

Les polynômes

Dans tout ce chapitre, K désigne un corps commutatif.

$K = \mathbb{R}$ ou bien $K = \mathbb{C}$

\mathbb{R} = Les nombres réels, \mathbb{C} = Les nombres complexes.

Définition 1 : On appelle polynôme à une indéterminée X de degré $n \in \mathbb{N}$ à coefficients a_i tel que $i \in \{0, \dots, n\}$, $a_i \in K$, toute écriture de la forme suivante :

$$P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n \quad \text{où } a_i \in K, \forall i \in \{0, \dots, n\} \text{ et } a_n \neq 0$$

On peut noter $P(X)$ par P , on écrit donc $P(X) = P$

Remarque : On peut ajouter à la définition précédente

X^n est X puissance n

a_nX^n est la multiplication de a_n et X^n

Donc on peut écrire $a_0 = a_0X^0$

Définition 2 : On appelle degré de P et on note par $\deg P$ ou bien $d^\circ P$

Le nombre $d^\circ P = \max \{i \in \mathbb{N}, a_i \neq 0\}$

Remarques : Dans les définitions précédentes on a :

- 1) Si $a_i = 0, \forall i \in \{0, \dots, n\}$, P est dit le polynôme nul et on note $P = 0$
Par convention, on pose $d^\circ 0 = -\infty$
- 2) Si $a_0 \neq 0$ et $a_i = 0 \forall i \in \{1, \dots, n\}$, P est dit polynôme constant.
- 3) Si $P \neq 0$ et $d^\circ P = n$, alors le terme a_n est appelé terme du plus grand degré ou bien terme dominant, si de plus $a_n = 1$, P est dit polynôme unitaire.

Exemple : Le polynôme $P(X) = 1 + 4X + X^2$ est un polynôme unitaire.

Notations : Dans la définition 1 on a :

- 1) L'ensemble des polynômes à l'indéterminée X à coefficients dans K se note $K[X]$.
- 2) L'ensemble des polynômes de $K[X]$ de degré inférieur ou égal à n se note $K_n[X]$.

Opérations : Soient $P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ et

$$Q(X) = b_0 + b_1X + b_2X^2 + \dots + b_mX^m \quad \text{deux polynômes de } K[X] \text{ tels que } n \leq m$$

Soit un élément $\lambda \in K$

- 1) La somme $P + Q$ des polynômes P et Q est le polynôme noté $(P + Q)(X)$ tel que

$$(P + Q)(X) =$$

$$(a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \dots + (a_n + b_n)X^n + (a_{n+1} + b_{n+1})X^{n+1}$$

$$+ \dots + (a_m + b_m)X^m \quad \text{avec } a_i = 0, \forall i \in \{n+1, \dots, m\}$$

2) On appelle produit des polynômes P et Q , le polynôme noté $(PQ)(X)$ tel que

$$(PQ)(X) = \sum_{k=0}^{n+m} C_k X^k$$

$$\text{où } C_k = \sum_{i=0}^{i=k} a_i b_{k-i}$$

3) On appelle produit de polynôme P par l'élément λ , le polynôme noté $(\lambda P)(X)$ tel que $(\lambda P)(X) = (\lambda a_0) + (\lambda a_1)X + (\lambda a_2)X^2 + \dots + (\lambda a_n)X^n$

4) On appelle polynôme dérivé du polynôme

$P(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$, le polynôme noté $P'(X)$ tel que :

$$P'(X) = a_1 + 2a_2X + \dots + na_nX^{n-1}$$

Notations : on note :

$P^{(0)} = P, P^{(1)} = P', P^{(2)} = P'', \dots, P^{(k)} = (P^{(k-1)})'$ où $P^{(k)}$ est appelé la dérivée d'ordre k de $P(X)$.

Exemple : $P(X) = 2 + 3X - X^2 \Rightarrow P'(X) = 3 - 2X$

Proposition : Soient P, Q deux polynômes de $K[X]$, alors :

$$(P + Q)' = P' + Q'$$

$$(PQ)' = P'Q + PQ'$$

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

$$\text{Où } C_n^k = \frac{n!}{k!(n-k)!} \quad \text{C'est la formule de Leibnitz}$$

$$\forall \lambda \in K, (\lambda P)' = \lambda P'$$

Arithmétique dans $K[X]$:

Définition : Soient A, B deux polynômes de $K[X]$ tel que $B \neq 0$, on dit que B divise A et on écrit B/A s'il existe un polynôme $Q \in K[X]$ tel que $A = BQ$

On dit que B est un diviseur de A ou bien A est divisible par B .

Division euclidienne :

Proposition – définition : Soient A, B deux polynômes de $K[X]$ avec $\deg A \geq \deg B, B \neq 0$ alors il existe un unique couple (Q, R) de polynômes dans $K[X]$ tels que : $A = BQ + R$ avec

$\deg R < \deg B$, c'est la division euclidienne de A par B , Q s'appelle le quotient de la division euclidienne de A par B et R s'appelle le reste de la division euclidienne de A par B , si le $R = 0$, on dit que A est divisible par B ou que B divise A .

Exemple 1 : $A(X) = X^5 + X^4 + 1$, $B(X) = X^2 + X + 1$

La division euclidienne de A par B donne :

le quotient $Q(X) = X^3 - X + 1$ et le reste $R(X) = 0$

Nous effectuons la division euclidienne de $A(X)$ par $B(X)$ comme suit :

$X^5 + X^4 + 1$	$X^2 + X + 1$
+	
$-(X^5 + X^4 + X^3)$	$X^3 - X + 1$
= $-X^3 + 1$	
+	
$-(X^3 - X^2 - X)$	
= $X^2 + X + 1$	
+	
$-(X^2 + X + 1)$	
= 0	

$$A(X) = B(X)Q(X) + 0$$

Exemple 2 : $A(X) = X^3 + 4X^2 + 5X + 1$, $B(X) = X^2 + X + 1$

La division euclidienne de A par B donne le quotient $Q(X) = X + 3$ et $R(X) = X - 2$

Nous effectuons la division euclidienne de $A(X)$ par $B(X)$ comme suit :

$X^3 + 4X^2 + 5X + 1$	$X^2 + X + 1$
+	
$-(X^3 + X^2 + X)$	$X + 3$
= $3X^2 + 4X + 1$	
+	
$-(3X^2 + 3X + 3)$	
= $X - 2$	

$$A(X) = B(X)Q(X) + R(X)$$

Remarque : Dans la division euclidienne d'un polynôme A par un polynôme B , il faut écrire tous les polynômes suivant les puissances décroissantes en l'indéterminé X ainsi que les polynômes A et B .

PGCD de deux polynômes : Un plus grand diviseur commun de deux polynômes A et B est un polynôme Q de degré le plus grand possible qui divise à la fois A et B . On dit que Q est un PGCD de A et B . On le note un $PGCD(A, B)$

Remarque : Un PGCD de deux polynômes n'est pas unique, il est unique à coefficients près.

On s'intéresse maintenant au plus grand diviseur commun unitaire de deux polynômes A et B qui est unique.

Notation : Le plus grand diviseur commun unitaire de deux polynômes A et B est noté Le $PGCD(A, B)$.

Proposition : Soient A et B deux polynômes de $K[X]$, et soit R le reste de la division euclidienne de A par B alors :

Le $PGCD(A, B) = \text{Le } PGCD(B, R)$ et si B est un diviseur de A (c'est-à-dire $R = 0$) alors

Le $PGCD(A, B) = B$

Algorithme de PGCD : Soient A et B deux polynômes de $K[X]$, $B \neq 0$ tels que $\deg B \leq \deg A$, alors suivant la théorie de la division euclidienne on a :

$$A = BQ_0 + R_0 \quad \text{avec} \quad \deg R_0 < \deg B \quad \text{et} \quad R_0 \neq 0$$

$$B = R_0Q_1 + R_1 \quad \text{avec} \quad \deg R_1 < \deg R_0 \quad \text{et} \quad R_1 \neq 0$$

$$R_0 = R_1Q_2 + R_2 \quad \text{avec} \quad \deg R_2 < \deg R_1 \quad \text{et} \quad R_2 \neq 0$$

$$R_1 = R_2Q_3 + R_3 \quad \text{avec} \quad \deg R_3 < \deg R_2 \quad \text{et} \quad R_3 \neq 0$$

⋮

⋮

⋮

$$R_{n-1} = R_nQ_{n+1} + R_{n+1} \quad \text{avec} \quad R_{n+1} = 0$$

Comme la suite $\deg(R_i)$ est strictement décroissante et positive alors il viendra un moment où $R_{n+1} = 0$, avec R_{n+1} est le reste de la division euclidienne de R_{n-1} par R_n

En utilisant la proposition précédente on a :

$$\text{Le } PGCD(A, B) = \text{Le } PGCD(B, R_0) =$$

$$\text{Le } PGCD(R_0, R_1) = \dots \dots \dots = \text{Le } PGCD(R_{n-1}, R_n) = R_n, \text{ car } R_{n+1} = 0$$

c'est-à-dire que Le $PGCD(A, B)$ est le dernier reste unitaire non nul dans cette suite des divisions euclidiennes.

Exemple : Soient A et B deux polynômes définis comme suit :

$$A(X) = X^5 - 2X^4 - 6X^3 + 5X^2 + 8X + 12$$

$$B(X) = X^4 + X^3 - X - 1$$

$$A = BQ_0 + R_0 \quad \text{où } Q_0 = X - 3, R_0 = -3X^3 + 6X^2 + 6X + 9$$

$$B = R_0Q_1 + R_1 \quad \text{où } Q_1 = \frac{-1}{3}X - 1, R_1 = 8X^2 + 8X + 8$$

$$R_0 = R_1Q_2 + R_2 \quad \text{où } Q_2 = \frac{-3}{8}X + \frac{9}{8}, R_2 = 0$$

$$\text{Le } PGCD(A, B) = \frac{1}{8}R_1 = X^2 + X + 1$$

Remarque : On a effectué la division euclidienne de A par B , ensuite de B par R_0 , ensuite de R_0 par R_1

Polynômes premiers entre eux : Deux polynômes P et Q sont dites premiers entre eux si et seulement si leur $PGCD$ est égal à 1 c'est-à-dire $\text{Le } PGCD(P, Q) = 1$

Théorèmes de Bézout : Soient P et Q deux polynômes premiers entre eux, alors il existe

$$u_1, u_2 \in K[X] \text{ tels que : } u_1P + u_2Q = 1$$

Théorème de Gauss : Soient A, B et C trois polynômes de $K[X]$ alors :

$$(A \text{ divise } BC) \text{ et } (\text{Le } PGCD(A, B) = 1) \Rightarrow A \text{ divise } C$$

Division suivant les puissances croissantes de X : Soient A et B deux polynômes tels que :

$$A(X) = a_0 + a_1X + a_2X^2 + \dots + a_mX^m \in K[X] \text{ et}$$

$$B(X) = b_0 + b_1X + b_2X^2 + \dots + b_nX^n \in K[X] \text{ tels que } b_0 \neq 0 \text{ et } h \in \mathbb{N}$$

Il existe un couple unique de polynômes (Q, R) tel que $A = BQ + X^{h+1}R$ avec $\deg Q \leq h$

Q s'appelle le quotient de la division suivant les puissances croissantes de A par B à l'ordre h

Et $X^{h+1}R$ s'appelle le reste de la division suivant les puissances croissantes de A par B à l'ordre h .

Exemple : Soient deux polynômes A et B définis comme suit :

$$A(X) = 1 - 2X + X^2 - 4X^4 + 2X^5 \quad \text{et} \quad B(X) = 1 + X^2, \quad h = 3$$

$$A = BQ + X^{h+1}R \quad \text{où } Q(X) = 1 - 2X + 2X^3, \quad R = -4$$

Nous effectuons la division suivant les puissances croissantes de $A(X)$ par $B(X)$ à l'ordre 3 comme suit :

$1 - 2X + X^2 - 4X^4 + 2X^5$	$1 + X^2$
$+$	<hr style="width: 100%;"/>
$-(1 + X^2)$	$1 - 2X + 2X^3$
<hr style="width: 100%;"/> $= -2X - 4X^4 + 2X^5$	
$+$	
$-(2X - 2X^3)$	
<hr style="width: 100%;"/> $= 2X^3 - 4X^4 + 2X^5$	
$+$	
$-(2X^3 + 2X^5)$	
<hr style="width: 100%;"/> $= -4X^4 = X^{h+1}R$	

C'est la division suivant les puissances croissantes de A par B à l'ordre $h = 3$

Remarque : Dans la division suivant les puissances croissantes d'un polynôme A par un polynôme B , il faut écrire tous les polynômes suivant les puissances croissantes.

Zéros des polynômes :

Définition : Soit $P \in K[X]$ et $\alpha \in K$, on dit que α est une racine de P ou bien on dit que α est un zéro de P si et seulement si $P(\alpha) = 0$

Proposition : Soit $P \in K[X]$ et $\alpha \in K$,

α est une racine de $P \Leftrightarrow (X - \alpha)$ divise $P(X)$

$$\Leftrightarrow \exists Q(X) \in K[X] \text{ tel que } P(X) = (X - \alpha)Q(X)$$

Multiplicité d'une racine :

Définition : Soient $P \in K[X]$ et $\alpha \in K, k \in \mathbb{N} - \{0\}$,

On dit que α est une racine de P d'ordre de multiplicité k si et seulement si $(X - \alpha)^k$ divise P et $(X - \alpha)^{k+1}$ ne divise pas P .

Remarques : Dans la définition précédente si :

$k = 1$ donc α est une racine simple de P .

$k = 2$ donc α est une racine double de P .

$k = 3$ donc α est une racine triple de P .

Proposition : Soit $P \in K[X]$ et $\alpha \in K, k \in \mathbb{N} - \{0\}$,

$$\alpha \text{ est une racine de } P \text{ d'ordre de multiplicité } k \Leftrightarrow \begin{cases} P(\alpha) = 0 \\ P^{(1)}(\alpha) = 0 \\ \vdots \\ P^{(k-1)}(\alpha) = 0 \\ P^{(k)}(\alpha) \neq 0 \end{cases}$$

Remarque : dans la proposition précédente, on dit que α est une racine de P d'ordre de multiplicité k ou bien simplement α est une racine de P d'ordre k .

Exemple : $\alpha = 1$ est une racine de $P(X)$.

$P(X) = X^3 - X^2 - X + 1$, α est une racine de P d'ordre de multiplicité 2 car :

$$P(1) = 0,$$

$$P'(X) = 3X^2 - 2X - 1$$

$$P'(1) = 0$$

$$P''(X) = 6X - 2$$

$$P''(1) \neq 0$$

Proposition : Soient P un polynôme à coefficients réels et Z un nombre complexe non réel, alors si Z est une racine de P d'ordre k alors le conjugué de Z noté \bar{Z} est aussi une racine de P de même ordre k .

Factorisation des polynômes :

Définition : Soit $P \in K[X]$, on dit que P est irréductible dans $K[X]$ si et seulement si

$$\forall A, B \in K[X], P = AB \Rightarrow A = \text{constante ou bien } B = \text{constante}$$

On peut déduire facilement le corollaire suivant :

Corollaire :

- 1) Les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de la forme $P(X) = aX + b$ où $a, b \in \mathbb{C}$
- 2) Les seuls polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de la forme $P(X) = aX + b$ où $a, b \in \mathbb{R}$
 $P(X) = aX^2 + bX + c$ où $a, b, c \in \mathbb{R}$ de discriminant $\Delta = b^2 - 4ac < 0$

Théorème de d'Alembert -Gauss : Tout polynôme non constant de $K[X]$, se factorise de façon unique en produit de polynômes irréductibles et unitaires dans $K[X]$.

Autrement dit :

Dans $\mathbb{C}[X]$:

$$\forall P \in \mathbb{C}[X], P \text{ non constant, } \exists \lambda \in \mathbb{C} - \{0\}, \exists n \in \mathbb{N} - \{0\}, \exists \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$$

deux à deux distincts, $\exists r_1, r_2, \dots, r_n \in \mathbb{N} - \{0\}$ tels que :

$$P(X) = \lambda \prod_{k=1}^{k=n} (X - \alpha_k)^{r_k} = \lambda (X - \alpha_1)^{r_1} (X - \alpha_2)^{r_2} \dots \dots \dots (X - \alpha_n)^{r_n}$$

Dans $\mathbb{R}[X]$:

$\forall P \in \mathbb{R}[X]$, P non constant, $\exists \lambda \in \mathbb{R} - \{0\}$, il existe un unique couple (A, B) de polynômes unitaires dans $\mathbb{R}[X]$ tel que :

$$P(X) = \lambda A(X)B(X) \text{ avec}$$

$$A(X) = (X - \alpha_1)^{r_1} (X - \alpha_2)^{r_2} \dots \dots \dots (X - \alpha_n)^{r_n}$$

Et

$$B(X) = (X^2 + p_1X + q_1)^{s_1} (X^2 + p_2X + q_2)^{s_2} \dots \dots \dots (X^2 + p_mX + q_m)^{s_m}$$

Avec $(p_i)^2 - 4q_i < 0$ pour tout $1 \leq i \leq m$

$$\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R} \quad r_1, r_2, \dots, r_n \in \mathbb{N} - \{0\}, \quad p_1, p_2, \dots, p_m \in \mathbb{R}$$

$$q_1, q_2, \dots, q_m \in \mathbb{R}, \quad s_1, s_2, \dots, s_m \in \mathbb{N} - \{0\}.$$

Et on a $\alpha_1, \alpha_2, \dots, \alpha_n$ deux à deux distincts et les couples

$(p_1, q_1), (p_2, q_2), \dots, (p_m, q_m)$ deux à deux distincts.

Exercice : Soit $P(X) = X^5 - 2X^4 + X^3 - X^2 + 2X - 1$ un polynôme de $\mathbb{R}[X]$

1) Montrer par deux méthodes différentes que $X_0 = 1$ est une racine triple de P .

2) Factoriser P en facteurs irréductible dans $\mathbb{R}[X]$.

Solution : $P(X) = X^5 - 2X^4 + X^3 - X^2 + 2X - 1 \in \mathbb{R}[X]$

1) $X_0 = 1$ est une racine triple de P

Première méthode :

$X_0 = 1$ est une racine triple de P c'est-à-dire que $X_0 = 1$ est une racine de P d'ordre de multiplicité $k = 3$

Selon une proposition vue dans le cours on a :

$$X_0 = 1 \text{ est une racine triple de } P \Leftrightarrow \begin{cases} P(1) = 0 \\ P'(1) = 0 \\ P''(1) = 0 \\ P'''(1) \neq 0 \end{cases}$$

$$P'(X) = 5X^4 - 8X^3 + 3X^2 - 2X + 1$$

$$P'(1) = 0$$

$$P''(X) = 20X^3 - 24X^2 + 6X - 2$$

$$P''(1) = 0$$

$$P'''(X) = 60X^2 - 48X + 6$$

$P'''(1) = 18 \neq 0$ donc $X_0 = 1$ est une racine de P d'ordre de multiplicité $k = 3$

Conclusion : $X_0 = 1$ est une racine triple de P

Deuxième méthode :

$$P(X) = X^5 - 2X^4 + X^3 - X^2 + 2X - 1 \in \mathbb{R}[X]$$

Selon la définition du cours :

$X_0 = 1$ est une racine triple de $P \Leftrightarrow (X - 1)^3$ divise P et $(X - 1)^4$ ne divise pas P

- Montrons que $(X - 1)^3$ divise P :

Le reste de la division euclidienne de P par $(X - 1)^3 = X^3 - 3X^2 + 3X - 1$ est nul,

En effet :

$X^5 - 2X^4 + X^3 - X^2 + 2X - 1$	$X^3 - 3X^2 + 3X - 1$
+	
$-(X^5 - 3X^4 + 3X^3 - X^2)$	$X^2 + X + 1$
=	
$X^4 - 2X^3 + 2X - 1$	
+	
$-(X^4 - 3X^3 + 3X^2 - X)$	
=	
$X^3 - 3X^2 + 3X - 1$	
+	
$-(X^3 - 3X^2 + 3X - 1)$	
=	
0	

Donc $(X - 1)^3$ divise P

- Montrons maintenant que $(X - 1)^4$ ne divise pas P :

Supposons que $(X - 1)^4$ divise P

Si $(X - 1)^4$ divise P donc selon la définition de la divisibilité on peut trouver $Q(X) \in \mathbb{R}[X]$ tel que $P(X) = (X - 1)^4 Q(X)$.

Mais selon la division euclidienne précédente on a $P(X) = (X - 1)^3(X^2 + X + 1)$

On peut déduire que $(X - 1)^4 Q(X) = (X - 1)^3(X^2 + X + 1)$

Cette dernière relation entraîne que $(X - 1)^4 Q(X) - (X - 1)^3(X^2 + X + 1) = 0$

Donc : $(X - 1)^3[(X - 1)Q(X) - (X^2 + X + 1)] = 0$

Et comme $(X - 1)^3$ divise P donc selon la définition de la divisibilité $(X - 1)^3 \neq 0$, on peut déduire que $[(X - 1)Q(X) - (X^2 + X + 1)] = 0$

donc $(X^2 + X + 1) = (X - 1)Q(X)$, c'est-à-dire $(X - 1)$ divise $(X^2 + X + 1)$

et selon une proposition vue dans le cours donc $X_0 = 1$, est une racine de $(X^2 + X + 1)$

alors selon la définition d'une racine d'un polynôme on a : $(1)^2 + 1 + 1 = 0$

C'est une contradiction donc $(X - 1)^4$ ne divise pas P

Conclusion : $X_0 = 1$ est une racine triple de P

2) Factoriser P en facteur irréductible dans $\mathbb{R}[X]$

Factoriser un polynôme P en facteur irréductible dans $\mathbb{R}[X]$ c'est-à-dire factoriser ce polynôme en produit de polynômes irréductibles et unitaires dans $\mathbb{R}[X]$.

Cette écriture est unique selon le théorème de d'Alembert - Gauss

On a :

$$P(X) = (X - 1)^3(X^2 + X + 1)^1$$

Le polynôme $(X - 1)$ est un polynôme de $\mathbb{R}[X]$, irréductible dans $\mathbb{R}[X]$ et il est unitaire.

Le polynôme $(X^2 + X + 1)$ est un polynôme de $\mathbb{R}[X]$ et il est unitaire.

Le polynôme $(X^2 + X + 1)$ est irréductible dans $\mathbb{R}[X]$ puisqu'il est de degré égal à 2,

et $\Delta(X^2 + X + 1) < 0$

Conclusion : L'écriture $P(X) = (X - 1)^3(X^2 + X + 1)^1$ est la factorisation du polynôme $P(X)$ en produit de polynômes irréductibles et unitaires dans $\mathbb{R}[X]$.

Remarque : pour la factorisation de $P(X)$ en produit de polynômes irréductibles et unitaires dans $\mathbb{C}[X]$, on peut la déduire facilement à partir de l'écriture suivante :

$$P(X) = (X - 1)^3(X^2 + X + 1)^1$$

Puisque $\Delta(X^2 + X + 1) < 0$ donc les racines du polynôme $h(X) = X^2 + X + 1$ sont complexes non réels

Soient α et λ les racines du polynôme $h(X) = X^2 + X + 1$

Donc $X^2 + X + 1 = (X - \alpha)(X - \lambda)$

$$\text{tels que } \alpha = \frac{-1}{2} + i\frac{\sqrt{3}}{2} \text{ et } \lambda = \frac{-1}{2} - i\frac{\sqrt{3}}{2}$$

On peut donc écrire :

$$P(X) = (X - 1)^3(X - \alpha)(X - \lambda) \text{ tels que } \alpha = \frac{-1}{2} + i\frac{\sqrt{3}}{2} \text{ et } \lambda = \frac{-1}{2} - i\frac{\sqrt{3}}{2}$$

est la factorisation de $P(X)$ en produit de polynômes irréductibles et unitaires dans $\mathbb{C}[X]$.