Chapitre 16

Polynômes

Mathieu Mansuy - Professeur de Mathématiques en supérieures PCSI au Lycée Saint Louis (Paris)
mansuy.mathieu@hotmail.fr

1 Ensemble $\mathbb{K}[X]$

Dans tout le chapitre $\mathbb{K}$ désigne l'ensemble des nombres réels $\mathbb{R}$ ou des nombres complexes $\mathbb{C}$.

1.1 Définitions

Définition.

- On appelle **polynôme P à coefficients dans** $\mathbb{K}$ toute suite (a_n) d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang, c'est à dire
$$\exists N \in \mathbb{N}, \forall n \geq N, a_n = 0.$$
- Les éléments de la suite (a_n) s'appellent les **coefficients du polynôme** P.

Remarque. Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux. En particulier, un polynôme est nul si et seulement si tous ses coefficients sont nuls.

Définition.

Soient $P = (a_n)$ et $Q = (b_n)$ deux polynômes à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. On définit

- la somme : $P + Q = (a_n + b_n)$
- le produit de P par λ : $\lambda \cdot P = (\lambda a_n)$
- le produit des polynômes : $P \times Q = (c_n)$ où pour tout $n \in \mathbb{N}$, c_n est défini par
$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{i+j=n} a_i b_j.$$

Remarque. Le produit des polynômes $P \times Q = (c_n)$ est bien encore un polynôme comme le montre la proposition suivante :

Propriété 1

Soient $P = (a_0, a_1, \cdots, a_p, 0, 0, \cdots)$ et $Q = (b_0, b_1, \cdots, b_q, 0, 0, \cdots)$ deux polynômes à coefficients dans $\mathbb{K}$, et considérons $P \times Q = (c_n)$ le produit de ces polynômes. Alors :

(1) $c_k = 0$ pour tout $k > p + q$;

(2) $c_{p+q} = a_p b_q$.

Preuve.

(1) Supposons $k > p + q$. Alors si $i + j = k$, on a $i > p$ ou $j > q$, et donc $a_i = 0$ ou $b_j = 0$. On en déduit alors
$$c_k = \sum_{i+j=k} a_i b_j = 0.$$

(2) Si $k = p + q$, on a :
$$c_k = \sum_{i=0}^{p-1} a_i b_{k-i} + a_p b_q + \sum_{i=p+1}^{p+q} a_i b_{k-i} = a_p b_q.$$

□

Notation. Pour tout $\lambda \in \mathbb{K}$, on identifiera λ avec le polynôme $(\lambda, 0, \cdots)$. On notera X le polynôme $(0, 1, 0, \cdots)$, appelée indéterminée. Avec le produit définit plus haut, on a :

$$X^2 = (0, 0, 1, 0, \cdots) \text{ et plus généralement } X^n = (0, \cdots, 0, \underbrace{1}_{n+1^{ieme} \text{ position}}, 0, \cdots).$$

Par convention on pose $X^0 = (1, 0, \cdots)$. Avec ces notations, le polynôme $P = (p_0, p_1, \cdots, p_n, 0, 0, \cdots)$ s'écrit maintenant :

$$\begin{aligned} P \text{ ou } P(X) &= p_0(1, 0, \cdots) + p_1(0, 1, 0, \cdots) + \cdots + p_n(0, 0, \cdots, 1, 0, \cdots) \\ &= p_0 + p_1 X + \cdots + p_n X^n. \end{aligned}$$

On notera alors $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ en l'indéterminée X.

Exemple. Considérons les polynômes $P = (1, -2, 0, -1, 0, \cdots)$ et $Q = (1, 0, 1, 0, \cdots)$. Avec les notations introduites précédemment, on a :

$$P(X) = 1 - 2X - X^3 \quad \text{et} \quad Q(X) = 1 + X^2.$$

Alors $(P + Q)(X) = 2 - 2X + X^2 - X^3$ et $(P \times Q)(X) = 1 - 2X + X^2 - 3X^3 - X^5$.

Propriété 2

L'addition dans $\mathbb{K}[X]$ est :

- associative : $\forall P, Q, R \in \mathbb{K}[X]$, $(P + Q) + R = P + (Q + R)$;
- commutative : $\forall P, Q, R \in \mathbb{K}[X]$, $P + Q = Q + P$;
- admet pour élément neutre le polynôme nul : $0 + P = P + 0 = P$.

Preuve. Ces propriétés découlent directement de celles de l'addition des suites réelles ou complexes. □

Propriété 3

Le produit dans $\mathbb{K}[X]$ est :

- associatif : $\forall P, Q, R \in \mathbb{K}[X]$, $(P \times Q) \times R = P \times (Q \times R)$;
- commutatif : $\forall P, Q \in \mathbb{K}[X]$, $P \times Q = Q \times P$;
- distributif par rapport à l'addition : $\forall P, Q, R \in \mathbb{K}[X]$, $P \times (Q + R) = P \times Q + P \times R$;
- admet pour élément neutre 1 : $\forall P \in \mathbb{K}[X]$, $P \times 1 = 1 \times P = P$;
- satisfait : $\forall \lambda \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$, $\lambda \cdot (P \times Q) = (\lambda \cdot P) \times Q = P \times (\lambda \cdot Q)$.

On dit que l'ensemble des polynômes est une **algèbre**, appelée **l'algèbre des polynômes à coefficients dans** $\mathbb{K}$.

Remarque. Contrairement à l'addition, le produit dans $\mathbb{K}[X]$ n'est pas le même que le produit défini pour les suites réelles ou complexes, et on ne peut pas en déduire directement toutes ces propriétés.

Preuve. Dans toute la preuve, on note $P = \sum_{n \geq 0} a_n X^n$, $Q = \sum_{n \geq 0} b_n X^n$ et $R = \sum_{n \geq 0} c_n X^n \in \mathbb{K}[X]$.

- On a

$$(P\times Q)\times R=\left(\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n\right)\times R=\sum_{n\geq 0}\sum_{l=0}^{n}\left(\sum_{k=0}^{l}a_kb_{l-k}\right)c_{n-l}X^n$$

et

$$\begin{aligned}P\times(Q\times R)&=P\times\left(\sum_{n\geq 0}\left(\sum_{l=0}^{n}b_lc_{n-l}\right)X^n\right)=\sum_{n\geq 0}\sum_{k=0}^{n}a_k\left(\sum_{l=0}^{n-k}b_lc_{n-k-l}\right)X^n\\&=\sum_{n\geq 0}\left(\sum_{k=0}^{n}\sum_{l=k}^{n}a_kb_{l-k}c_{n-l}\right)X^n \text{ en posant le changement d'indice } l=l+k\\&=\sum_{n\geq 0}\left(\sum_{l=0}^{n}\sum_{k=0}^{l}a_kb_{l-k}c_{n-l}\right)X^n \text{ en intervertissant les deux signes sommes}\\&=\sum_{n\geq 0}\sum_{k=0}^{n}a_k\left(\sum_{l=0}^{n-k}b_{l-k}c_{n-l}\right)X^n\end{aligned}$$

donc $(P\times Q)\times R=P\times(Q\times R)$.

- On a, en posant le changement d'indice $k=n-k$:

$$P\times Q=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_{n-k}b_k\right)X^n=Q\times P.$$

- On a

$$P\times 1=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_k\delta_{0,n-k}\right)X^n=\sum_{n\geq 0}a_nX^n=P$$

car tous les termes de la somme sont nuls, sauf quand $n-k=0$ i.e. $k=n$. Par commutativité de $\times$, $1\times P=P$.

- On a

$$\begin{aligned}P\times(Q+R)&=P\times\left(\sum_{n\geq 0}(b_n+c_n)X^n\right)=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_k(b_{n-k}+c_{n-k})\right)X^n\\&=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n+\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_kc_{n-k}\right)X^n\\&=(P\times Q)+(P\times R)\end{aligned}$$

et comme $\times$ est commutative, on a $(P+Q)\times R=(P\times R)+(Q\times R)$.

- On a

$$\begin{aligned}\lambda\cdot(P\times Q)&=\lambda\cdot\left(\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n\right)=\sum_{n\geq 0}\left(\sum_{k=0}^{n}(\lambda a_k)b_{n-k}\right)X^n=\sum_{n\geq 0}\left(\sum_{k=0}^{n}a_k(\lambda b_{n-k})\right)X^n\\&=(\lambda\cdot P)\times Q=P\times(\lambda\cdot Q).\end{aligned}$$

□

Définition.

Pour $P\in\mathbb{K}[X]$, on définit par récurrence P^n en posant $P^0=1$, et $\forall n\in\mathbb{N}$, $P^{n+1}=P^n\times P$.

Définition.

Si $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{i=0}^{q} b_i X^i$ sont deux polynômes, on définit le polynôme composé $P \circ Q$ par :

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

Exemple. ♦ $(X^2+1) \circ (X-2) = (X-2)^2 + 1 = X^2 - 4X + 5$.
♦ $(X-2) \circ (X^2+1) = X^2 + 1 - 2 = X^2 - 1$.
♦ Pour tout polynôme $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, $P \circ (X+a)$ sera noté $P(X+a)$.

Propriété 4 (Formule du binôme de Newton)

Pour $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$, on a

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

Propriété 5

Pour $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}^*$, on a

$$P^n - Q^n = (P-Q) \sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

1.2 Degré d'un polynôme

Définition.

Soit P un polynôme non nul.
On appelle **degré du polynôme** P le plus grand entier n tel que $p_n \neq 0$. On note cet entier $\deg(P)$. On dit alors que p_n est le **coefficient dominant** de P. On dit que P est **unitaire** si son coefficient dominant p_n est égal à 1.

Remarque. Par convention, le degré du polynôme nul est $-\infty$.

Exemple. $X^{1515} - 1$ est unitaire de degré 1515.

Définition.

On dit que P est un polynôme constant si $deg(P) \leq 0$. On identifiera l'ensemble des polynômes constants à $\mathbb{K}$.

Propriété 6 (degré de la somme, du produit, de la composée)

Soient $P(X) = a_0 + a_1X + \cdots + a_pX^p$ et $Q(X) = b_0 + b_1X + \cdots + b_qX^q$ deux polynômes à coefficients dans un corps $\mathbb{K}$. Alors :

(1) $deg(P+Q) \leq \max(deg(P), deg(Q))$;

(2) Si $\deg(P) \neq \deg(Q)$, alors $deg(P+Q) = max(deg(P), deg(Q))$;

(3) Si $\deg(P) = \deg(Q) = n$, alors :

- si $a_n + b_n = 0$, $deg(P+Q) < max(deg(P), deg(Q))$;
- si $a_n + b_n \neq 0$, $deg(P+Q) = max(deg(P), deg(Q))$;

(4) $\forall \lambda \in \mathbb{K}^*$, $deg(\lambda.P) = deg(P)$;

(5) $deg(PQ) = deg(P) + deg(Q)$;

(6) Si $\deg(Q) \geq 1$, $deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Preuve. Soient $P(X) = a_0 + a_1X + \cdots + a_pX^p$ et $Q(X) = b_0 + b_1X + \cdots + b_qX^q$ avec $a_p, b_q \neq 0$ (on vérifiera sans difficulté que toutes ses propriétés s'étendent si P ou Q sont les polynômes nuls).

(1) Pour tout $k > \max(p,q)$, on a $a_k = b_k = 0$ et donc $a_k + b_k = 0$. Ainsi $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$.

(2) Supposons par exemple que $p > q$ (le cas $q < p$ se traite de la même façon). Alors $a_p + b_p = a_p \neq 0$. De plus on a montré que pour tout $k > p$, $a_k + b_k = 0$. Ainsi on a bien $\deg(P+Q) = p = \max(\deg(P), \deg(Q))$.

(3) Si $\deg(P) = \deg(Q) = n$, alors :

- si $a_n + b_n = 0$, alors $a_k + b_k = 0$ pour tout $k \geq n$, et donc $\deg(P+Q) < n = \max(\deg(P), \deg(Q))$;
- si $a_n + b_n \neq 0$, on a montré de plus que pour tout $k > n$, $a_k + b_k = 0$. Donc on a $\deg(P+Q) = n = \max(\deg(P), \deg(Q))$.

(4) Pour tout $\lambda \in \mathbb{K}^*$, on a $\lambda a_p \neq 0$ et pour tout $k > p$, $\lambda a_k = 0$. Donc on a bien $deg(\lambda.P) = p = deg(P)$.

(5) Notons $c_k = \sum_{i+j=k} a_i b_j$ le coefficient d'indice k de PQ. On a montré que $c_k = 0$ si $k > p+q$ et que $c_{p+q} = a_p b_q \neq 0$. Ainsi on a bien $deg(PQ) = p + q = deg(P) + deg(Q)$.

(6) Supposons $\deg(Q) \geq 1$. On a par définition

$$P \circ Q(X) = a_0 + a_1 Q(X) + \cdots + a_p Q(X)^p.$$

Pour tout $0 \leq k \leq p$, on a montré que $\deg(Q^k) = k \deg(Q)$. En utilisant alors le point (2), on obtient :

$$deg(P \circ Q) = p \times \deg(Q) = \deg(P) \times \deg(Q).$$

□

Exemple. Pour tout $n \in \mathbb{N}^*$, $P(X) = (X^2+1)^n - (X^2-1)^n$ est de degré $2n-2$ et de coefficient dominant $2n$.

On a $\deg(P) \leq 2n$ grâce à la propriété précédente. En utilisant la formule du binôme, on observe que :

- le coefficient en X^{2n} est nul ;

- le coefficient en X^{2n-1} est nul (il n'apparait que des puissances paires de X dans P) ;
- le coefficient en X^{2n-2} est (toujours par la formule du binôme) :
$$nX^{2n-2} - (-nX^{2n-2}) = 2nX^{2n-2}.$$

Ainsi P est bien de degré $2n-2$ et de coefficient dominant $2n$.

Exercice. Déterminer tous les polynômes P satisfaisant $P(X^2) = (X^2+1)P(X)$.

En prenant le degré dans cette identité, on obtient $2\deg(P) = 2 + \deg(P)$, soit $\deg(P) = -\infty$ ou $\deg(P) = 2$. Pour $P(X) = aX^2 + bX + c$, on obtient :
$$aX^4 + bX^2 + c = aX^4 + bX^3 + (a+c)X^2 + bX + c.$$
En identifiant les coefficients, on en déduit $b = 0$ et $a + c = b$. Ainsi l'ensemble des polynômes satisfaisant cette identité est :
$$\{aX^2 - a | a \in \mathbb{R}\}.$$

Propriété 7 (intégrité)

$\mathbb{K}[X]$ est **intègre**, c'est à dire :
$$\forall\, P, Q \in \mathbb{K}[X],\ PQ = 0 \Leftrightarrow P = 0 \text{ ou } Q = 0$$

Preuve. Soit $P, Q \in \mathbb{K}[X]$ tel que $PQ = 0$. Alors $\deg(PQ) = -\infty$. Par la proposition précédente, on en déduit que $\deg(P) + \deg(Q) = -\infty$, et donc $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$. Ainsi $P = 0$ ou $Q = 0$. □

Propriété 8 (éléments inversibles)

Soit $P \in \mathbb{K}[X]$, on a :
$$\exists Q \in \mathbb{K}[X], P \times Q = 1 \quad \Leftrightarrow \quad P \in \mathbb{K}^*.$$

Preuve. Soit $P \in \mathbb{K}[X]$. Si $P = p \in \mathbb{K}^*$, alors le polynôme $Q = \frac{1}{p}$ convient.
Réciproquement, supposons qu'il existe $Q \in \mathbb{K}[X]$ tel que $P \times Q = 1$. En prenant le degré dans cette équation, on obtient :
$$\deg(P) + \deg(Q) = 0 \quad \Rightarrow \quad \deg(P) = \deg(Q) = 0.$$
Ainsi on a $P \in \mathbb{K}^*$. □

Notation. Pour tout $n \geq 0$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieurs ou égaux à n.

Propriété 9

L'ensemble $\mathbb{K}_n[X]$ est stable par combinaison linéaire :
$$\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}_n[X], \quad \lambda P + \mu Q \in \mathbb{K}_n[X].$$

Remarque. $\mathbb{K}_n[X]$ n'est pas stable par produit en général. Il est stable par produit si et seulement si $n = 0$.

Preuve. Soient $\lambda, \mu \in K$ et $P, Q \in \mathbb{K}_n[X]$. Alors on a :
$$\deg(\lambda P + \mu Q) \leq \max(\deg(\lambda P), \deg(\mu Q)) \leq \max(\deg(P), \deg(Q)) \leq n.$$
Ainsi on a bien $\lambda P + \mu Q \in \mathbb{K}_n[X]$. □

1.3 Fonctions polynomiales

Remarque. Soit $P(X) \in \mathbb{K}[X]$ un polynôme. L'indéterminée X désigne ici la suite $(0, 1, 0, \cdots)$. On souhaite substituer à X des éléments de $\mathbb{K}$, et ainsi évaluer polynôme P en un scalaire $a \in \mathbb{K}$. Ceci nous amène à la définition suivante.

Définition.

On appelle fonction polynomiale associée à $P = a_0 + a_1X + \cdots + a_pX^p \in \mathbb{K}[X]$, la fonction :

$$\bar{P} : \left\{ \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \tilde{P}(x) = a_0 + a_1x + \cdots + a_px^p. \end{array} \right.$$

On note $\mathcal{P}_{\mathbb{K}} = \{x \mapsto \tilde{P}(x) | P \in \mathbb{K}[X]\}$ l'ensemble des fonctions polynomiales à coefficients dans $\mathbb{K}$.

Propriété 10

Considérons l'application $\phi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{P}_{\mathbb{K}} \\ P(X) & \mapsto & \tilde{P}. \end{array} \right.$ Alors :

(1) $\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X]$, $\phi(\lambda P + \mu Q) = \lambda\phi(P) + \mu\phi(Q)$;

(2) $\forall P, Q \in \mathbb{K}[X]$, $\phi(P \times Q) = \phi(P) \times \phi(Q)$;

(3) L'application ϕ est surjective.

Preuve.

(1) Soient $P = a_0 + a_1X + \cdots + a_nX^n$, $Q = b_0 + b_1X + \cdots + b_nX^n$ deux polynômes avec $n = \max(\deg(P), \deg(Q))$. Pour tout $x \in \mathbb{K}$, on a :

$$\begin{aligned} (\lambda P \tilde{+} \mu Q)(x) &= (\lambda a_0 + \mu b_0) + (\lambda a_1 + \mu b_1)x + \cdots + (\lambda a_n + \mu b_n)x^n \\ &= \lambda(a_0 + a_1x + \cdots + a_nx^n) + \mu(b_0 + b_1x + \cdots + b_nx^n) \\ &= \lambda\tilde{P}(x) + \mu\tilde{Q}(x) \end{aligned}$$

Donc on a bien $\phi(\lambda P + \mu Q) = \lambda\phi(P) + \mu\phi(Q)$.

(2) On montre ce point de même que précédemment.

(3) La surjectivité est immédiate, puisque pour toute fonction polynomiale $f(x) = p_0 + p_1x + \cdots + p_nx^n \in \mathcal{P}_{\mathbb{K}}$, on a $\phi(P) = f$ avec $P(X) = p_0 + p_1X + \cdots + p_nX^n \in \mathbb{K}[X]$.

□

Remarque. On verra dans la suite que l'application ϕ est également injective, ce qui nous permettra d'identifier les polynômes et les fonctions polynomiales.

Définition.

Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. On appelle évaluation de P en a le nombre $\bar{P}(a)$. Par abus de notation, on le notera $P(a)$, et on parlera de la valeur de P en a.

Algorithme de Hörner. Pour évaluer en x une fonction polynomiale, il suffit de faire n additions et n multiplications en suivant le parenthèsage ci-dessous (en commençant par la parenthèse la plus intérieure) :

$$P(x) = ((\cdots((p_nx + p_{n-1})x + p_{n-2})x + \cdots)x + p_1)x + p_0.$$

C'est la méthode la plus efficace pour évaluer une fonction polynomiale en un point x.

Exemple. Évaluer $P = 2X^4 - X^3 + 3X^2 - 1$ en -2 grâce à l'algorithme d'Hörner.

Exercice. Écrire un algorithme d'évaluation de la fonction polynomiale associée à un polynôme.

Un polynôme $P = p_0 + p_1X + \cdots + p_nX^n$ sera représenté en machine par un tableau p à $n+1$ entrée numérotées de 0 à n et contenant l'ensemble de ses coefficients : $p[k] = p_k$ pour tout $0 \leq k \leq n$. On obtient de la factorisation ci-dessus l'algorithme suivant :

Entrer x ;
$y := p[n]$;
Pour $k := 1$ à n, faire :
    $y := yx + p[n-k]$;
Sortir y.

2 Divisibilité et division euclidienne dans $\mathbb{K}[X]$

2.1 Divisibilité dans $\mathbb{K}[X]$

Définition.

Soient $A, B \in \mathbb{K}[X]$. On dit que A **divise** B ou que B est **un multiple de** A s'il existe $Q \in \mathbb{K}[X]$ tel que: $B = AQ$. On notera $A\mathbb{K}[X]$ l'ensemble des multiples de A.

Exemple. Dans $\mathbb{K}[X]$, on a $X - 1 \mid X^n - 1$ et $X + 1 \mid X^{2n+1} + 1$.
Dans $\mathbb{C}[X]$ (mais pas dans $\mathbb{R}[X]$), $X - i$ divise $X^2 + 1$.

Remarque. On a A divise B si et seulement si $B\mathbb{K}[X] \subset A\mathbb{K}[X]$. En effet :

- si $B\mathbb{K}[X] \subset A\mathbb{K}[X]$, alors $B \in A\mathbb{K}[X]$ et B est un multiple de A.
- si A divise B, alors il existe $Q \in \mathbb{K}[X]$ tel que $B = AQ$. Et alors pour $R \in \mathbb{K}[X]$, on a $BR = AQR \in A\mathbb{K}[X]$. Donc $B\mathbb{K}[X] \subset A\mathbb{K}[X]$.

Propriété 11

Soit A, B et D des polynômes. On a alors :

$$\Big(D \mid A \text{ et } D \mid B\Big) \implies D \mid PA + QB \quad \forall (P, Q) \in \mathbb{K}[X]^2.$$

Preuve. En effet, si $D|A$ et $D|B$, il existe $E, F \in \mathbb{K}[X]$ tels que :

$$A = DE \text{ et } B = DF.$$

Alors pour tout $P, Q \in \mathbb{K}[X]$,

$$PA + QB = PDE + QDF = D(PE + QF) \ \Rightarrow \ D|PA + QB.$$

□

Propriété 12 (caractérisation des polynômes associés)

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

$$A|B \text{ et } B|A \Leftrightarrow A\mathbb{K}[X] = B\mathbb{K}[X] \Leftrightarrow \exists \lambda \in \mathbb{K}^*,\ A = \lambda B$$

Si l'une de ces assertions est vérifiée, on dit alors que A et B sont des **polynômes associés**.

Preuve. On a déjà vu que les deux premiers points sont équivalents. Montrons qu'ils sont équivalents au troisième point. On suppose $A, B \neq 0$ (sinon c'est immédiat).

$\Leftarrow$ Immédiat.

$\Rightarrow$ Si $A|B$ et $B|A$, alors il existe $C, D \in \mathbb{K}[X]$ tels que :

$$B = AC \text{ et } A = BD.$$

Ainsi $B = B \times (CD)$. Comme $\mathbb{K}[X]$ est intègre et $B \neq 0$, on obtient $CD = 1$, et donc $C, D \in \mathbb{K}^*$. Ainsi il existe bien $\lambda \in \mathbb{K}^*$ tel que $B = \lambda A$.

□

2.2 Division euclidienne dans $\mathbb{K}[X]$

Théorème 13 (de la division euclidienne)

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

$$\begin{cases} A = BQ + R \\ deg(R) < deg(B) \end{cases}$$

Les polynômes Q et R seront alors appelés le **quotient** et le **reste** dans la **division euclidienne de A par B**.

Preuve.
Existence : Tout d'abord si $A = 0$, le couple $(Q, R) = (0, 0)$ convient.
Montrons par récurrence (forte) sur $n \in \mathbb{N}$ la propriété $\mathcal{P}(n)$: pour tout $A \in \mathbb{K}[X]$ tel que $\deg(A) = n$, il existe (Q, R) satisfaisant le propriété de division euclidienne.

- Initialisation : Supposons $n = 0$. Alors si $\deg(B) \geq 1$, le couple $(Q, R) = (0, A)$ convient. Sinon $B \in \mathbb{K}^*$ et on peut prendre $(Q, R) = (A/B, 0)$. Ainsi $\mathcal{P}(0)$ est vraie.
- Hérédité : Soit $n \geq 1$ et supposons la propriété $\mathcal{P}(k)$ vraie pour tout $k \leq n - 1$.
  Soit $A \in \mathbb{K}[X]$ tel que $\deg(A) = n$. Si $n < \deg(B)$, le couple $(Q, R) = (0, A)$ convient.
  Sinon notons a_n le coefficient dominant de A et $p = \deg(B)$, $b_p \neq 0$ le coefficient dominant de B. Par hypothèse $p \geq n$. Alors le polynôme $A - \dfrac{a_n}{b_p} X^{n-p} B$ est de degré $\leq n - 1$. Si ce polynôme est nul, alors le couple $(Q, R) = (\dfrac{a_n}{b_p} X^{n-p}, 0)$ convient. Sinon par hypothèse de récurrence, il existe (Q_0, R_0) tels que :

  $$A - \frac{a_n}{b_p} X^{n-p} B = Q_0 B + R_0 \quad \text{avec} \quad \deg(R_0) < \deg(B).$$

  Ainsi, $A = (Q_0 + \dfrac{a_n}{b_p} X^{n-p})B + R_0$ et le couple $(Q, R) = (Q_0 + \dfrac{a_n}{b_p} X^{n-p}, R_0)$ convient. La propriété est donc vraie au rang $n + 1$.

On conclut par principe de récurrence.

Unicité : Soient (Q_1, R_1) et (Q_2, R_2) satisfaisant cette propriété. On a :

$$BQ_1 + R_1 = BQ_2 + R_2 \quad \Rightarrow \quad B(Q_1 - Q_2) = R_2 - R_1.$$

En prenant les degrés dans cette expression, on a : $\deg(B(Q_1 - Q_2)) \leq \max(\deg(R_1), \deg(R_2)) < \deg(B)$. Ainsi $Q_1 = Q_2$ nécessairement, et donc $R_1 = R_2$ en reportant dans l'égalité de départ. □

Exemple. Déterminons le quotient et le reste dans la division euclidienne de :

1. $X^3 + 2X^2 + X + 1$ par $X^2 + 1$.
2. $X^5 + 3X^4 + 1$ par $X^3 + X + 1$

Exercice. Soit $n \in \mathbb{N}$. Déterminer le reste de la division euclidienne de X^n par $X^2 - 2\cos(\theta)X + 1$.

Par le théorème de division euclidienne, il existe $(Q, R) \in \mathbb{R}[X]^2$ tels que :

$$X^n = (X^2 - 2\cos(\theta)X + 1)Q(X) + R(X) \quad \text{avec } \deg(R) < \deg(X^2 - 2\cos(\theta)X + 1) = 2.$$

Ainsi, il existe $\lambda, \mu \in \mathbb{R}$ tels que $R(X) = \lambda X + \beta$. On cherche donc λ et μ. Pour cela, on va évaluer X^n en certains points bien choisis :

- en $e^{i\theta}$: $e^{in\theta} = \lambda e^{i\theta} + \mu$.
- en $e^{-i\theta}$: $e^{-in\theta} = \lambda e^{-i\theta} + \mu$.

En résolvant, on obtient $R = \dfrac{\sin(n\theta)}{\sin(\theta)}X - \dfrac{\sin((n-1)\theta)}{\sin(\theta)}$.

Propriété 14

Soient $A, B \in \mathbb{K}[X]$. On a :

$$A \text{ divise } B \quad \Leftrightarrow \quad \text{le reste de la division euclidienne de } A \text{ par } B \text{ est nul.}$$

Preuve.

$\Rightarrow$ Si $A|B$, alors il existe Q tel que $A = BQ$. Alors le couple $(Q, 0)$ satisfait la définition de la division euclidienne. Par unicité du reste de la division euclidienne pour les polynômes, on en déduit que ce reste est nul.

$\Leftarrow$ Si le reste de la division euclidienne de A par B est nul, on obtient qu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ + 0 = BQ$. Donc on a bien $A|B$.

□

3 Dérivation dans $\mathbb{K}[X]$

Définition.

On appelle **dérivée (formelle)** d'un polynôme $P = \sum_{k=0}^{n} p_k X^k$ le polynôme noté P', tel que :

$$P' = \sum_{k=1}^{n} k p_k X^{k-1} = \sum_{i=0}^{n-1} (i+1) p_{i+1} X^i.$$

Remarque. Cette définition s'inspire de la règle connue de dérivation des fonctions polynomiales à coefficients réels. Ainsi pour $\mathbb{K} = \mathbb{R}$, on a $\phi(P') = \phi(P)'$ où la dérivée de droite est celle des fonctions numériques de la variable réelle. On étend ces règles pour définir formellement, quel que soit le corps $\mathbb{K}$ (et donc pour $\mathbb{K} = \mathbb{C}$ également), la notion de polynôme dérivé.

Propriété 15

Soient $P, Q \in \mathbb{K}[X]$ des polynômes.

(1) On a $P' = 0 \Leftrightarrow P$ est constant.

(2) Si $\deg(P) \geq 1$, on a $\deg(P') = \deg(P) - 1$.

(3) La dérivation est linéaire : pour tout $\lambda, \mu \in \mathbb{K}$, $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.

(4) $(P \times Q)' = P' \times Q + P \times Q'$.

(5) $(P \circ Q)' = Q' \times (P' \circ Q)$

Preuve.

(1) Supposons $P = \sum_{k=0}^{n} a_k X^k$ avec $\deg(P) = n > 0$. On a donc $a_n \neq 0$.

Comme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ avec $n a_n \neq 0$, on en déduit que $\deg(A) = n - 1$.

(2) Si P est un polynôme constant, alors $P' = 0$. Et si $\deg(P) > 0$, alors d'après (1), on a $\deg(P') \geq 0$ donc $P' \neq 0$.

(3) Prenons $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$. On a $\lambda P + \mu Q = \sum_{k=0}^{n} (\lambda a_k + \mu b_k) X^k$, donc

$$(\lambda P + \mu Q)' = \sum_{k=0}^{n} (k+1)(\lambda a_{k+1} + \mu b_{k+1}) X^k = \lambda \sum_{k=0}^{n} (k+1) a_{k+1} X^k + \mu \sum_{k=0}^{n} (k+1) b_{k+1} X^k = \lambda P' + \mu Q'.$$

(4) Pour $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{j=0}^{q} b_j X^j$, on a :

$$(PQ)(X) = \left(\sum_{i=0}^{p} a_i X^i \right) \left(\sum_{j=0}^{q} b_j X^j \right) = \sum_{i=0}^{p} \sum_{j=0}^{q} a_i b_j X^{i+j}.$$

On obtient par définition de la dérivation :

$$(PQ)'(X) = \sum_{i=0}^{p} \sum_{j=0}^{q} (i+j) a_i b_j X^{i+j-1} = \sum_{i=1}^{p} \sum_{j=0}^{q} i a_i b_j X^{i+j-1} + \sum_{i=0}^{p} \sum_{j=1}^{q} j a_i b_j X^{i+j-1}.$$

On en déduit :

$$(PQ)'(X) = \left(\sum_{i=1}^{p} i a_i X^{i-1} \right) \left(\sum_{j=0}^{q} b_j X^j \right) + \left(\sum_{i=0}^{p} a_i X^i \right) \left(\sum_{j=1}^{q} j b_j X^{j-1} \right) = P'Q + PQ'.$$

(5) On montre par récurrence sur $n \in \mathbb{N}^*$ la propriété $\mathcal{P}(n)$: $(P^n)' = nP'P^{n-1}$.

- Initialisation : $\mathcal{P}(1)$ est vraie de façon immédiate.
- Hérédité : Soit $n \in \mathbb{N}^*$ tel que $\mathcal{P}(n)$ est vraie. On a $(P^{n+1})' = (P^n \times P)' = (P^n)'P + P^n P'$ (d'après le point précédent) $= nP'P^{n-1}P + P^n P' = (n+1)P'P^n$. Ainsi on a $\mathcal{P}(n+1)$ est vraie.

On conclut par principe de récurrence que $\forall n \in \mathbb{N}^*$, $\mathcal{P}(n)$ est vraie.

Prenons alors $P = \sum_{k=0}^{p} a_k X^k$, et dérivons $P \circ Q$. D'après les points (1) et (4), on en déduit que :

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

□

Définition.

Soit $P \in \mathbb{K}[X]$. On définit par itération les polynômes dérivés successifs de P par $P^{(0)} = P$ et $P^{(n)} = (P^{(n-1)})'$ pour tout $n \geq 1$.

Exemple. Soit $a \in \mathbb{K}$ et soit $n \in \mathbb{N}$. Pour tout $p \in [|0, n|]$, on a :

$$((X-a)^n)^{(p)} = \begin{cases} n(n-1)\cdots(n-p+1)X^{n-p} = \dfrac{n!}{(n-p)!}X^{n-p} & \text{si } p \in [|0,n|] \\ 0 & \text{si } p > n \end{cases}$$

Propriété 16

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

(1) Si $\deg(P) = n$, alors $P^{(k)} = 0$ pour tout $k > n$.

(2) Pour tout $\lambda, \mu \in \mathbb{K}$ et $n \in \mathbb{N}$, $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.

Propriété 17 (Formule de Leibniz)

Soient $P, Q \in \mathbb{K}[X]$ des polynômes, $n \in \mathbb{N}$. On a :

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

Preuve. On raisonne comme dans la preuve de la formule de Leibniz pour les fonctions n fois dérivables, en utilisant le point (4) de la proposition précédente. □

Propriété 18 (Formule de Taylor)

Pour tout polynôme $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$, pour tout $a \in \mathbb{K}$, on a :

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

Preuve. La formule est satisfaite pour $P = 0$. Montrons par récurrence sur $n \in \mathbb{N}$ la propriété $\mathcal{P}(n)$: pour tout polynôme P tel que $\deg(P) = n$, $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$.

- Initialisation : Si $\deg(P) = 0$, P est constant, donc $P = P(a)$. Ainsi on a $\mathcal{P}(0)$.
- Hérédité : Soit $n \in \mathbb{N}$ et supposons $\mathcal{P}(n)$ vraie.
  Soit $P \in \mathbb{K}[X]$ tel que $\deg(P) = n+1$. Alors $\deg(P') = n$ et par hypothèse de récurrence,

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

  Soit $Q = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(X-a)^k$. On a

$$Q' = \sum_{k=1}^{n+1} \frac{P^{(k)}(a)}{k!}k(X-a)^{k-1} = \sum_{k=1}^{n+1} \frac{P^{(k)}(a)}{(k-1)!}(X-a)^{k-1} = \sum_{k=0}^{n} \frac{P^{(k+1)}(a)}{k!}(X-a)^k = P'$$

  donc $(Q-P)' = 0$. Ainsi $Q - P$ est constant. En prenant la valeur en a, on obtient $Q - P = Q(a) - P(a) = P(a) - P(a) = 0$, donc $P = Q$ et on a prouvé $\mathcal{P}(n+1)$.

En conclusion, $\forall n \in \mathbb{N}$, $\mathcal{P}(n)$. □

Remarque. Pour $P = \sum_{k=0}^{n} a_k X^k$, et prenons $a = 0$ dans la formule de Taylor. On obtient par identification des coefficients :

$$\forall 0 \leq k \leq n, \quad a_k = \frac{P^{(k)}(0)}{k!}.$$

4 Racines d'un polynôme

4.1 Racines

Définition.

On dit que $a \in \mathbb{K}$ est une **racine** (ou un zéro) d'un polynôme $P \in \mathbb{K}[X]$ si $P(a) = 0$.

Exemple.

- Tout polynôme de degré 1 a une racine : la racine de $aX + b$ est $-\frac{b}{a}$.
- Pour un polynôme de degré 2, l'existence de racines dépend du corps K : par exemple $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$, il a les racines $\pm i$ dans $\mathbb{C}$.
- Si $z \in \mathbb{C}$ est racine de $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{R}[X]$, alors $\bar{z}$ est aussi racine de P, puisqu'en prenant le conjugué, on a :

$$\sum_{k=0}^{p} a_k z^k = 0 \quad \Rightarrow \quad \sum_{k=0}^{p} a_k \bar{z}^k = 0.$$

  Cette propriété est **fausse** si $P \in \mathbb{C}[X]$.

Propriété 19

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

$$a \text{ est racine de } P \quad \Leftrightarrow \quad (X-a) | P.$$

Preuve.

⇐ Supposons que $(X-a)|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q(X)$. Alors on obtient :

$$P(a) = (a-a)Q(a) = 0.$$

⇒ Supposons que a soit racine de P, et écrivons la division euclidienne de P par $X-a$: il existe $(Q,R) \in \mathbb{K}[X]$ tels que :

$$P(X) = (X-a)Q(X) + R(X) \quad \text{et} \quad \deg(R) < \deg(X-a) = 1.$$

Ainsi $\deg(R) \leq 0$, et $R(X) = r \in \mathbb{K}$. On évalue alors l'égalité précédente en a :

$$P(a) = (a-a)Q(a) + r = r \quad \text{soit} \quad r = 0$$

car $P(a) = 0$. Ainsi $P(X) = (X-a)Q(X)$ et $(X-a)$ divise P.

□

Exemple. Considérons le polynôme $P = X^3 - X + 6$. On voit que -2 est racine évidente de P. Par la proposition précédente, P se factorise par $(X+2)$. Pour obtenir sa factorisation, on peut :

- soit écrire $P = (X+2)(aX^2+bX+c)$, développer et procéder par identification des coefficients ;
- soit faire la division euclidienne de P par $(X+2)$: le quotient correspond à l'autre facteur de la factorisation.

Propriété 20

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $a_1, \cdots a_n \in \mathbb{K}$ des scalaires deux à deux distincts.

$$a_1, a_2, \cdots, a_n \text{ sont racines de } P \quad \Leftrightarrow \quad (X-a_1)\cdots(X-a_n)|P.$$

Preuve.

⇐ Si $(X-a_1)\cdots(X-a_n)|P$, alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a_1)\cdots(X-a_n)Q(X)$. En évaluant en a_i pour tout $1 \leq i \leq n$, on obtient $P(a_i) = 0$.

⇒ Démontrons par récurrence sur n la propriété $\mathcal{P}(n)$: Si $P \in \mathbb{K}[X]$ admet n racines deux à deux distinctes $a_1, \cdots, a_n$, alors $\prod_{i=1}^{n}(X-a_i)$ divise P.

- Initialisation : On a montré que $\mathcal{P}(1)$ est vraie à la proposition précédente.
- Hérédité : Soit $n \in \mathbb{N}$, et supposons $\mathcal{P}(n)$ vraie.
  Soit $P \in \mathbb{K}[X]$ un polynôme admettant $n+1$ racines deux à deux distinctes $a_1, \cdots, a_{n+1}$. D'après l'hypothèse de récurrence, il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = \prod_{i=1}^{n}(X-a_i)Q.$$

Comme a_{n+1} est racine de P, on a : $Q(a_{n+1})\prod_{i=1}^{n}(a_{n+1}-a_i) = 0$. Or, $\prod_{i=1}^{n}(a_{n+1}-a_i)$ est un élément de $\mathbb{K}$ non nul. Donc $Q(a_{n+1}) = 0$ et il existe un polynôme $Q_1 \in \mathbb{K}[X]$ tel que $Q_1 = (X-a_{n+1})Q$. On obtient ainsi :

$$P = \prod_{i=1}^{n+1}(X-a_i)Q_1.$$

et $\mathcal{P}(n+1)$ est vraie.

On conclut par principe de récurrence.

□

On obtient la conséquence importante suivante de cette proposition.

Théorème 21

(1) Un polynôme de degré $n \in \mathbb{N}$ a au plus n racines distinctes.

(2) Le seul polynôme qui possède une infinité de racines est le polynôme nulle.

Preuve.

(1) Soit P un polynôme et supposons que P admette p racines deux à deux distinctes $a_1, \cdots, a_p$. D'après la proposition précédente, il existe alors $Q \in \mathbb{K}[X]$ tel que :

$$P(X) = (X - a_1) \cdots (X - a_p)Q(X).$$

En prenant les degrés dans cette égalité, on en déduit que $\deg(P) = p + \deg(Q)$ et donc $p \leq \deg(P)$.

(2) C'est une conséquence directe de la proposition précédente : si P est non nul, il n'a qu'un nombre fini de racines.

□

Remarque. Un polynôme de degré au plus n et ayant au moins $n + 1$ racines est le polynôme nul.

Comme autre conséquence, on obtient le résultat suivant qui permettra d'identifier les polynômes et le fonctions polynomiales.

Propriété 22

L'application $\phi : \left\{ \begin{array}{ccc} \mathbb{K}[X] & \to & \mathcal{P}_{\mathbb{K}} \\ P(X) & \mapsto & \tilde{P}. \end{array} \right.$ est bijective.

Preuve.

- $\phi(P) = 0$ implique $P = 0$: en effet, si $\phi(P) = 0$, alors $\tilde{P} = 0$, c'est à dire que la fonction polynomiale $x \mapsto \tilde{P}(x)$ est nulle sur $\mathbb{R}$. Ainsi P admet une infinité de racines. C'est donc le polynôme nul : $P = 0$.
- ϕ est injective : soient P_1 et P_2 des polynômes tels que $\phi(P_1) = \phi(P_2)$. Alors $\phi(P_1 - P_2) = 0$, et par le point précédent on en déduit que $P_1 - P_2 = 0_{\mathbb{K}[X]}$. Ainsi $P_1 = P_2$ et ϕ est injective.

□

Remarque. Pour un polynôme $P = \sum a_k X^k$, on a donc équivalence entre :

$$P = 0 \text{ (c'est à dire } a_k = 0 \ \forall k \in \mathbb{N}) \quad \Leftrightarrow \quad \bar{P} = 0 \text{ (c'est à dire } \bar{P}(t) = 0 \ \forall t \in \mathbb{K}).$$

4.2 Ordre de multiplicité des racines d'un polynôme

Propriété 23

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}^*$. On a l'équivalence entre :

- $(X-a)^r$ divise P,
- $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$.

Si l'une de ces conditions est satisfaite, on dit alors que a **est racine de** P **de multiplicité au moins** r.

Preuve.

$\Leftarrow$ Supposons que $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$. Alors en appliquant la formule de Taylor à P en a, on obtient (avec $n = \deg(P)$:

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

Ainsi $(X-a)^r$ divise bien P.

$\Rightarrow$ Supposons que $(X-a)^r$ divise bien P. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^r Q(X)$. Par la formule de Leibniz, on obtient que pour tout $k \leq r-1$:

$$\begin{aligned} P^{(k)}(X) &= \sum_{i=0}^{k} \binom{k}{i} \frac{d^i}{dX^i}((X-a)^r) Q^{(k-i)} \\ &= \sum_{i=0}^{k} \binom{k}{i} \frac{r!}{(r-i)!}(X-a)^{r-i} Q^{(k-i)} \\ &= (X-a) \left(\sum_{i=0}^{k} \binom{k}{i} \frac{r!}{(r-i)!}(X-a)^{r-i-1} Q^{(k-i)} \right) \end{aligned}$$

où $r-i-1 \geq r-k-1 \geq 0$. Ainsi en évaluant $P^{(k)}$ en a, on obtient $P^{(k)}(a) = 0$ pour tout $0 \leq k \leq r-1$.

□

Exemple. Considérons $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$. On a $P(1) = P'(1) = P''(1) = 0$. Donc 1 est racine de P de multiplicité au moins 3.

Propriété 24

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}^*$. On a l'équivalence entre :

(1) $\exists Q \in \mathbb{K}[X]$, $P = (X-a)^r Q$ et $Q(a) \neq 0$

(2) $(X-a)^r$ divise P et $(X-a)^{r+1}$ ne divise pas P ;

(3) $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$ et $P^{(r)}(a) \neq 0$.

Si l'une de ces conditions est satisfaite, on dit alors que a **est racine de** P **de multiplicité** r **exactement**.

Vocabulaire.

- Lorsque $m \geq 2$, on parle de racine multiple.
- Les racines d'ordre 1,2,3 de P sont respectivement appelés racines simples, doubles, triples de P.

Preuve.

- (1) $\Rightarrow$ (2) : On a déjà que $(X-a)^r$ divise P. Supposons que $(X-a)^{r+1}$ divise aussi P, alors il existe $S \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^{r+1}S(X)$. D'où l'égalité :

$$(X-a)^r Q(X) = (X-a)^{r+1}S(X) \underset{\mathbb{K}[X] \text{ est intègre}}{\Rightarrow} Q(X) = (X-a)S(X).$$

  Mais alors $Q(a) = 0$ ce qui est contradictoire.

- (2) $\Rightarrow$ (3) : Par la proposition précédente, on a déjà que $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$. De plus, si $P^{(r)}(a) = 0$, alors $(X-a)^{r+1}$ diviserait également P, ce qui n'est pas le cas. Donc $P^{(r)}(a) \neq 0$.
- (3) $\Rightarrow$ (1) : D'après la proposition précédente, on a déjà que $(X-a)^r$ divise P, et li existe donc $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^r Q(X)$.

  Montrons que $Q(a) \neq 0$. Sinon, a est racine de Q et $(X-a)$ diviserait Q. Mais alors $(X-a)^{r+1}$ divise P et on aurait avec la proposition précédente $P^r(a) = 0$. D'où une contradiction. Donc $Q(a) \neq 0$.

□

Exemple. Considérons toujours $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$. On a $P(1) = P'(1) = P''(1) = 0$ et que $P^{(3)}(1) = 6$. Donc 1 est racine de P de multiplicité 3 exactement.
On sait alors que $(X-1)^3$ divise le polynôme P, c'est à dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-1)^3 Q(X)$. Pour obtenir le polynôme Q, on peut alors :

- soit développer $P(X) = (X-1)^3 Q(X)$ et obtenir Q en identifiant les coefficients ;
- soit faire la division euclidienne de P par $(X-1)^3$. Le reste est alors nul, et le quotient est Q.

Exercice. Soit $P \in \mathbb{R}[X]$. Montrer que si $z \in \mathbb{C}\backslash\mathbb{R}$ est racine de P de multiplicité $r \geq 1$, alors $\overline{a}$ est aussi racine de P de multiplicité r.

En effet, si z est racine de P de multiplicité r, alors

$$P(z) = P'(z) = \cdots = P^{(r-1)}(z) = 0 \text{ et } P^{(r)}(z) \neq 0.$$

En passant au conjugué, on obtient (puisque les polynômes $P^{(i)}$ sont à coefficients réels) :

$$P(\bar{z}) = P'(\bar{z}) = \cdots = P^{(r-1)}(\bar{z}) = 0 \text{ et } P^{(r)}(\bar{z}) \neq 0,$$

et donc $\bar{z}$ est racine de multiplicité r de P.

Propriété 25

Soit $P \in \mathbb{K}[X]$, $a_1, \cdots, a_n \in \mathbb{K}$ n scalaires deux à deux distincts (avec $n \geq 1$) et $r_1, \cdots, r_n \in \mathbb{N}^*$. Alors :

a_i racine de P de multiplicité au moins r_i, $\forall 1 \leq i \leq n \quad \Leftrightarrow \quad (X-a_1)^{r_1} \cdots (X-a_n)^{r_n} | P$.

Preuve.

⇐ Puisque $(X-a_1)^{r_1}\cdots(X-a_n)^{r_n}$ divise P, on a en particulier que pour tout i, $(X-a_i)^{r_i}$ divise P. Par une proposition précédente, on en déduit que a_i est racine de P de multiplicité (au moins) r_i.

⇒ Montrons par récurrence sur n la propriété $\mathcal{P}(n)$: pour tout $P\in\mathbb{K}[X]$, $a_1,\cdots,a_n\in\mathbb{K}[X]$, si $a_1,\cdots,a_n$ sont racines de P, alors $(X-a_1)^{r_1}\cdots(X-a_n)^{r_n}|P$.

- Initialisation : Si $n=1$, la propriété est vraie par définition de l'ordre d'une racine.
- Hérédité : Supposons la propriété vraie à un rang $n\in\mathbb{N}^*$. Considérons $P\in\mathbb{K}[X]$ et $a_1,\cdots,a_{n+1}$ des racines deux à deux distinctes de P d'ordres de multiplicités respectivement au moins égales à $r_1,...,r_{n+1}$.
  D'après l'hypothèse de récurrence, il existe $Q\in\mathbb{K}[X]$ tel que

$$P=\prod_{i=1}^{n}(X-a_i)^{r_i}Q.$$

  De plus, $P(a_{n+1})=0$ donc $Q(a_{n+1})\prod_{i=1}^{n}(a_{n+1}-a_i)^{r_i}=0$. Ainsi, $Q(a_{n+1})=0$ car les a_i sont deux à deux distincts. Notons r l'ordre de multiplicité de a_{n+1} en tant que racine de Q. On sait alors qu'il existe $Q_1\in\mathbb{K}[X]$ tel que :

$$Q=(X-a_{n+1})^rQ_1 \quad \text{et} \quad Q_1(a_{p+1})\neq 0$$

  On a alors :

$$P=(X-a_{n+1})^r\underbrace{Q_1\prod_{i=1}^{n}(X-a_i)^{r_i}}_{=Q_2}$$

  On a alors $Q_2(a_{n+1})=Q_1(a_{n+1})\times\prod_{i=1}^{n}(a_{n+1}-a_i)^{r_i}\neq 0$. Ainsi, a_{n+1} est racine de P d'ordre de multiplicité exactement r. Par suite, $r_{n+1}\leq r$, et $\prod_{i=1}^{n+1}(X-a_i)^{r_i}$ divise $(X-a_{n+1})^r\prod_{i=1}^{n}(X-a_i)^{r_i}$ et donc aussi P. D'où la proposition au rang $n+1$.

On conclut par principe de récurrence.

□

On obtient la conséquence directe suivante de ce résultat.

Propriété 26

Un polynôme de degré n a au plus n racines comptées avec leurs ordres de multiplicité.

5 Factorisation

5.1 Polynômes scindés, polynômes irréductibles

Définition.

On dit qu'un polynôme $P\in\mathbb{K}[X]$ de degré ≥ 1 est **scindé** s'il peut être factorisé en produit de n polynômes du premier degré de $\mathbb{K}[X]$, c'est à dire s'il existe $\lambda\in\mathbb{K}$ et $a_1,\dots a_n\in\mathbb{K}$ distincts ou non tels que :

$$P=\lambda(X-a_1)\cdots(X-a_n).$$

c'est à dire aussi, en regroupant les racines distinctes avec leurs ordres de multiplicité :

$$P = \lambda(X - a_1)^{\alpha_1} \dots (X - a_k)^{\alpha_k}.$$

Remarque. Ainsi un polynôme est scindé si et seulement si la somme des ordres de multiplicité de ses racines est égale à son degré.

Remarque. La notion de polynôme scindé dépend du corps $\mathbb{K}$ considéré : ainsi $X^2+1 = (X-i)(X+i)$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$ car $i \notin \mathbb{R}$.

Exemple. Le polynôme $X^n - 1$ est scindé dans $\mathbb{C}$. En effet, on connait n racines distinctes de ce polynôme, les racines n-ièmes de l'unité $e^{\frac{2ik\pi}{n}}$. Puisque le polynôme $X^n - 1$ est de degré n et unitaire, on obtient grâce à la propriété précédente précédente :

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

Définition.

Un polynôme non constant $P \in \mathbb{K}[X]$ est dit **irréductible sur** $\mathbb{K}$ s'il satisfait :

$$\forall A, B \in \mathbb{K}[X], \quad P(X) = A(X)B(X) \quad \Rightarrow \quad \deg(A) = 0 \text{ ou } \deg(B) = 0.$$

Remarque.

- Les polynômes irréductibles dans $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans $\mathbb{N}$.
- Les polynômes de degré un sont irréductibles.

  Soit P un polynôme de degré un. Supposons que $P = AB$, alors en prenant le degré $\deg(P) = 1 = \deg(A) + \deg(B)$. Donc on a bien $\deg(A) = 0$ ou $\deg(B) = 0$.
- Un polynôme $P \in \mathbb{K}[X]$ est scindé et irréductible sur $\mathbb{K}$ si et seulement si $\deg(P) = 1$.
- $X^2 + 1$ est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$ puisqu'il peut s'écrire $X^2 + 1 = (X - i)(X + i)$.

  Montrons que $X^2 + 1$ est irréductible sur $\mathbb{R}$: supposons que $X^2 + 1$ s'écrive $X^2 + 1 = AB$ avec $A, B \in \mathbb{R}[X]$. Si $\deg(A) = 1$, alors $A = aX + b$ et $-b/a \in \mathbb{R}$ serait racine de $X^2 + 1$. Donc $\deg(A) = 0$ ou $\deg(A) = 2$ (et alors $\deg(B) = 0$).

Exercice. Montrer qu'un polynôme réel de degré 3 n'est jamais irréductible.

Soit P un tel polynôme, $\tilde{P}$ sa fonction polynomiale associée. Alors $\lim_{\pm\infty} \tilde{P} = \pm\infty$. Par le TVI, il existe $\alpha \in \mathbb{R}$ tel que $\tilde{P}(\alpha) = 0$ et donc $(X - \alpha)|P$. Donc P n'est pas irréductible.

5.2 Factorisation des polynômes dans $\mathbb{C}[X]$

Théorème 27 (Théorème de d'Alembert-Gauss)

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.
On traduit cette propriété en disant que $\mathbb{C}$ est **algébriquement clos**.

Preuve. Admis □

On a la conséquence suivante de ce résultat.

Propriété 28

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

Preuve. Montrons par récurrence la propriété $\mathcal{P}(n)$: tout polynôme de $\mathbb{C}[X]$ de degré n est scindé.

- Initialisation : $P \in \mathbb{K}^*$ est bien scindé par définition, donc $\mathcal{P}(0)$ est vraie.
- Hérédité : Soit $n \in \mathbb{N}$ et supposons $\mathcal{P}(n)$ vraie. Soit P de degré $n+1$. D'après le Théorème de d'Alembert Gauss, P admet au moins une racine $a \in \mathbb{C}$. Alors $(X-a)$ divise P et il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)Q(X)$. Or $\deg(Q) = n$ et par hypothèse de récurrence, Q est scindé :
$$Q = \lambda(X-a_1)\cdots(X-a_n).$$
Ainsi $P = \lambda(X-a)(X-a_1)\cdots(X-a_n)$ est scindé, et $\mathcal{P}(n+1)$ est vraie.
On conclut par principe de récurrence.

□

Propriété 29

(1) Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

(2) Tout polynôme P de $\mathbb{C}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{C}[X]$ sous la forme :
$$P(X) = \lambda \prod_{i=1}^{k} (X-a_i)^{\alpha_i}.$$

Preuve.

(1) On a déjà que les polynômes de degré 1 sont irréductibles. Réciproquement, soit P un polynôme irréductible. Par le Théorème de d'Alembert Gauss, il existe a tel que $P(a) = 0$. Il existe donc $Q \in \mathbb{K}[X]$ tel que $P = (X-a)Q$. Comme de plus P est irréductible, on en déduit que $Q \in \mathbb{K}^*$ et que P est de degré 1.

(2) Soit P un polynôme de degré ≥ 1 de $\mathbb{C}[X]$. D'après la proposition précédente, P est scindé sur $\mathbb{C}[X]$, d'où l'existence d'une telle factorisation. L'unicité à l'ordre des facteurs près résulte du fait que λ est le coefficient dominant de P, $a_1, \cdots, a_k$ les racines de P et $\alpha_1, \cdots, \alpha_k$ leurs multiplicités, donc des éléments déterminés par le polynôme P.

□

5.3 Factorisation des polynômes dans $\mathbb{R}[X]$

Propriété 30

(1) Les polynômes irréductibles de $\mathbb{R}[X]$ sont

- les polynômes de degré 1 ;
- les polynômes de degré 2 à discriminant strictement négatif.

(2) Tout polynôme P de $\mathbb{R}[X]$ se factorise de façon unique (à l'ordre près des facteurs) en produit de polynômes irréductibles de $\mathbb{R}[X]$ sous la forme :

$$P(X) = \lambda \left(\prod_{i=1}^{p} (X - a_i)^{\alpha_i} \right) \left(\prod_{j=1}^{q} (X^2 - (z_j + \bar{z_j})X + z_j\bar{z_j})^{s_j} \right).$$

Preuve.

(1) On a déjà vu que les polynômes de degré 1 sont irréductibles. Soit P un polynôme de degré 2 à discriminant strictement négatif et $A, B \in \mathbb{R}[X]$ tels que $P = AB$. Si $\deg(A) = 1$, P aurait une racine réelle. Donc $\deg(A) = 0$ ou $\deg(A) = 2$ (et alors $\deg(B) = 0$). Reste à montrer que ce sont les seuls, on le fera après avoir établi la décomposition.

(2) Soit P de degré ≥ 1 appartenant à $\mathbb{R}[X]$. Alors P est scindé dans $\mathbb{C}[X]$ et on peut l'écrire comme suit (les multiplicités des racines complexes conjuguées sont égales) :

$$P(X) = \lambda \left(\prod_{i=1}^{p} (X - a_i)^{\alpha_i} \right) \left(\prod_{j=1}^{q} (X - z_j)^{s_j} (X - \bar{z_j})^{s_j} \right)$$

avec $a_1, \cdots, a_p$ les racines réelles de P, $z_1, \bar{z_1}, \cdots, z_q, \bar{z_q}$ les racines complexes non réelles de P.

En effectuant le produit des facteurs conjugué, on obtient la factorisation **réelle** suivante :

$$P(X) = \lambda \left(\prod_{i=1}^{p} (X - a_i)^{\alpha_i} \right) \left(\prod_{j=1}^{q} (X^2 - (z_j + \bar{z_j})X + z_j\bar{z_j})^{s_j} \right).$$

D'où l'existence de la factorisation. L'unicité découle alors du fait que λ est le coefficient dominant de P, $a_1, \cdots, a_p$ les racines réelles de P et $\alpha_1, \cdots, \alpha_p$ leurs multiplicités, $z_1, \bar{z_1}, \cdots, z_q, \bar{z_q}$ les racines complexes non réelles de P et $s_1, \cdots, s_q$ leurs multiplicités. Or ces éléments sont déterminés uniquement par le polynôme P.

Fin du (1) Montrons que les seuls polynômes irréductibles sont de degré 1 et de degré 2 à $\Delta < 0$: si P n'est pas de l'une de ces deux formes, alors :

- soit $\deg(P) = 2$ et $\Delta \geq 0$: P est réductible dans $\mathbb{R}[X]$, puisqu'il se factorise en produit de deux polynômes de degré 1 ;
- soit $\deg(P) \geq 3$: P est réductible d'après la factorisation obtenue en (2).

□

► *Pour factoriser sur $\mathbb{R}$, on peut factoriser sur $\mathbb{C}$, puis regrouper les termes complexes conjugués (comme dans la preuve précédente).*

Exemple. Factorisons $X^4 + 1$ dans $\mathbb{R}[X]$.

- Méthode 1 : On cherche la factorisation de X^4+1 dans $\mathbb{C}[X]$ pour commencer. On cherche pour cela les solutions de $z^4=-1$. Ce sont les racines 4^{iemes} de $-1=e^{i\pi}$:

$$z_k = e^{i\frac{\pi}{4}+i\frac{k\pi}{2}} \text{ avec } k=0,\cdots,3.$$

On a $z_0=\bar{z_3}$, $z_1=\bar{z_2}$. Ainsi X^4+1 a quatre racines complexes distinctes. Puisque X^4+1 est de degré 4 et unitaire, on obtient :

$$\begin{aligned} X^4+1 &= \prod_{k=0}^{3}(X-z_k) \text{ factorisation dans } \mathbb{C}[X] \\ &= (X-z_0)(X-\bar{z_0})(X-z_1)(X-\bar{z_1}) \\ &= (X^2-2Re(z_0)X+|z_0|^2)(X^2-2Re(z_1)X+|z_1|^2) \\ &= (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1) \end{aligned}$$

- Méthode 2 : On utilise l'astuce suivante :

$$X^4+1=(X^2+1)^2-2X^2=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$

C'est la factorisation irréductible de X^4+1 dans $\mathbb{R}[X]$ car ces deux polynômes sont à $\Delta<0$.

Exemple. Factorisons le polynôme X^n-1 dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ ($n\geq 1$). On a déjà obtenu la factorisation dans $\mathbb{C}[X]$:

$$X^n-1=\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right).$$

Pour obtenir la factorisation dans $\mathbb{R}$, on doit distinguer les cas n pair et n impair.

- Si $n=2k$ est pair, on a en regroupant les termes complexes conjugués :

$$\begin{aligned} X^{2k}-1 &= (X-1)(X+1)\prod_{j=1}^{k-1}\left(X-e^{\frac{ij\pi}{n}}\right)\left(X-e^{\frac{-jk\pi}{n}}\right) \\ &= (X-1)(X+1)\prod_{j=1}^{k-1}\left(X-2\cos(\frac{j\pi}{n})X+1\right). \end{aligned}$$

- Si $n=2k+1$ est impair, on a de même :

$$\begin{aligned} X^{2k+1}-1 &= (X-1)\prod_{j=1}^{k}\left(X-e^{\frac{ij\pi}{n}}\right)\left(X-e^{\frac{-ij\pi}{n}}\right) \\ &= (X-1)\prod_{j=1}^{k}\left(X-2\cos(\frac{j\pi}{n})X+1\right). \end{aligned}$$

5.4 Relations entre coefficients et racines

Rappelons le résultat suivant.

Propriété 31 (Relations coefficients racines)

Soit $P(X)=aX^2+bX+c\in\mathbb{K}[X]$. Alors :

$$\alpha_1,\alpha_2 \text{ sont racines de } P \quad\Leftrightarrow\quad \begin{cases}\alpha_1+\alpha_2=-\frac{b}{a}\\ \alpha_1\alpha_2=\frac{c}{a}\end{cases}$$

Preuve.

$\Rightarrow$ Si α_1, α_2 sont racines de P, alors P est scindé et $P = a(X-\alpha_1)(X-\alpha_2)$. En développant et en identifiants les coefficients, on obtient $\begin{cases} \alpha_1+\alpha_2 = -\frac{b}{a} \\ \alpha_1\alpha_2 = \frac{c}{a} \end{cases}$.

$\Leftarrow$ Supposons que $\begin{cases} \alpha_1+\alpha_2 = -\frac{b}{a} \\ \alpha_1\alpha_2 = \frac{c}{a} \end{cases}$. Alors $P = a(X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2) = a(X-\alpha_1)(X-\alpha_2)$.

□

Ce résultat se généralise aux polynômes de degré n de la manière suivante.

Propriété 32

Soit $P = \sum_{k=0}^{n} p_k X^k \in \mathbb{K}[X]$ un polynôme scindé, $a_1, \cdots, a_n$ ses racines (distinctes ou non). Alors :

$$-\frac{p_{n-1}}{p_n} = \sum_{k=1}^{n} a_k \quad \text{et} \quad (-1)^n \frac{p_0}{p_n} = \prod_{k=1}^{n} a_k.$$

Preuve. Comme P est scindé, et les a_i sont ses racines, P s'écrit sous la forme

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

avec λ le coefficient dominant de P. En développant, on obtient :

$$P = \lambda \prod_{i=1}^{n} (X - a_i) = \lambda X^n - \lambda(a_1 + \cdots + a_n)X^{n-1} + \cdots + (-1)^n \lambda \prod_{i=1}^{n} a_i.$$

En identifiant avec les coefficients de P, on obtient :

$$p_n = \lambda \quad ; \quad p_{n-1} = -\lambda \sum_{i=1}^{n} a_i \quad ; \quad p_0 = \lambda(-1)^n \prod_{i=1}^{n} a_i.$$

Ainsi, on obtient bien $\prod_{i=1}^{n} a_i = (-1)^n \frac{p_0}{p_n}$ et $\sum_{i=1}^{n} a_i = -\frac{p_{n-1}}{p_n}$. □

Exemple. Les racines de $P = X^n - 1$ dans $\mathbb{C}$ sont les racines n-ièmes de l'unité. Il y en a $n = d^\circ(X^n - 1)$, donc P est scindé. D'après les relations coefficients racines,

$$\sum_{\omega \in \mathbb{U}_n} \omega = -\frac{0}{1} = 0 \quad \text{et} \quad \prod_{\omega \in \mathbb{U}_n} \omega = (-1)^n \frac{-1}{1} = (-1)^{n+1}.$$