,  $A \mid B$  si et seulement si, pour tout racine  $a$  de  $A$  de multiplicité  $m$ ,  $a$  est racine de  $B$  avec une multiplicité  $\geq m$ .

**Proposition.** Soit  $P \in \mathbb{R}[X]$  et  $z \in \mathbb{C} \setminus \mathbb{R}$  une racine de  $P$  de multiplicité  $m$ . Alors  $\bar{z}$  est racine de  $P$  de multiplicité  $m$ .

## 4.6 Rappel : relations coefficients-racines

**Proposition.** Soit

$$P = aX^2 + bX + c = a(X - x_1)(X - x_2)$$

un polynôme scindé de degré 2,  $a \neq 0$ . Alors :

$$x_1 + x_2 = -\frac{b}{a} \text{ et } x_1 x_2 = \frac{c}{a}$$

**Proposition.** Si  $x_1, x_2$  satisfont  $\begin{cases} x_1 + x_2 = s \\ x_1 x_2 = p \end{cases}$  alors ce sont les racines du polynôme  $X^2 - sX + p$ .

**Définition.** Soit  $P = \sum_{i=0}^n a_i X^i$  un polynôme scindé,  $x_1, \dots, x_n$  ses racines (répétées si elles sont multiples). On appelle **fonctions symétriques**

élémentaires de  $x_1, \dots, x_n$  les quantités :

$$\sigma_1 = x_1 + \dots + x_n$$

$$\sigma_2 = x_1 x_2 + \dots + x_1 x_n + x_2 x_3 + \dots + x_{n-1} x_n$$

⋮

$$\sigma_{n-1} = x_1 \dots x_{n-1} + x_1 \dots x_{n-2} x_n + \dots + x_2 \dots x_{n-1}$$

$$\sigma_n = x_1 \dots x_n$$

c'est-à-dire :

$$\sigma_k = \sum_{\substack{i_1, \dots, i_k \in \{1, \dots, n\} \\ i_1 < i_2 < \dots < i_k}} x_{i_1} x_{i_2} \dots x_{i_k}$$

**Remarque.** Ce sont des fonctions symétriques : si on mélange les  $x_i$ , on ne change pas les  $\sigma_k$ .

**Remarque.**  $\sigma_k$  est la somme de tous les produits de  $k$  termes pris parmi  $x_1, \dots, x_n$ .

**Théorème.**

$$\sigma_1 = -\frac{a_{n-1}}{a_n} \text{ et } \sigma_n = (-1)^n \frac{a_0}{a_n}$$

**Remarque.** Il faut savoir retrouver :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

## Exercices et résultats classiques à connaître

### Relations coefficients-racines

#### 130.1

Soit  $n \in \mathbb{N}^*$  et  $P = (X + 1)^n - (X - 1)^n$ .

- Déterminer le coefficient dominant et le degré de  $P$ .
- Montrer que les racines complexes de  $P$  sont des racines simples.
- Préciser le produit et la somme des racines de  $P$ .
- Déterminer explicitement les racines de  $P$ .

### Autour des racines $n$ -ièmes de l'unité

#### 130.2

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

- Décomposer  $X^n - 1$  en facteurs irréductibles dans  $\mathbb{C}[X]$ .
- Décomposer  $X^n - 1$  en facteurs irréductibles dans  $\mathbb{R}[X]$ .



## Exercices du CCINP

130.3

 85

- Soient  $n \in \mathbb{N}^*$ ,  $P \in \mathbb{R}_n[X]$  et  $a \in \mathbb{R}$ .
  - Donner sans démonstration, en utilisant la formule de Taylor, la décomposition de  $P(X)$  dans la base  $(1, X - a, (X - a)^2, \dots, (X - a)^n)$ .
  - Soit  $r \in \mathbb{N}^*$ . En déduire que :  
 $a$  est une racine de  $P$  d'ordre de multiplicité  $r$  si et seulement si  $P^{(r)}(a) \neq 0$  et  $\forall k \in \llbracket 0, r - 1 \rrbracket$ ,  $P^{(k)}(a) = 0$ .
- Déterminer deux réels  $a$  et  $b$  pour que 1 soit racine double du polynôme  $P = X^5 + aX^2 + bX$  et factoriser alors ce polynôme dans  $\mathbb{R}[X]$ .

130.4

 87

Soient  $a_0, a_1, \dots, a_n$ ,  $n + 1$  réels deux à deux distincts.

- Montrer que si  $b_0, b_1, \dots, b_n$  sont  $n + 1$  réels quelconques, alors il existe un unique polynôme  $P$  vérifiant

$$\deg P \leq n \text{ et } \forall i \in \llbracket 0, n \rrbracket, P(a_i) = b_i.$$

- Soit  $k \in \llbracket 0, n \rrbracket$ .  
 Expliciter ce polynôme  $P$ , que l'on notera  $L_k$ , lorsque :

$$\forall i \in \llbracket 0, n \rrbracket, b_i = \begin{cases} 0 & \text{si } i \neq k \\ 1 & \text{si } i = k \end{cases}$$

- Prouver que  $\forall p \in \llbracket 0, n \rrbracket$ ,  $\sum_{k=0}^n a_k^p L_k = X^p$ .

130.5

 90

$\mathbb{K}$  désigne le corps des réels ou celui des complexes.  
 Soient  $a_1, a_2, a_3$  trois scalaires distincts donnés de  $\mathbb{K}$ .

- Montrer que  $\Phi : \mathbb{K}_2[X] \longrightarrow \mathbb{K}^3$   
 $P \longmapsto (P(a_1), P(a_2), P(a_3))$  est un isomorphisme d'espaces vectoriels.
- On note  $(e_1, e_2, e_3)$  la base canonique de  $\mathbb{K}^3$  et on pose  $\forall k \in \{1, 2, 3\}$ ,  $L_k = \Phi^{-1}(e_k)$ .
  - Justifier que  $(L_1, L_2, L_3)$  est une base de  $\mathbb{K}_2[X]$ .
  - Exprimer les polynômes  $L_1, L_2$  et  $L_3$  en fonction de  $a_1, a_2$  et  $a_3$ .
- Soit  $P \in \mathbb{K}_2[X]$ . Déterminer les coordonnées de  $P$  dans la base  $(L_1, L_2, L_3)$ .
- Application** : on se place dans  $\mathbb{R}^2$  muni d'un repère orthonormé et on considère les trois points  $A(0, 1), B(1, 3), C(2, 1)$ .  
 Déterminer une fonction polynomiale de degré 2 dont la courbe passe par les points  $A, B$  et  $C$ .

## Exercices

130.6

- Montrer que  $X^2 + X + 1$  divise  $X^{10} + X^5 + 1$ .
- Montrer que  $X^3 - X^2 + 1$  et  $X^2 - 2X + 2$  sont premiers entre eux.

130.7

Soit  $\lambda, \mu$  deux éléments distincts de  $\mathbb{K}$ , et  $P \in \mathbb{K}[X]$ .

- Exprimer en fonction de  $P$  le reste de la division de  $P$  par  $(X - \lambda)(X - \mu)$ .
- Exprimer en fonction de  $P$  le reste de la division de  $P$  par  $(X - \lambda)^2$ .

130.8

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

- Décomposer  $X^n - 1$  en facteurs irréductibles dans  $\mathbb{C}[X]$ .
- Décomposer  $X^n - 1$  en facteurs irréductibles dans  $\mathbb{R}[X]$ .

**130.9**

Déterminer les polynômes  $P$  vérifiant :

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

**130.10**

Soit  $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  un polynôme à coefficients entiers, tel que  $a_n \neq 0$  et  $a_0 \neq 0$ .

(a) On suppose que  $P$  admet une racine rationnelle  $r = \frac{p}{q}$  exprimée sous forme irréductible. Montrer que  $p \mid a_0$  et  $q \mid a_n$ .

(b) Factoriser dans  $\mathbb{R}[X]$  :

$$P = 2X^3 - X^2 - X - 3$$

### Petits problèmes d'entraînement

**130.11**

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

(a) Déterminer le PGCD des polynômes  $(X^n - 1)$  et  $(X - 1)^n$ .

(b) Montrer l'existence de  $U, V$  polynômes tels que :

$$(X^3 - 1)U + (X - 1)^3 V = (X - 1)$$

et déterminer explicitement de tels polynômes.

**130.12**

Montrer que, pour tout  $a, b \in \mathbb{N}^*$  :

$$b \mid a \iff X^b - 1 \mid X^a - 1$$

**130.13**

Soit  $P$  un polynôme réel non constant.

(a) On suppose que  $P$  est scindé à racines simples. Montrer que  $P'$  est aussi scindé.

(b) Montrer que le résultat perdure même si les racines de  $P$  ne sont pas simples.

(c) Le polynôme  $X^6 - X + 1$  est-il scindé sur  $\mathbb{R}$  ?

**130.14**

Soit  $n \in \mathbb{N}$  et  $f_n : [-1, 1] \rightarrow \mathbb{R}$  définie par :

$$f_n(x) = \cos(n \operatorname{Arccos} x)$$

(a) Soit  $x \in [-1, 1]$ . Simplifier les expressions  $f_0(x), f_1(x), f_2(x)$ .

Exprimer  $f_{n+1}(x) + f_{n-1}(x)$  en fonction de  $f_n(x)$ , et donner  $f_3(x)$ .

(b) Montrer qu'il existe un unique polynôme  $T_n \in \mathbb{R}[X]$  dont la fonction polynomiale associée coïncide avec  $f_n$  sur  $[-1, 1]$ .

(c) Donner le degré de  $T_n$  ainsi que son coefficient dominant.

(d) Montrer que  $T_n$  possède  $n$  racines distinctes, toutes dans  $] -1, 1[$ .

**130.15**

Pour  $n \in \mathbb{N}$ , on pose :

$$L_n = \frac{n!}{(2n)!} \frac{d^n}{dX^n} ((X^2 - 1)^n)$$

(a) Montrer que  $L_n$  est un polynôme unitaire, de degré  $n$ .

(b) Vérifier que, pour tout  $Q \in \mathbb{R}_{n-1}[X]$  :

$$\int_{-1}^1 L_n(t) Q(t) dt = 0$$

(c) En déduire que  $L_n$  possède  $n$  racines simples, toutes dans l'intervalle  $] -1, 1[$ .

**130.16**

Soit  $a \in \mathbb{R}$ ,  $n \in \mathbb{N}^*$  et  $P = (X + 1)^n - e^{2ina}$ .

(a) Déterminer les racines du polynôme  $P_n$ , ainsi que leurs multiplicités.

(b) En déduire la valeur de :

$$\prod_{k=0}^{n-1} \sin \left( a + \frac{k\pi}{n} \right)$$