Chapitre 18 : Polynômes

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

I. $\mathbb{K}[X]$

I.1. Polynômes à une indéterminée

Définition I.1. Un **polynôme** à coefficients dans $\mathbb{K}$ est une expression de la forme

$$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n = \sum_{k=0}^{n} a_k X^k,$$

où $n \in \mathbb{N}$ et $a_0, a_1, \ldots, a_n \in \mathbb{K}$.
On appelle X l'**indéterminée** du polynôme et on pose $X^0 = 1$ par convention.
Les a_i sont les **coefficients** du polynôme.
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ d'indéterminée X.
Le **polynôme nul** est le polynôme $P = 0$ dont tous les coefficients sont nuls.
Un **polynôme constant** est un polynôme dont seul le premier coefficient peut-être non nul.
Un **monôme** est un polynôme qui n'a qu'un seul coefficient non nul.

Remarques I.1.
- Attention, la lettre X n'est pas une variable, ce n'est qu'une notation. On ne peut pas la remplacer par un nombre.
- On notera parfois $P(X)$ à la place de P.

Proposition I.1 (Identification des coefficients). *Deux polynômes P et Q sont égaux si et seulement si ils ont les mêmes coefficients.*

Remarque I.2. On peut donc résumer un polynôme à une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ qui sont tous nuls à partir d'un certain rang : $(a_k) = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$.

Définition I.2. Soit P un polynôme à coefficients dans $\mathbb{K}$. Le **degré** de P est :
- $\deg(P) = -\infty$ si $P = 0$;
- $\deg(P) = n$ si $P = a_0 + a_1 X + \ldots + a_n X^n$, avec $a_n \neq 0$.
  Dans ce cas, a_n est le **coefficient dominant** de P.
  Si $a_n = 1$, on dit que P est **unitaire**.

On note $\mathbb{K}_n[X]$ le sous-ensemble de $\mathbb{K}[X]$ constitué des polynômes de degré inférieur ou égal à n.

I.2. Opérations sur les polynômes

Définition I.3. Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ deux polynômes à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. On définit les polynômes :
- $\lambda P = \sum_{k=0}^{n} \lambda a_k X^k$;
- $P + Q = \sum_{k=0}^{\max(n,m)} c_k X^k$, où $c_k = a_k + b_k$;
- $P \times Q = \sum_{k=0}^{n+m} c_k X^k$, où $c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$.

Remarque I.3. On admet que l'addition et la multiplication vérifient les mêmes propriétés que celles de $\mathbb{Z}$: elles sont associatives, ont un élément neutre et sont distributives, et tous les polynômes ont un inverse par $+$, de sorte que $(\mathbb{K}[X], +, \times)$

est un anneau. Ce n'est pas un corps car le polynôme $P = X$ n'a pas d'inverse pour $\times$: il n'existe pas de polynôme Q tel que $X \times Q = 1$.
Pour résumer : on ajoute et on multiplie les polynômes comme on a naturellement envie de le faire. On fait simplement attention à ne pas diviser par un polynôme.
En particulier la formule du binôme de Newton est vraie pour des polynômes.

Définition I.4. Soient $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ deux polynômes à coefficients dans $\mathbb{K}$. On définit la **composée** de P et Q par :

$$P \circ Q = a_0 + a_1 Q + a_2 Q^2 + \ldots + a_n Q^n$$

Proposition I.2. *Soient P et Q deux polynômes non nuls, $\lambda \in \mathbb{K}^*$ et $N \in \mathbb{N}$.*

1. $\deg(\lambda P) = \deg P$;
2. $\deg(P+Q) \leq \max\{\deg P, \deg Q\}$. *De plus, si $\deg P \neq \deg Q$, alors il y a égalité, sinon, il faut comparer les coefficients dominants de P et Q ;*
3. $\deg(PQ) = \deg P + \deg Q$;
4. $\deg(P^N) = N \deg P$;
5. $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Remarque I.4. Si un des polynômes est nul, les degrés précédents sont faciles à calculer.

Proposition I.3. *Soient $P, Q \in \mathbb{K}[X]$: $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$.*
On dit que $\mathbb{K}[X]$ est ***intègre****.*

Corollaire I.4. *Soient $P, Q, R \in \mathbb{K}[X]$ avec $P \neq 0$: $PQ = PR \Rightarrow Q = R$.*

I.3. Dérivation formelle des polynômes

Définition I.5. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$. On appelle **polynôme dérivé** de P le polynôme P' défini par :

$$P' = \sum_{k=0}^{n} k a_k X^{k-1} = \begin{cases} 0 & \text{si } \deg P \leq 0 \\ a_1 + 2a_2 X + \ldots + n a_n X^{n-1} & \text{si } \deg(P) \geq 1 \end{cases}$$

On définit les **polynômes dérivés successifs** par $P^{(0)} = P$ et pour tout $k \in \mathbb{N}^*$, $P^{(k)} = \left(P^{(k-1)}\right)'$.

Proposition I.5. *Soit $P \in \mathbb{K}[X]$ et $m \in \mathbb{N}$.*

1. $\deg P' = \begin{cases} -\infty & \text{si } \deg P \leq 0 \\ \deg P - 1 & \text{si } \deg P \geq 1 \end{cases}$
2. $m \leq \deg P \Rightarrow \deg P^{(m)} = \deg(P) - m$.
3. $m > \deg P \iff P^{(m)} = 0$.

Remarque I.5. En particulier, $\mathbb{K}_n[X]$ est l'ensemble des polynômes P tels que $P^{(n+1)} = 0$.

Proposition I.6. *Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.*

1. $(P+Q)' = P' + Q'$
2. $(\lambda P)' = \lambda P'$
3. $(PQ)' = P'Q + PQ'$
4. $(P \circ Q)' = Q' \times P' \circ Q$.

Théorème I.7 (Formule de Leibniz)

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

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

II. Arithmétique dans $\mathbb{K}[X]$

II.1. Divisibilité dans $\mathbb{K}[X]$

Définition II.1. Soient $A, B \in \mathbb{K}[X]$. On dit que B **divise** A si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B|A$, et B est un **diviseur** de A et A un **multiple** de B.

Proposition II.1. *Soient $A, B, C, D \in \mathbb{K}[X]$ et $n \in \mathbb{N}^*$.*

$$\begin{cases} A|B \\ B|C \end{cases} \Rightarrow A|C \qquad \begin{cases} A|B \\ A|C \end{cases} \Rightarrow \forall (P, Q) \in \mathbb{K}[X]^2, A|PB+QC \qquad \begin{cases} A|C \\ B|D \end{cases} \Rightarrow AB|CD.$$

Remarques II.1.

- Tous les polynômes divisent le polynôme nul.
- Les polynômes de degré 0 divisent tous les polynômes.

Proposition II.2. *Soient $A, B \in \mathbb{K}[X]$. Si A est non nul et B divise A, alors* $\deg B \leq \deg A$.

Proposition II.3. *Soient $A, B \in \mathbb{K}[X]$ non nuls. Alors :*

$$(A|B \text{ et } B|A) \iff \exists \lambda \in \mathbb{K}^* \mid B = \lambda A.$$

On dit alors que A et B sont ***associés****.*

II.2. Division euclidienne de polynômes

Effectuons la division euclidienne de $2X^4 + X^3 - X^2 + X + 1$ par $2X^2 - X - 2$. Il s'agit de procéder par étapes : à chaque étape, on élimine le monôme de plus haut degré.
On choisit généralement de représenter ces étapes successives de la manière suivante :

- Pour la première étape :

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

- Division complète :

$$
\begin{array}{rrrrr|l}
2X^4 & +X^3 & -X^2 & +X & +1 & 2X^2-X-2 \\ \cline{6-6}
-(2X^4 & -X^3 & -2X^2) & & & \\ \cline{1-5}
 & & & & & \underbrace{X^2+X+1}_{\text{Quotient}} \\
 & 2X^3 & +X^2 & +X & +1 & \\
 & -(2X^3 & -X^2 & -2X) & & \\ \cline{1-5}
 & & 2X^2 & +3X & +1 & \\
 & & -(2X^2 & -X & -2) & \\ \cline{1-5}
 & & & \underbrace{4X+3}_{\text{Reste}} & &
\end{array}
$$

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

Théorème II.4 (Division euclidienne)

Soient A et B deux polynômes de $\mathbb{K}[X]$ tels que $B \neq 0$. Il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que :

$$A = BQ + R \quad \textit{et} \quad \deg R < \deg B$$

*Q est le **quotient** et R le **reste** de la division euclidienne de A par B.*

Remarque II.2. B divise A si et seulement si le reste de la division de A par B est le polynôme nul.

Le jeu est maintenant comme pour les entiers : comment peut-on exprimer un polynôme P comme produit de polynômes les plus simples possible (« premier ») ?

II.3. Polynômes irréductibles

Définition II.2. Un polynôme $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ si et seulement si $\deg P \geq 1$ et P n'admet comme diviseurs dans $\mathbb{K}[X]$ que les polynômes constants et les polynômes associés à P.

Proposition II.5. *Tout polynôme de degré 1 de $\mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$.*

Théorème II.6

Tout polynôme P de $\mathbb{K}[X]$ non constant se décompose en un produit de facteurs irréductibles unitaires de $\mathbb{K}[X]$: il existe $\lambda \in \mathbb{K}^*$ et $P_1, P_2 \dots, P_m \in \mathbb{K}[X]$ unitaires et irréductibles et $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{N}^*$ tels que $P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m}$.
De plus, cette décomposition est unique à l'ordre des facteurs près.

Toute la question est de savoir quels sont les polynômes irréductibles.

III. Racines d'un polynôme

III.1. Fonctions polynomiales

Définition III.1. Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients dans $\mathbb{K}$. La **fonction polynomiale** associée à P est la fonction f définie sur $\mathbb{K}$ par :

$$f : \left\{ \begin{array}{ccl} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & a_0 + a_1 x + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k \end{array} \right.$$

Remarque III.1. On notera souvent P à la fois le polynôme et sa fonction polynomiale. On verra dans le paragraphe III.2 que ce n'est pas un gros abus de notation. On peut déjà remarquer

- que la fonction polynomiale associée à la somme/au produit/à la composée de deux polynômes est la même que la somme/le produit/la composée des fonctions polynomiales des deux polynômes,
- que $P^{(k)}$ est la dérivée k-ième de la fonction polynomiale de P lorsque $\mathbb{K} = \mathbb{R}$.

Lemme III.1. *Soient $n, p \in \mathbb{N}$ et $a \in \mathbb{K}$.*

$$\left((X-a)^n\right)^{(p)} = \begin{cases} 0 & \text{si } p > n \\ n! & \text{si } p = n \\ \dfrac{n!}{(n-p)!}(X-a)^{n-p} & \text{si } p < n. \end{cases}$$

Théorème III.1 (Formule de Taylor)

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré n et $\alpha \in \mathbb{K}$.

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

En particulier,

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

donc pour tout $k \in [\![0, n]\!]$, $a_k = \dfrac{P^{(k)}(0)}{k!}$.

Remarque III.2. Attention : ici $P^{(k)}(\alpha)$ se calcule en faisant la dérivée formelle k fois puis en prenant la fonction polynomiale associée.

III.2. Racines d'un polynôme

Définition III.2. Soit $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. On dit que α est une **racine** de P si $P(\alpha) = 0$.

Proposition III.2. *Soient $\alpha \in \mathbb{K}$ et $P \in \mathbb{K}[X]$.*

$$\alpha \text{ est une racine de } P \iff (X-\alpha) | P.$$

Remarques III.3.

- Comme l'ensemble $\{k \in \mathbb{N}^* \mid (X-\alpha)^k | P\}$ est non vide et majoré par $\deg P$, il admet un plus grand élément, donc la multiplicité m est bien définie.
- De plus, $(X-\alpha)^m | P$ et $(X-\alpha)^{m+1} \nmid P$.

Définition III.3. Soit $P \in \mathbb{K}[X]$ non nul et $\alpha \in \mathbb{K}$ une racine de P. On appelle **multiplicité** de α le plus grand entier $m \in \mathbb{N}^*$ tel que $(X-\alpha)^m | P$.

Proposition III.3. *Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}$. Alors α est racine de P de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $Q(\alpha) \neq 0$ et $P = (X-\alpha)^m Q$.*

Proposition III.4. *Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P. La multiplicité de α est le nombre m qui vérifie $P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$ et $P^{(m)}(\alpha) \neq 0$, autrement dit, $m = \min\{k \in \mathbb{N}^* \mid P^{(k)}(\alpha) \neq 0\}$.*

III.3. Nombre maximal de racines

Théorème III.5

Soient $P \in \mathbb{K}[X]$ non nul et $r \geq 1$ un entier. Si $\alpha_1, \alpha_2, \ldots, \alpha_r$ sont des racines distinctes de P de multiplicités respectives $m_1, m_2, \ldots, m_r$, alors P est divisible par $(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\ldots(X-\alpha_r)^{m_r}$.

Corollaire III.6. *Soient $P, Q \in \mathbb{K}_n[X]$.*

1. *Si P admet $n+1$ racines comptées avec multiplicités, alors P est le polynôme nul. Autrement dit, si P est non nul, alors il admet au maximum n racines comptées avec multiplicités.*
2. *Si P admet une infinité de racines, alors $P = 0$.*
3. *Si les fonctions polynomiales associées à P et Q coïncident en $n+1$ points de $\mathbb{K}$, alors $P = Q$.*
4. *Si les fonctions polynomiales associées à P et Q coïncident en une infinité de points de $\mathbb{K}$, alors $P = Q$.*
5. *L'application $\varphi : P \in \mathbb{K}[X] \mapsto f \in \{$fonctions polynomiales$\}$ est une bijection.*

IV. Factorisation des polynômes de $\mathbb{K}[X]$

IV.1. Polynômes scindés

Définition IV.1. Un polynôme $P \in \mathbb{K}[X]$ de degré au moins 1 est dit **scindé** sur $\mathbb{K}$ s'il peut s'écrire comme un produit de polynômes de degré 1.

Proposition IV.1. *Un polynôme de degré $n \geq 1$ est scindé sur $\mathbb{K}$ si et seulement si il possède exactement n racines dans $\mathbb{K}$ comptées avec multiplicités.*

Remarque IV.1. Lorsque P est scindé sur $\mathbb{K}$, on peut donc le factoriser sous la forme $P = \lambda \prod_{k=1}^{r}(X-\alpha_k)^{m_k}$, avec $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$. Dans ce cas, λ est le coefficient dominant de P.
On peut aussi écrire $P = \lambda \prod_{k=1}^{n}(X-\alpha_k)$, où les α_k ne sont pas forcément distincts.

Pour un polynôme scindé dont on connaît ses racines, on peut retrouver ses coefficients en développant l'expression précédente.
Par exemple, si P est de degré 2 et a deux racines α_1 et α_2, alors :

$$P = aX^2 + bX + c = a(X-\alpha_1)(X-\alpha_2) = aX^2 - a(\alpha_1+\alpha_2)X + a\alpha_1\alpha_2.$$

Donc on a les relations : $\alpha_1 + \alpha_2 = -\frac{b}{a}$ et $\alpha_1\alpha_2 = \frac{c}{a}$.

Proposition IV.2 (Relations coefficients-racines). *Soit $P = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{K}[X]$ scindé de degré n et notons $\alpha_1, \ldots, \alpha_n$ ses racines. Alors*

$$\alpha_1 + \alpha_2 + \ldots + \alpha_n = -\frac{a_{n-1}}{a_n}$$
$$\alpha_1\alpha_2\ldots\alpha_n = (-1)^n\frac{a_0}{a_n}$$

IV.2. Lorsque $\mathbb{K} = \mathbb{C}$

Théorème IV.3 (d'Alembert-Gauss)

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

Corollaire IV.4. *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*
En particulier, tout polynôme $P \in \mathbb{C}[X]$ se factorise sous la forme :

$$P = \lambda \prod_{k=1}^{m} (X - \alpha_k)^{m_k}$$

Autrement dit, tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Exemple IV.1. Les racines du polynôme $X^n - 1$ sont les racines n-ièmes de l'unité, donc $X^n - 1 = \prod_{k=0}^{n-1} \left(X - \mathrm{e}^{\frac{2ik\pi}{n}}\right)$.

IV.3. Lorsque $\mathbb{K} = \mathbb{R}$

Lemme IV.1. *Soit $P \in \mathbb{R}[X]$ et $\alpha \in \mathbb{C}$. Alors pour tout $k \in \mathbb{N}$, $\overline{P^{(k)}(\alpha)} = P^{(k)}(\overline{\alpha})$.*

Proposition IV.5. *Soit $P \in \mathbb{R}[X]$. Si $\alpha \in \mathbb{C}$ est racine de P, alors $\overline{\alpha}$ est aussi racine de P. De plus, α et $\overline{\alpha}$ ont la même multiplicité.*

Proposition IV.6. *Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.*

Corollaire IV.7. *Soit $P \in \mathbb{R}[X]$. La décomposition de P dans $\mathbb{R}[X]$ est de la forme :*

$$P = \lambda \prod_{k=1}^{r} (X - \alpha_k)^{m_k} \prod_{k=1}^{s} (X^2 + b_k X + c_k)^{n_k}$$

où $\lambda \in \mathbb{R}^*$, $\alpha_k \in \mathbb{R}$, $b_k, c_k \in \mathbb{R}$ avec $b_k^2 - 4c_k < 0$.

V. Décomposition en éléments simples d'une fraction rationnelle

Théorème V.1

Soit P et Q deux polynômes de $\mathbb{K}[X]$ non nuls, et B le quotient de P par Q. On suppose que $Q = \lambda \prod_{k=1}^{n} (X - \alpha_k)$ est scindé à racines simples. Alors il existe un unique $(b_1, \ldots, b_n) \in \mathbb{K}^n$ tel que :

$$\frac{P}{Q} = B + \sum_{k=1}^{n} \frac{b_k}{X - \alpha_k}.$$