N. Laillet
nlaillet.math@gmail.com

# Chapitre 16
# Polynômes

## 1 Anneau des polynômes à une indéterminée

Dans tout le chapitre, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

### 1.1 Construction

**Définition 1**

Un polynôme à coefficient dans $\mathbb{K}$ est une suite presque nulle d'éléments de $\mathbb{K}$, c'est-à-dire une suite nulle à partir d'un certain rang.
Deux polynômes sont égaux si et seulement si leurs coefficients sont tous égaux.

**Définition 2 (Somme et produit de polynômes)**

Soient $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ deux polynômes, soit $\lambda$ un élément de $\mathbb{K}$. On définit

**(i)** La somme de $P$ et $Q$ par $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$.

**(ii)** La multiplication de $P$ par $\lambda$ par $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$.

**(iii)** Le produit de $P$ et $Q$ par $P \times Q = (c_n)_{n\in\mathbb{N}}$ et

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

(produit de Cauchy/produit de convolution).

**(iv)** On définit enfin l'**indéterminée** $X = (\delta_{1,n})_{n\in\mathbb{N}}$.

**Proposition 3**

1. L'ensemble des polynômes à coefficients dans $\mathbb{K}$ muni de $+$ et de $\times$ est un anneau commutatif, de neutre pour $+$ la suite nulle et de neutre pour $\times$ la suite $(\delta_{0,n})_{n\in\mathbb{N}}$, notée 1.
2. Pour tout $p$ dans $\mathbb{N}$, $X^p = (\delta_{p,n})_{n\in\mathbb{N}}$.
3. Si $P = (a_n)_{n\in\mathbb{N}}$ est un polynôme, alors $P = \sum_{n=0}^{+\infty} a_n X^n$.

   On notera même $P(X) = \sum_{n=0}^{+\infty} a_n X^n$.

**Définition 4**

1. On note $\mathbb{K}[X]$ l'ensemble des suites presque nulles, appelées ici **ensemble des polynômes en une indéterminée.**
2. $(\mathbb{K}[X], +, \times)$ est donc l'anneau des polynômes en une indéterminée.

N. Laillet
nlaillet.math@gmail.com

**3.** Si $P \in \mathbb{K}[X]$, $P = P(X) = \sum_{n=0}^{+\infty} a_n X^n$, la suite $(a_n)_{n\in\mathbb{N}}$ est la suite des **coefficients** de $P$.

**4.** On dit que $(X^n)_{n\in\mathbb{N}}$ est la base canonique de $\mathbb{K}[X]$.

**Définition 5**

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

**1.** Si $P \neq 0_{\mathbb{K}[X]}$, alors $\{k \in \mathbb{N},\ a_k \neq 0\}$ est une partie non vide de $\mathbb{N}$, majorée : elle admet un plus grand élément $d$, appelé **degré** de $P$ et noté $\deg(P)$.

**2.** Si $P(X) = \sum_{k=0}^{d} a_k X^k$ et $a_d \neq 0$, alors $a_d$ est appelé coefficient dominant de $P$, $a_d X^d$ est appelé monôme dominant de $P$. Si $a_d = 1$, on dit que $P$ est unitaire.

**3.** Par convention, $\deg(0_{\mathbb{K}[X]}) = -\infty$.

**Proposition 6**

Soient $P$ et $Q$ dans $\mathbb{K}[X]^2$.

**1.** $\deg(P+Q) \leqslant \max(\deg(P), \deg(Q))$. Si $\deg(P) \neq \deg(Q)$, on a égalité.

**2.** $\deg(P \times Q) = \deg(P) + \deg(Q)$.

**3.** L'anneau $(\mathbb{K}[X], +, \times)$ est intègre.

**Définition 7**

Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X],\ \deg(P) \leqslant n\}$.

**Définition 8**

Soient $P$ et $Q$ deux polynômes, $P(X) = \sum_{k=0}^{n} a_k X^k$ et $Q(X) = \sum_{k=0}^{m} b_k X^k$. On définit la composée de $P$ et $Q$, notée $P \circ Q$, par

$$P \circ Q(X) = \sum_{k=0}^{n} a_k \left( \sum_{i=0}^{m} b_i X^i \right)^k .$$

**Proposition 9**

Si $Q$ n'est pas constant, $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

N. Laillet
nlaillet.math@gmail.com

## 1.2 Divisibilité et division euclidienne

**Définition 10**

Soient $A$ et $B$ deux polynômes à coefficients dans $\mathbb{K}$. On dit que $A$ divise $B$ et on écrit $A|B$ s'il existe $P \in \mathbb{K}[X]$ tel que $B = AP$.

**Proposition 11**

**(i)** La relation de divisibilité sur les polynômes est une relation réflexive et transitive.

**(ii)** Si $A$ divise $B$ et $B \neq 0_{\mathbb{K}[X]}$, alors $\deg(A) \leqslant \deg(B)$.

**(iii)** Pour tous $A$ et $B$ de $\mathbb{K}[X]$,

$$(A|B \text{ et } B|A) \Rightarrow (\exists \lambda \in \mathbb{K},\ A = \lambda B).$$

**Def.** Dans ce cas, on dit que $A$ et $B$ sont associés.

**(iv)** Si $A$ divise $B$ et $\deg(A) = \deg(B)$, alors $A$ et $B$ sont associés.

**(v)** Si $A$ divise $B$ et $A$ divise $C$, alors pour tous $U$ et $V$ polynômes de $\mathbb{K}[X]$, $A$ divise $BU + CV$.

**Théorème 12**

Soient $A$ et $B$ deux polynômes non nuls de $\mathbb{K}[X]$. Alors il existe deux polynômes $Q$ et $R$ tels que

$$A = BQ + R \text{ et } \deg(R) < \deg(B).$$

## 1.3 Fonctions polynomiales et racines

**Définition 13**

Soit $P$ un polynôme de $\mathbb{K}[X]$, $P(X) = \sum_{k=0}^{n} a_k X^k$. Soit $\alpha \in \mathbb{K}$. L'évaluation de $P$ en $\alpha$, notée $\alpha$, est l'élément de $\mathbb{K}$

$$P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k.$$

Cette expression permet de définit une **fonction polynomiale** sur $\mathbb{K}$.
Un élément $\alpha$ de $\mathbb{K}$ est une racine de $P$ si $P(\alpha) = 0_{\mathbb{K}}$.

**Proposition 14**

Soit $P$ dans $\mathbb{K}[X]$, $\alpha$ dans $\mathbb{K}$.

1. Le reste de la division euclidienne de $P$ par $X - \alpha$ est $P(\alpha)$.
2. $\alpha$ est racine de $P$ si et seulement si $X - \alpha$ divise $P$.

N. Laillet
nlaillet.math@gmail.com

**Définition 15 (Et prop)**

Soit $P$ dans $\mathbb{K}[X]$, $\alpha$ dans $\mathbb{K}$. L'ensemble $\{m \in \mathbb{N},\ (X-\alpha)^m | P\}$ possède un plus grand élément. On l'appelle multiplicité de $\alpha$ dans $P$.

- si cette multiplicité vaut 0, $\alpha$ n'est pas racine de $P$,
- si cette multiplicité vaut 1, on dit que $\alpha$ est une racine simple de $P$,
- si cette multiplicité est $\geqslant 2$, on dit que $\alpha$ est racine multiple de $P$.

**Proposition 16**

Soit $P$ dans $\mathbb{K}[X]$, $\alpha$ dans $\mathbb{K}$. $m \in \mathbb{N}$. Les assertions suivantes sont équivalentes :

1. $\alpha$ est de multiplicité $m$ dans $P$.
2. $(X-\alpha)^m$ divise $P$ mais $(X-\alpha)^{m+1}$ ne divise pas $P$.
3. Il existe $Q$ dans $\mathbb{K}[X]$ tel que $P(X) = (X-\alpha)^m Q(X)$ et $Q(\alpha) \neq 0$.

**Proposition 17**

1. Soient $P$ et $Q$ dans $\mathbb{K}[X]$, $\alpha \in \mathbb{K}$. Si $m$ est la multiplicité de $\alpha$ dans $P$ et $n$ la multiplicité de $\alpha$ dans $Q$, alors la multiplicité de $\alpha$ dans $PQ$ est $m+n$.
2. Soit $P$ dans $\mathbb{K}[X]$ et $\alpha_1, \dots, \alpha_n$ $n$ éléments de $\mathbb{K}$, de multipicités respectives $m_1, \dots, m_n$. Alors $(X-\alpha_1)^{m_1} \dots (X-\alpha_n)^{m_n}$ divise $P$.

**Proposition 18**

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

1. Si $P$ est non nul, $P$ a au plus $\deg(P)$ racines distinctes.
2. Si $P \in \mathbb{K}_n[X]$ et $P$ admet au moins $n+1$ racines distinctes.
3. Si $P$ s'annule une infinité de fois sur $\mathbb{K}$, $P = 0_{\mathbb{K}[X]}$.
4. Si $P$ est non nul, $P$ a au plus $\deg(P)$ racines comptées avec multiplicité.

**Proposition 19**

Si $P \neq 0_{\mathbb{K}[X]}$, si $n = \deg(P)$, si $(\alpha_1, \dots, \alpha_r)$ sont $r$ racines de $P$, de multiplicités respectives au moins égales à $(m_1, \dots, m_r)$, si $m_1 + \dots + m_r = n$, alors

$$P(X) = C \prod_{i=1}^{r} (X-\alpha_i)^{m_i},$$

où $C \in \mathbb{K}$ est le coefficient dominant de $P$.

N. Laillet
nlaillet.math@gmail.com

## 1.4 Polynômes scindés

**Définition 20**

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

1. On dit que $P$ est scindé s'il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{K}^n$, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$, $C \in \mathbb{K}$ tels que
$$P = C \prod_{i=1}^{r} (X - \alpha_i)^{m_i}.$$
2. Si de plus $m_1 = \dots = m_r = 1$, on dit que $P$ est simplement scindé ou bien scindé à racines simples (srs).

**Proposition 21**

1. $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}})$.
2. Si $a = \rho e^{i\theta} \in \mathbb{C}$, si on note $z_0 = \sqrt[n]{\rho} e^{i\frac{\theta}{n}}$, alors $X^n - a = \prod_{\omega \in \mathbb{U}_n} (X - z_0\omega)$.

**Proposition 22**

Soient $P$ et $Q$ des polynômes scindés. Alors $P$ divise $Q$ si et seulement si toute racine de $P$ est racine de $Q$ avec une multiplicité supérieure ou égale.

**Proposition 23 (Relations de Viète ou coefficients-racines)**

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé, $\alpha_1, \dots, \alpha_n$ ses racines (**comptées avec multiplicité**, c'est-à-dire répétées si ce sont des racines multiples). On définit, pour $k$ dans $[\![1, n]\!]$,
$$\sigma_k = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \alpha_{i_1} \dots \alpha_{i_k}.$$
Alors pour tout $k$ dans $[\![1, n]\!]$,
$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}.$$

N. Laillet
nlaillet.math@gmail.com

## 1.5 Dérivation

**Définition 24**

Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme. On appelle polynôme dérivé de $P$ le polynôme nommé $P'$ et défini par $P'(X) = \sum_{k=1}^{n} k a_k X^{n-1} = \sum_{\ell=0}^{n-1} (\ell+1) a_{\ell+1} X^{\ell}$. On définit aussi la dérivée $n$-ième de $P$ par récurrence.

**Proposition 25**

Pour tous $P$ et $Q$ polynômes de $\mathbb{K}[X]$, pour tous $\lambda$ et $\mu$ dans $\mathbb{K}$ et $n$ dans $\mathbb{N}$,

**(i) Dérivée première.**

1. $\deg(P') = \deg(P) - 1$ si $\deg(P) \geqslant 1$. Sinon $\deg(P') = -\infty$.
2. $(\lambda P + \mu Q)' = P' + Q'$
3. $(PQ)' = P'Q + PQ'$
4. $(P \circ Q)' = Q' \times P' \circ Q$

**(ii) Dérivée $n$-ième.** Soit $n \in \mathbb{N}$.

1. $\deg(P^{(n)}) = \begin{cases} \deg(P) - n \text{ si } n \leqslant \deg(P), \\ -\infty \text{ sinon.} \end{cases}$
2. $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.
3. $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

**Proposition 26**

Soit un polynôme scindé $P(X) = K \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$. Alors $P'(X) = K \sum_{i=1}^{r} m_i (X - \alpha_i)^{m_i - 1} \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - \alpha_j)^{m_j}$.

**Proposition 27 (Formule de Taylor pour les polynômes)**

Soit $P \in \mathbb{K}[X]$, $\deg(P) = n$, $\alpha$ dans $\mathbb{K}$. Alors $P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k = \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!} (X - \alpha)^k$.

**Proposition 28**

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$, $m \in \mathbb{N}^*$.

1. Si $\alpha$ est une racine de $P$ de multiplicité $m$, alors $\alpha$ est une racine de $P'$ de multiplicité $m - 1$.
2. $\alpha$ est de multiplicité $m$ dans $P$ si et seulement si $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$ **et** $P^{(m)}(\alpha) \neq 0$.
3. $\alpha$ est de multiplicité au moins $m$ dans $P$ si et seulement si $P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0$.

**Proposition 29**

Soit $P \in \mathbb{R}[X]$, $\alpha$ une racine de $P$, complexe non réelle. Alors $\overline{\alpha}$ est une racine de $P$ de même multiplicité que $\alpha$.

N. Laillet
nlaillet.math@gmail.com

# 2 Arithmétique dans $\mathbb{K}[X]$

## 2.1 PGCD, PPCM, polynômes premiers entre eux

**Définition 30**

Soient $A$ et $B$ deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. Un pgcd de $A$ et $B$ est un diviseur commun de $A$ et $B$ de degré maximal.

**Proposition 31 (Proposition de Bézout)**

Soient $A$ et $B$ deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls.

1. Si $D$ est un pgcd de $A$ et $B$, alors il existe $(U, V)$ dans $\mathbb{K}[X]$ tels que $D = AU + BV$.
2. Tous les pgcd de $A$ et $B$ sont associés.
3. Si $D$ est un pgcd de $A$ et $B$, si $P$ est un polynôme vérifiant $P|A$ et $P|B$, alors $P|D$.

**Définition 32**

On note $A \wedge B$ l'unique pgcd **unitaire** de $A$ et $B$. Par convention, $0 \wedge 0 = 0$.

**Proposition 33**

Soient $A$, $B$, $C$ dans $\mathbb{K}[X]$.

1. Si $A = BQ + R$, alors $A \wedge B = B \wedge R$.
2. $(AB) \wedge (AC)$ et $A(B \wedge C)$ sont associés.
3. (associativité) $A \wedge (B \wedge C) = (A \wedge B) \wedge C$, que l'on note $A \wedge B \wedge C$.

**Proposition 34 (Algorithme d'Euclide)**

Soient $A$ et $B$ dans $\mathbb{K}[X]$, non tous deux nuls. On définit la suite $(R_n)_{n\in\mathbb{N}}$ par $R_0 = A$, $R_1 = B$ et, pour $n \in \mathbb{N}$,

- si $R_{n+1} = 0$, $R_{n+2} = 0$,
- sinon, $R_{n+2}$ est le reste de la division euclidienne de $R_n$ par $R_{n+1}$

Alors $(R_n)_{n\in\mathbb{N}}$ est de degré strictement décroissant, jusqu'à être stationnaire égale au polynôme nul. Si $N$ vérifie $R_N \neq 0_{\mathbb{K}[X]}$ et $R_{N+1} = 0_{\mathbb{K}[X]}$, alors $R_N$ est un pgcd de $A$ et $B$.

**Définition 35**

Deux polynômes $A$ et $B$ sont premiers entre eux si $A \wedge B = 1$.

**Théorème 36 (Bézout)**

Deux polynômes $A$ et $B$ sont premiers entre eux si et seulement s'il existe $U$ et $V$ deux polynômes tels que $AU + BV = 1$.

N. Laillet
nlaillet.math@gmail.com

**Proposition 37 (Théorème de Gauss)**

Soient $A$, $B$ et $C$ trois polynômes.

1. Si $A$ divise $BC$ et $A \wedge B = 1$ alors $A$ divise $C$.
2. Si $A$ divise $C$, si $B$ divise $C$ et si $A \wedge B = 1$, alors $AB$ divise $C$.

**Proposition 38**

Soient $A$ et $B$ deux polynômes non tous deux nuls. Si $S$ est le quotient de $A$ par $A \wedge B$ et $T$ est le quotient de $B$ par $A \wedge B$, alors $S \wedge T = 1$.

**Définition 39**

Soient deux polynômes de $\mathbb{K}[X]$ non tous les deux nuls. Un PPCM de $A$ et $B$ est un multiple commun à $A$ et à $B$ de degré minimal.

**Proposition 40**

Soient $A$ et $B$ dans $\mathbb{K}[X]$, tous deux non nuls.

1. Si $M$ est le quotient de $A \times B$ par $A \wedge B$, alors $M$ est un ppcm de $A$ et $B$.
2. Tous les ppcm de $A$ et $B$ sont associés. On note $A \vee B$ le ppcm unitaire de $A$ et $B$.
3. Si $N$ est un ppcm de $A$ et $B$, si $P$ est un multiple commun de $A$ et $B$, alors $M$ divise $P$.

**Définition 41**

1. Un pgcd de $n$ polynômes $P_1, \dots, P_n$ est un diviseur commun $D$ à $P_1, \dots, P_n$ de degré maximal. Tout diviseur commun à $P_1, \dots, P_n$ est alors un diviseur de $D$.
2. On définit, de la même manière, un ppcm de $P_1, \dots, P_n$.

**Proposition 42**

1. Tous les pgcd de $P_1, \dots, P_n$ sont associés. On note l'unique pgcd unitaire de $P_1, \dots, P_n$ $P_1 \wedge \dots \wedge P_n$.
2. Il existe $n$ polynômes $U_1, \dots, U_n$ tels que $U_1 P_1 + \dots + U_n P_n = P_1 \wedge \dots \wedge P_n$.

**Définition 43**

$P_1, \dots, P_n$ sont dits premiers entre eux dans leur ensemble si $P_1 \wedge \dots \wedge P_n = 1$.

**Théorème 44 (Bézout)**

$P_1, \dots, P_n$ sont premiers entre eux dans leur ensemble ssi il existe $n$ polynômes $U_1, \dots, U_n$ tels que $U_1 P_1 + \dots + U_n P_n = 1$.

N. Laillet
nlaillet.math@gmail.com

## 2.2 Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$, factorisation

**Définition 45**

Un polynôme $P$ de $\mathbb{K}[X]$ est irréductible si $P$ n'est pas constants et si ses seuls diviseurs sont soit constants non nuls, soit les polynômes associés à $P$.

**Proposition 46**

1. $\forall \alpha \in \mathbb{K}$, $X-\alpha$ est irréductible.
2. Si $\deg(P) \geqslant 2$ et $P$ s'annule sur $\mathbb{K}$, alors $P$ n'est pas irréductible.
3. Sur $\mathbb{R}$, tout polynôme de degré 2 de discriminant $<0$ est irréductible.

**Théorème 47 (D'Alembert-Gauss)**

Soit $P \in \mathbb{C}[X]$, non constant. Alors il existe $\alpha \in \mathbb{C}$ tel que $P(\alpha)=0$.
Les seuls polynômes irréductibles sur $\mathbb{C}$ sont donc les polynômes de degré 1.

**Théorème 48 (Décomposition en produit d'irréductibles sur $\mathbb{C}$)**

Soit $P \in \mathbb{C}[X]$, non nul. Alors il existe $K \in \mathbb{C}$, $r \in \mathbb{N}$, $(\alpha_1,\dots,\alpha_r) \in \mathbb{C}^r$, deux à deux distincts, $(m_1,\dots,m_r) \in (\mathbb{N}^*)^r$, tels que

$$P(X) = K\prod_{i=1}^{r}(X-\alpha_i)^{m_i}.$$

Cette décomposition est unique à permutation des racines près. De plus,

- $K$ est le coefficient dominant de $P$,
- $\deg(P) = m_1+\dots+m_r$.

**Théorème 49 (Décomposition en produit d'irréductibles sur $\mathbb{R}$.)**

Soit $P \in \mathbb{R}[X]$, non nul. Alors il existe

- $K \in \mathbb{R}^*$,
- $r \in \mathbb{N}$, $(\alpha_1,\dots,\alpha_r) \in \mathbb{R}$, deux à deux distincts, $(m_1,\dots,m_r) \in (\mathbb{N}^*)^r$,
- $s \in \mathbb{N}$, $\Big((b_1,c_1),\dots,(b_s,c_s)\Big) \in (\mathbb{R}^2)^s$, deux à deux distincts, vérifiant $\forall i \in [\![1,s]\!]$, $b_i^2-4c_i<0$, $(n_1,\dots,n_s) \in (\mathbb{N}^*)^s$

tels que

$$P(X) = K\left(\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\right)\cdot\left(\prod_{j=1}^{s}(X^2+b_jX+c_j)^{n_j}\right)$$

De plus, cette décomposition est unique à permutation près, $\Lambda$ est le coefficient dominant de $P$ et $\deg(P) = \sum_{i=1}^{r} m_i + 2\sum_{j=1}^{s} n_j$.

N. Laillet
nlaillet.math@gmail.com

**Proposition 50 (Conséquences arithmétiques)**

Soient $P$ et $Q$ scindés (cette condition est inutile sur $\mathbb{C}[X]$).

1. $P$ divise $Q$ si et seulement si pour tout réel $\alpha$, la multiplicité de $\alpha$ dans $P$ est inférieure ou égale à la multiplicité de $\alpha$ dans $Q$.
2. Si $P(X) = \prod_{i=1}^{r}(X - \alpha_i)^{m_i}$ et $Q(X) = \prod_{i=1}^{r}(X - \alpha_i)^{n_i}$, avec certains exposants éventuellement nuls, alors
$$P \wedge Q = \prod_{i=1}^{r}(X - \alpha_i)^{\min(m_i, n_i)} \text{ et } P \vee Q = \prod_{i=1}^{r}(X - \alpha_i)^{\max(m_i, n_i)}.$$
3. $P$ et $Q$ sont premiers entre eux si et seulement s'ils n'ont pas de racine en commun.
4. En particulier, $P$ est scindé à racines simples si et seulement si $P \wedge P' = 1$.

# 3 Formule d'interpolation de Lagrange

**Proposition 51**

Soit $(x_0 \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts.
Pour tout $k$ dans $[\![0, n]\!]$, il existe un unique $L_k$ dans $\mathbb{K}_n[X]$ tel que : $\forall i \in [\![0, n]\!],\ L_k(x_i) = \delta_{ik}$. On a, plus précisément, $L_k = \prod_{\substack{1 \leqslant i \leqslant n \\ i \neq k}} \frac{X - x_k}{x_i - x_k}$.
On dit que $(L_0, \dots, L_n)$ est la base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$.

**Théorème 52 (Théorème d'interpolation de Lagrange)**

Soit $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts. Soit $(y_0, \dots, y_n) \in \mathbb{K}^{n+1}$.
Alors il existe un unique polynôme $P$ dans $\mathbb{K}_n[X]$ tel que : $\forall i \in [\![0, n]\!],\ P(x_i) = y_i$.
On a, précisément, $P = \sum_{k=0}^{n} y_k L_k$, où $(L_0, \dots, L_n)$ est la base d'interpolation de Lagrange associée à $(x_0, \dots, x_n)$.

**Proposition 53**

Soit $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts, $(L_0, \dots, L_n)$ la base d'interpolation de Lagrange associée. Alors pour tout $P$ dans $\mathbb{K}_n[X]$, $P = \sum_{k=0}^{n} P(x_k) L_k$.

**Proposition 54**

Soit $(x_0, \dots, x_n) \in \mathbb{K}^{n+1}$, deux à deux distincts, $(y_0, \dots, y_n) \in \mathbb{K}^{n+1}$. Soit $P$ l'unique polynôme de $\mathbb{K}_n[X]$ valant $y_i$ en chaque $x_i$. Alors
$$\{Q \in \mathbb{K}[X],\ \forall i \in [\![0, n]\!],\ Q(x_i) = y_i\} = \left\{P + R \times \prod_{i=0}^{n}(X - x_i),\ R \in \mathbb{K}[X]\right\}.$$