Mathématiques pour l'informatique 2

Polynômes

Émilie Charlier

Université de Liège

Ensemble $\mathbb{K}$

Nous supposerons partout dans le cours que $\mathbb{K}$ est l'un des quatre ensembles de nombres suivants : $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{Z}_m$ avec m un nombre premier

Lorsque nous utiliserons les notations $+$ et $\cdot$ entre éléments de $\mathbb{K}$, il est entendu que nous faisons référence à l'addition et la multiplication usuelle dans $\mathbb{K}$.

Rappelons que l'addition et la multiplication dans $\mathbb{Z}_m$ étaient notées $+_m$ et $\cdot_m$ dans le cours "Mathématique pour l'informatique 1". Nous ne prendrons plus toujours ces précautions s'il est clair que nous travaillons dans $\mathbb{Z}_m$.

Nous utiliserons la notation $\mathbb{K}_0$ pour désigner l'ensemble $\mathbb{K} \setminus \{0\}$.

Polynômes formels

Définition

Un polynôme à coefficients dans $\mathbb{K}$ est une expression de la forme

$$P = p_0 + p_1 X + p_2 X^2 + \cdots + p_d X^d$$

où d est un naturel, $p_0, p_1, \ldots, p_d$ sont des éléments de $\mathbb{K}$ et où X est un symbole spécial.

Les éléments $p_0, p_1, \ldots$ de $\mathbb{K}$ sont appelés les coefficients de P tandis que X est appelé l'indéterminée de P.

Lorsque $P \neq 0$, le naturel d est appelé le degré de P et est noté $\deg(P)$. Par convention, on pose $\deg(0) = -\infty$.

Le coefficient p_d est appelé le coefficient dominant de P.

Un polynôme constant est un polynôme de degré 0 ou $-\infty$.

L'ensemble des polynômes à coefficients dans $\mathbb{K}$ et d'intéterminée X est noté $\mathbb{K}[X]$.

Exemple

Soient $P = 2X^3 + 3X^2 - 1$ et $Q = X^2 - X + 2$.

- On peut voir P et Q vu comme des polynômes de $\mathbb{Q}[X]$.
- On peut aussi les voir comme des polynômes de $\mathbb{Z}_3[X]$.
  Dans ce cas, on a $P = 2X^3 + 2$ et $Q = X^2 + 2X + 2$.

Un polynôme est donné par la suite de ses coefficients.

Formellement, un polynôme de $\mathbb{K}[X]$ est en fait simplement une suite finie de $\mathbb{K}$, c'est-à-dire une suite d'éléments de $\mathbb{K}$ valant 0 à partir d'un certain rang :

$$P = (p_0, p_1, \ldots, p_d, 0, 0, \ldots).$$

Ainsi, lorsqu'on ne souhaite pas spécifier le degré d'un polynôme P, on écrit plus généralement

$$P = p_0 + p_1 X + p_2 X^2 + \cdots$$

où il est entendu que $p_i = 0$ pour tout $i > \deg(P)$.

Manipuler des polynômes

On munit l'ensemble $\mathbb{K}[X]$ de deux opérations internes

$$\mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X], (P, Q) \mapsto P + Q \qquad \text{(somme)}$$
$$\mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X], (P, Q) \mapsto P \cdot Q \qquad \text{(produit)}$$

et d'une opération externe

$$\mathbb{K} \times \mathbb{K}[X] \to \mathbb{K}[X], (k, P) \mapsto kP. \qquad \text{(multiplication scalaire)}$$

Manipuler des polynômes

Si $P = p_0 + p_1 X + p_2 X^2 + \cdots$ et $Q = q_0 + q_1 X + q_2 X^2 + \cdots$ sont des polynômes de $\mathbb{K}[X]$ et si $k \in \mathbb{K}$, alors

$$P + Q = (p_0 + q_0) + (p_1 + q_1)X + (p_2 + q_2)X^2 + \cdots$$
$$P \cdot Q = (p_0 q_0) + (p_0 q_1 + p_1 q_0)X + (p_0 q_2 + p_1 q_1 + p_2 q_0)X^2 + \cdots$$
$$kP = (kp_0) + (kp_1)X + (kp_2)X^2 + \cdots .$$

Autrement dit, pour tout $n \in \mathbb{N}$, le coefficient de X^n dans

- $P + Q$ est égal à $p_n + q_n$
- $P \cdot Q$ est égal à $\sum_{i=0}^{n} p_i \, q_{n-i}$
- kP est égal à kp_n.

Exemple

- Soient $P = 3X^3 + 2X^2 - 1$ et $Q = X^2 - X + 2$ vu comme polynômes de $\mathbb{Q}[X]$. On calcule

$$\begin{aligned}
P + Q &= 3X^3 + (2+1)X^2 - X + (-1+2) \\
&= 3X^3 + 3X^2 - X + 1 \\
P \cdot Q &= (3 \cdot 1)X^5 + (3 \cdot (-1) + 2 \cdot 1)\, X^4 + (3 \cdot 2 + 2 \cdot (-1))\, X^3 \\
&\quad + (2 \cdot 2 + (-1) \cdot 1)\, X^2 + ((-1) \cdot (-1))\, X + ((-1) \cdot 2) \\
&= 3X^5 - X^4 + 4X^3 + 3X^2 + X - 2 \\
3P &= (3 \cdot 3)X^3 + (3 \cdot 2)X^2 + (3 \cdot (-1)) \\
&= 9X^3 + 6X^2 - 3.
\end{aligned}$$

Exemple

- Soient $P = 3X^3 + 2X^2 - 1$ et $Q = X^2 - X + 2$ vu comme polynômes de $\mathbb{Z}_3[X]$. On a donc $P = 2X^2 + 2$, $Q = X^2 + 2X + 2$ et $\deg(P) = \deg(Q) = 2$.

$$
\begin{aligned}
P + Q &= (2X^2 + 2) + (X^2 + 2X + 2) \\
&= 3X^2 + 2X + (2 + 2) \\
&= 2X + 1 \\
P \cdot Q &= (2X^2 + 2)(X^2 + 2X + 2) \\
&= (2 \cdot 1)X^4 + (2 \cdot 2)X^3 + (2 \cdot 2 + 2 \cdot 1)X^2 \\
&\quad + (2 \cdot 2)X + (2 \cdot 2) \\
&= 2X^4 + X^3 + X + 1 \\
3P &= 0P = 0.
\end{aligned}
$$

La proposition suivante explicite le comportement du degré par rapport à ces trois opérations.

Proposition

Pour tous $P, Q \in \mathbb{K}[X]$ et tous $k \in \mathbb{K}_0$, on a

1. $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$,
2. $\deg(P \cdot Q) = \deg(P) + \deg(Q)$,
3. $\deg(kP) = \deg(P)$.

Remarquons que ces formules sont correctes même si P ou Q est nul, avec la convention que $\max\{-\infty, d\} = d$ et $-\infty + d = -\infty$ pour tout $d \in \mathbb{N} \cup \{-\infty\}$.

$\mathbb{K}[X]$ est intègre

.

Corollaire

Si $P, Q \in \mathbb{K}[X]$ sont tels que $P \cdot Q = 0$, alors $P = 0$ ou $Q = 0$.

Preuve

Nous montrons la contraposée. Si P et Q sont deux polynômes non nuls de $\mathbb{K}[X]$, alors $\deg(P \cdot Q) = \deg(P) + \deg(Q) \geq 0$, et donc $P \cdot Q \neq 0$.

Division euclidienne de polynômes

De la même façon que nous avons montré la division euclidienne dans $\mathbb{Z}$ dans le cours "Mathématiques pour l'informatique 1", nous pouvons montrer le résultat suivant.

Théorème (Division euclidienne de polynômes)

Pour tous polynômes $P, D \in \mathbb{K}[X]$ tels que $D \neq 0$, il existe des polynômes $Q, R \in \mathbb{K}[X]$ uniques tels que $P = QD + R$ et $\deg(R) < \deg(D)$.

Exemple

Avant de donner une preuve de ce théorème, considérons un exemple qui nous aidera à comprendre le raisonnement utilisé dans cette preuve.

Soient $P = 6X^5 + X^4 - X^3 + 2X - 1$ et $D = 2X^2 + X - 3$.

On souhaite trouver des polynômes Q et R de $\mathbb{Q}[X]$ tels que $P = QD + R$ et $\deg(R) < 2$.

Si de tels polynômes existent, alors nécessairement $\deg(Q) = 3$.

Écrivons donc $Q = aX^3 + bX^2 + cX + d$.

Exemple (suite)

En identifiant les coefficients de X^5 dans l'égalité $P = QD + R$, c'est-à-dire

$$6X^5 + X^4 - X^3 + 2X - 1 = (aX^3 + bX^2 + cX + d)(2X^2 + X - 3) + R$$

on obtient l'équation $6 = 2a$. D'où $a = \frac{6}{2} = 3$.

Nous pouvons donc écrire $Q = 3X^3 + Q'$, avec $Q' = bX^2 + cX + d$.

Exemple (suite)

On doit avoir

$$P = QD + R = \left(3X^3 + Q'\right) D + R$$

donc

$$P - 3X^3 D = Q'D + R.$$

Posons $P' = P - 3X^3 D$.

On a $\deg(P') < \deg(P)$ car

$$\begin{aligned} P' &= (6X^5 + X^4 - X^3 + 2X - 1) - 3X^3(2X^2 + X - 3) \\ &= (6-6)\,X^5 + (1-3)\,X^4 + (-1+9)\,X^3 + 2X - 1 \\ &= -2X^4 + 8X^3 + 2X - 1. \end{aligned}$$

Exemple (suite)

Nous nous sommes ramenés au problème initial où le polynôme P de degré 5 a été remplacé par un polynôme P' de degré 4 : nous devons maintenant trouver des polynômes Q' et R tels que $P' = Q'D + R$ et $\deg(R) < \deg(D)$.

Cette observation nous incitera à utiliser le principe de la récurrence sur le degré du polynôme P dans la démonstration du théorème.

Exemple (suite)

Poursuivons notre raisonnement pour obtenir les coefficients restants de Q, c'est-à-dire b, c, d.

En identifiant les coefficients de X^4 dans l'équation $P' = Q'D + R$, c'est-à-dire

$$-2X^4 + 8X^3 + 2X - 1 = (bX^2 + cX + d)(2X^2 + X - 3) + R$$

on obtient l'équation $-2 = 2b$. D'où $b = -1$.

On peut donc écrire $Q' = -X^2 + Q''$ avec $Q'' = cX + d$.

Exemple (suite)

En posant $P'' = P' + X^2 D$, on doit avoir $P'' = Q''D + R$ et $\deg(P'') < \deg(P')$.

On calcule

$$\begin{aligned} P'' &= \left(-2X^4 + 8X^3 + 2X - 1\right) + X^2(2X^2 + X - 3) \\ &= (-2+2)\,X^4 + (8+1)\,X^3 + (0-3)\,X^2 + 2X - 1 \\ &= 9X^3 - 3X^2 + 2X - 1. \end{aligned}$$

Exemple (suite)

Nous nous sommes à nouveau ramené au problème initial avec maintenant un polynôme P'' de degré 3.

En identifiant les coefficients de X^3 dans l'équation $P'' = Q''D + R$, c'est-à-dire

$$9X^3 - 3X^2 + 2X - 1 = (cX + d)(2X^2 + X - 3) + R$$

on obtient l'équation $9 = 2c$. D'où $c = \frac{9}{2}$.

On peut donc écrire $Q'' = \frac{9}{2}X + Q'''$ avec $Q''' = d$.

Exemple (suite)

En posant $P''' = P'' - \frac{9}{2}XD$, on doit avoir $P''' = Q'''D + R$ et $\deg(P''') < \deg(P'')$.

On calcule

$$\begin{aligned} P''' &= (9X^3 - 3X^2 + 2X - 1) - \frac{9}{2}X(2X^2 + X - 3) \\ &= \left(9 - \frac{9}{2} \cdot 2\right) X^3 + \left(-3 - \frac{9}{2}\right) X^2 + \left(2 - \frac{9}{2} \cdot (-3)\right) X - 1 \\ &= -\frac{15}{2}X^2 + \frac{31}{2}X - 1. \end{aligned}$$

Exemple (suite)

Une fois de plus, nous nous sommes ramenés au problème initial avec maintenant un polynôme P''' de degré 2.

En identifiant les coefficients de X^2 dans l'équation $P''' = Q'''D + R$, on obtient l'équation $-\frac{15}{2} = 2d$. D'où $d = -\frac{15}{4}$.

On obtient aussi que

$$\begin{aligned} R &= P''' + \frac{15}{4}D \\ &= \left(-\frac{15}{2}X^2 + \frac{31}{2}X - 1\right) + \frac{15}{4}\left(2X^2 + X - 3\right) \\ &= \left(-\frac{15}{2} + \frac{15}{4}\cdot 2\right)X^2 + \left(\frac{31}{2} + \frac{15}{4}\right)X + \left(-1 - \frac{45}{4}\right) \\ &= \frac{77}{4}X - \frac{49}{4}. \end{aligned}$$

Exemple (fin)

Nous devons donc avoir

$$Q = 3X^3 - X^2 + \frac{9}{2}X - \frac{15}{4} \quad \text{et} \quad R = \frac{77}{4}X - \frac{49}{4}$$

et on peut vérifier qu'en effet $P = QD + R$ et que $\deg(R) < \deg(D)$.

Preuve du théorème

Soient $P, D \in \mathbb{K}[X]$ tels que $D \neq 0$.

Nous montrons d'abord l'existence de polynômes Q et R tels que

$$P = QD + R \quad \text{et} \quad \deg(R) < \deg(D)$$

par récurrence sur le degré de P.

Cas de base : Si $\deg(P) < \deg(D)$, alors il suffit de choisir $Q = 0$ et $R = P$.

Hypothèse de récurrence : Supposons maintenant que $\deg(P) \geq \deg(D)$ et que le résultat soit vérifié pour tout polynôme de degré strictement inférieur à celui de P.

Si p et d sont les coefficients dominants de P et D respectivement, alors le polynôme $P' = P - \frac{p}{d} X^{\deg(P)-\deg(D)} D$ a un degré strictement inférieur à celui de P.

Par hypothèse de récurrence, il existe des polynômes Q' et R' de $\mathbb{K}[X]$ tels que

$$P' = Q'D + R' \quad \text{et} \quad \deg(R') < \deg(D).$$

On obtient donc que

$$\begin{aligned} P &= P' + \frac{p}{d} X^{\deg(P)-\deg(D)} D \\ &= Q'D + R' + \frac{p}{d} X^{\deg(P)-\deg(D)} D \\ &= \left(Q' + \frac{p}{d} X^{\deg(P)-\deg(D)} \right) D + R'. \end{aligned}$$

D'où $Q = Q' + \frac{p}{d} X^{\deg(P)-\deg(D)}$ et $R = R'$ conviennent.

Montrons à présent l'unicité des polynômes Q et R.

Supposons qu'il existe des polynômes $Q_1, R_1, Q_2, R_2 \in \mathbb{K}[X]$ tels que

$$P = Q_1 D + R_1 = Q_2 D + R_2,\ \deg(R_1) < \deg(D),\ \deg(R_2) < \deg(D).$$

Alors on doit avoir $(Q_1 - Q_2)D = R_2 - R_1$.

Si $Q_1 \neq Q_2$, alors

$$\deg((Q_1 - Q_2)D) = \deg(Q_1 - Q_2) + \deg(D) \geq \deg(D).$$

C'est impossible puisque

$$\deg(R_2 - R_1) \leq \max\{\deg(R_1), \deg(R_2)\} < \deg(D).$$

D'où $Q_1 = Q_2$ et par conséquent $R_1 = R_2$ aussi.

Exemple (suite)

La preuve précédente (plus précisément, la partie “existence”) nous procure en fait un algorithme pour obtenir Q et R.

On peut organiser les calculs effectués dans un tableau de division à la manière de la division des entiers classiques :

$$
\begin{array}{rrrrrr|l}
6X^5 & +X^4 & -X^3 & & +2X & -1 & 2X^2+X-3 \\
\cline{7-7}
-6X^5 & -3X^4 & +9X^3 & & & & 3X^3-X^2+\frac{9}{2}X-\frac{15}{4} \\
\cline{1-3}
 & -2X^4 & +8X^3 & & +2X & -1 & \\
 & +2X^4 & +X^3 & -3X^2 & & & \\
\cline{2-4}
 & & 9X^3 & -3X^2 & +2X & -1 & \\
 & & -9X^3 & -\frac{9}{2}X^2 & +\frac{27}{2}X & & \\
\cline{3-5}
 & & & -\frac{15}{2}X^2 & +\frac{31}{2}X & -1 & \\
 & & & +\frac{15}{2}X^2 & +\frac{15}{4}X & -\frac{45}{4} & \\
\cline{4-6}
 & & & & \frac{77}{4}X & -\frac{49}{4} &
\end{array}
$$

Autres exemples

Effectuons la division euclidienne de $P = X^5 + iX^3 + (1+i)X - 1$ par $D = 2X^3 - 2X^2 + 1$ dans $\mathbb{C}[X]$:

$$
\begin{array}{rrrrrr|l}
X^5 & & +iX^3 & & +(1+i)X & -1 & 2X^3 - 2X^2 + 1 \\
\cline{7-7}
-X^5 & +X^4 & & -\frac{1}{2}X^2 & & & \frac{1}{2}X^2 + \frac{1}{2}X + \frac{1+i}{2} \\
\cline{1-5}
 & X^4 & +iX^3 & -\frac{1}{2}X^2 & +(1+i)X & -1 & \\
 & -X^4 & +X^3 & & -\frac{1}{2}X & & \\
\cline{2-5}
 & & (1+i)X^3 & -\frac{1}{2}X^2 & +(\frac{1}{2}+i)X & -1 & \\
 & & -(1+i)X^3 & +(1+i)X^2 & & -\frac{1+i}{2} & \\
\cline{3-6}
 & & & (\frac{1}{2}+i)X^2 & +(\frac{1}{2}+i)X & -\frac{3+i}{2} &
\end{array}
$$

On obtient $Q = \frac{1}{2}X^2 + \frac{1}{2}X + \frac{1+i}{2}$ et $R = (\frac{1}{2}+i)X^2 + (\frac{1}{2}+i)X - \frac{3+i}{2}$.

Effectuons maintenant la division euclidienne de $P = X^4 + X^3 + 2X + 1$ par $D = 2X^3 + X^2 + 1$ dans $\mathbb{Z}_3[X]$:

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

On obtient $Q = 2X + 1$ et $R = 2X^2$.

En effet, dans $\mathbb{Z}_3[X]$, on a bien

$$\begin{aligned}
QD + R &= (2X + 1)(2X^3 + X^2 + 1) + 2X^2 \\
&= X^4 + 2X^3 + 2X + 2X^3 + X^2 + 1 + 2X^2 \\
&= X^4 + X^3 + 2X + 1 \\
&= P.
\end{aligned}$$

Un autre algorithme pour trouver Q et R dans le cas où $\deg(P) \geq \deg(D)$ est de remarquer que $\deg(Q) = \deg(P) - \deg(D)$.

Dans notre exemple, on cherche donc des polynômes Q et R de $\mathbb{Z}_3[X]$ de la forme $Q = aX + b$ et $R = cX^2 + dX + e$.

En identifiant les coefficients des polynômes dans les deux membres de l'équation $P = QD + R$, c'est-à-dire l'équation

$$X^4 + X^3 + 2X + 1 = (aX + b)(2X^3 + X^2 + 1) + cX^2 + dX + e$$

on obtient le système d'équations

$$\begin{cases} 1 = 2a \\ 1 = a + 2b \\ 0 = b + c \\ 2 = a + d \\ 1 = b + e. \end{cases}$$

En résolvant ce système dans $\mathbb{Z}_3$ (par la méthode de Gauss par exemple), on obtient l'unique solution $(a, b, c, d, e) = (2, 1, 2, 0, 0)$, c'est-à-dire $Q = 2X + 1$ et $R = 2X^2$.

Définition

Soient $P, D \in \mathbb{K}[X]$ avec $D \neq 0$. Les polynômes (uniques) Q, R donnés dans l'énoncé du théorème précédent sont appelés respectivement le quotient et le reste de la division euclidienne de P par D.

Définition

Dans $\mathbb{K}[X]$, on dit qu'un polynôme D divise un polynôme P lorsque le reste R de la division euclidienne de P par D vaut 0.

Autrement dit, D divise P s'il existe un polynôme Q (nécessairement unique au vu du théorème précédent) tel que $P = QD$.

Pour continuer notre analogie entre l'ensemble des polynômes $\mathbb{K}[X]$ et l'ensemble des entiers $\mathbb{Z}$, nous donnons ici la définition du PGCD de deux polynômes.

Définition

Un PGCD de deux polynômes P et Q de $\mathbb{K}[X]$ est un polynôme D qui divise P et Q et qui est tel que tout polynôme divisant simultanément P et Q divise aussi D.

Remarquons que la notion de PGCD de polynômes n'est définie qu'à une constante multiplicative non nulle près : si D est un PGCD de P et Q, alors pour tout $k \in \mathbb{K} \setminus \{0\}$, le polynôme kD est aussi un PGCD de P et Q.

Parmi tous les PGCD, on privilégie parfois celui ayant 1 comme coefficient dominant : on parle alors du PGCD de deux polynômes.

Algorithme d'Euclide

Maintenant que nous disposons de la division euclidienne dans $\mathbb{K}[X]$, l'algorithme d'Euclide pour la recherche du PGCD de deux polynômes s'effectue de façon similaire à celui pour obtenir le PGCD de deux entiers.

Exemple

Plaçons-nous dans $\mathbb{Z}_3[X]$ et calculons le PGCD de $P = X^5 + 2X$ et de $Q = X^4 + 2X^3 + 2X$.

Comme $\deg(Q) < \deg(P)$, on pose $R_0 = Q$ et on obtient successivement

$$\begin{aligned} P &= (X+1)R_0 + X^3 + X^2, & R_1 &= X^3 + X^2, \\ R_0 &= (X+1)R_1 + 2X^2 + 2X, & R_2 &= 2X^2 + 2X, \\ R_1 &= (2X)R_2, & R_3 &= 0. \end{aligned}$$

Le PGCD obtenu est le dernier reste non nul, c'est-à-dire $2X^2 + 2X$. Remarquons que le PGCD étant défini à une constante multiplicative près, le polynôme $2(2X^2 + 2X) = X^2 + X$ est aussi un PGCD de P et Q.

Bézout

En remontant l'algorithme d'Euclide, on obtient le théorème de Bézout pour les polynômes.

Théorème (Bézout)

Soient $P, Q \in \mathbb{K}[X]$ et $D \in \mathbb{K}[X]$ un PGCD de P et Q. Alors il existe $A, B \in \mathbb{K}[X]$ tels que $AP + BQ = D$.

Exemple (suite)

On calcule

$$\begin{aligned} 2X^2+2X &= R_0-(X+1)R_1 \\ &= Q-(X+1)(P-(X+1)Q) \\ &= -(X+1)P+(1+(X+1)^2)Q \\ &= (2X+2)P+(X^2+2X+2)Q. \end{aligned}$$

On a donc obtenu que les polynômes $A=2X+2$ et $B=X^2+2X+2$ vérifiaient l'égalité de Bézout $AP+BQ=D$ pour le PGCD $D=2X^2+2X$.

Pour obtenir des coefficients de Bézout pour le PGCD X^2+X, on multiplie cette égalité par 2 (inverse de 2 dans $\mathbb{Z}_3$) :

$$X^2+X=(X+1)P+(2X^2+X+1)Q.$$

Définition

Deux polynômes P et Q de $\mathbb{K}[X]$ sont premiers entre eux si 1 est un PGCD de P et Q.

Théorème (Gauss)

Si $P, Q, D \in \mathbb{K}[X]$ sont tels que D divise PQ et que D et P sont premiers entre eux, alors D divise Q.

Preuve

Soient $P, Q, D \in \mathbb{K}[X]$ tels que D divise PQ et que D et P sont premiers entre eux.

Alors d'une part, il existe $S \in \mathbb{K}[X]$ tel que $PQ = SD$ et d'autre part, par le théorème de Bézout, il existe $A, B \in \mathbb{K}[X]$ tels que $AD + BP = 1$.

On obtient que

$$Q = ADQ + BPQ = ADQ + BSD = (AQ + BS)D,$$

ce qui montre que D divise Q. □

Polynôme et fonction polynomiale

Définition

Pour $P \in \mathbb{K}[X]$ et $k \in \mathbb{K}$, la notation $P(k)$ désigne l'élément de $\mathbb{K}$ obtenu en substituant dans P l'indéterminée X par k et en exécutant les opérations $+$ et $\cdot$ dans $\mathbb{K}$: si

$$P = p_0 + p_1 X + p_2 X^2 + \cdots + p_d X^d,$$

alors

$$P(k) = p_0 + p_1 k + p_2 k^2 + \cdots + p_d k^d.$$

On dit qu'on a évalué P en k.

La fonction induite par P est la fonction

$$\mathbb{K} \to \mathbb{K},\ k \mapsto P(k).$$

Une fonction polynomiale de $\mathbb{K}$ est une fonction induite par un polynôme de $\mathbb{K}[X]$.

Deux polynômes différents peuvent donner lieu à une même fonction induite.

Par exemple, pour tout $k \in \mathbb{Z}_2$, on a $k^2 = k$. Les polynômes X^2 et X de $\mathbb{Z}_2[X]$ donnent donc lieu à la même fonction polynomiale induite.

Voici un autre exemple : les polynômes $X^3 + 2X$ et 0 de $\mathbb{Z}_3[X]$ donnent lieu à la même fonction polynomiale induite puisque pour tout $k \in \mathbb{Z}_3$, on a $k^3 + 2k = 0$.

Nous verrons plus loin, grâce au théorème fondamental de l'algèbre, que ceci n'est pas possible lorsque $\mathbb{K}$ est $\mathbb{C}, \mathbb{R}$ ou $\mathbb{Q}$.

Dérivation des polynômes

On définit ensuite la notion de dérivée (formelle) d'un polynôme.

Définition

L'opérateur de dérivation

$$\mathrm{D}\colon\ \mathbb{K}[X] \to \mathbb{K}[X]$$

est défini comme suit.

Pour tout polynôme

$$P = p_0 + p_1 X + p_2 X^2 + \cdots + p_d X^d$$

de $\mathbb{K}[X]$, le polynôme dérivé $\mathrm{D}\,P$ est le polynôme

$$\mathrm{D}\,P = p_1 + 2p_2 X + \cdots + d p_d X^{d-1}.$$

Autrement dit, pour tout $n \in \mathbb{N}$, le coefficient de X^n dans $\mathrm{D}\,P$ est égal à $(n+1)p_{n+1}$.

Proposition

L'opérateur de dérivation $\mathrm{D}\colon \mathbb{K}[X] \to \mathbb{K}[X]$ est linéaire : pour tous $k, \ell \in \mathbb{K}$ et tous $P, Q \in \mathbb{K}[X]$, on a $\mathrm{D}(kP + \ell Q) = k\,\mathrm{D}\,P + \ell\,\mathrm{D}\,Q$.

Preuve

C'est une simple vérification.

On utilise la notation $\mathrm{D}^i P$ pour signifier qu'on applique i fois l'opérateur D à P :

$$\mathrm{D}^0 P = P,\ \mathrm{D}^1 P = \mathrm{D} P,\ \mathrm{D}^2 P = \mathrm{D}(\mathrm{D} P),\ \mathrm{D}^3 P = \mathrm{D}(\mathrm{D}(\mathrm{D} P))),\ \ldots.$$

Proposition

Supposons que $\mathbb{K}$ est $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$. Alors pour tous $d, i \in \mathbb{N}$, on a

$$\mathrm{D}^i \left(\frac{1}{d!} X^d \right) = \begin{cases} \frac{1}{(d-i)!} X^{d-i} & \text{si } d \geq i, \\ 0 & \text{si } d < i. \end{cases}$$

Preuve

La preuve s'obtient par récurrence sur i.

Exemple

Pour $d = 7$ et $i = 3$, on calcule

$$\mathrm{D}^3\left(\frac{1}{7!}X^7\right) = \mathrm{D}^2\left(\frac{7}{7!}X^6\right) = \mathrm{D}\left(\frac{7\cdot 6}{7!}X^5\right) = \frac{7\cdot 6\cdot 5}{7!}X^4 = \frac{1}{4!}X^4$$

et on a bien $4 = 7 - 3 = d - i$.

Proposition (Binôme de Newton)

Pour tout $P, Q \in \mathbb{K}[X]$ et tout $n \in \mathbb{N}$, on a

$$(P+Q)^n = \sum_{i=0}^{n} \mathrm{C}_n^i \, P^i \, Q^{n-i}.$$

Preuve

Laissée en exercice. C'est une adaptation directe de la preuve du binôme de Newton pour les complexes que vous avez vue au bloc 1 dans le cours "Mathématique".

Proposition (Formule de Leibniz)

Pour tous $P, Q \in \mathbb{K}[X]$ et tout $n \in \mathbb{N}$, on a

$$\mathrm{D}^n(PQ) = \sum_{i=0}^{n} \mathrm{C}_n^i \, \mathrm{D}^i P \cdot \mathrm{D}^{n-i} Q.$$

Preuve

Laissée en exercice. C'est une adaptation directe de la preuve de la formule de Leibniz pour les fonctions d'une variable réelle que vous avez vue au bloc 1 dans le cours "Mathématique".

Proposition (Formule de Taylor)

Supposons que $\mathbb{K}$ est $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$. Alors pour tout $P \in \mathbb{K}[X]$ et tout $k \in \mathbb{K}$, on a

$$P = \sum_{i=0}^{\deg(P)} \frac{\mathrm{D}^i P(k)}{i!}(X-k)^i.$$

Preuve

Soit $P = \sum_{n=0}^{d} p_n X^n$ (où $d = \deg(P)$) et soit $k \in \mathbb{K}$.

En utilisant le binôme de Newton et en échangeant ensuite les sommes, on obtient

$$\begin{aligned} P &= \sum_{n=0}^{d} p_n (X-k+k)^n \\ &= \sum_{n=0}^{d} p_n \sum_{i=0}^{n} \mathrm{C}_n^i (X-k)^i k^{n-i} \\ &= \sum_{i=0}^{d} \left(\sum_{n=i}^{d} p_n \, \mathrm{C}_n^i \, k^{n-i} \right) (X-k)^i. \end{aligned}$$

Pour conclure, il suffit donc de montrer que

$$\sum_{n=i}^{d} p_n \, \mathrm{C}_n^i \, k^{n-i} = \frac{\mathrm{D}^i \, P(k)}{i!}.$$

Ceci est vrai puisque pour tout $i \in \{0, \ldots, d\}$,

$$\begin{aligned}
\frac{1}{i!} \mathrm{D}^i \, P &= \frac{1}{i!} \mathrm{D}^i \left(\sum_{n=0}^{d} p_n X^n \right) \\
&= \frac{1}{i!} \sum_{n=0}^{d} p_n \, \mathrm{D}^i \left(X^n \right) \\
&= \sum_{n=i}^{d} p_n \frac{n!}{i!(n-i)!} X^{n-i} \\
&= \sum_{n=i}^{d} p_n \, \mathrm{C}_n^i \, X^{n-i}.
\end{aligned}$$

Exemple

Soient $P = 2X^2 + 3X - 1$ dans $\mathbb{C}[X]$ et $k = 2$.

On a $\mathrm{D}\,P = 4X + 3$ et $\mathrm{D}^2\,P = 4$.

Ainsi $P(2) = 8 + 6 - 1 = 13$, $\mathrm{D}\,P(2) = 11$ et $\mathrm{D}^2\,P(2) = 4$.

On obtient

$$\begin{aligned}\sum_{i=0}^{2} \frac{\mathrm{D}^i\,P(2)}{i!}(X-2)^i &= \frac{\mathrm{D}^2\,P(2)}{2!}(X-2)^2 + \mathrm{D}\,P(2)(X-2) + P(2)\\ &= \frac{4}{2}(X^2 - 4X + 4) + 11(X-2) + 13\\ &= 2X^2 + 3X - 1\\ &= P.\end{aligned}$$

Zéros d'un polynôme

Définition

Soit $P \in \mathbb{K}[X]$. Un zéro de P est un nombre $k \in \mathbb{K}$ tel que le polynôme $X - k$ divise P.

Si P est non nul, la multiplicité d'un nombre k en tant que zéro du polynôme P est le plus grand entier α tel que $(X - k)^\alpha$ divise P.

Remarque

Avec cette définition, le fait que k soit un zéro de multiplicité 0 de P équivaut au fait que k ne soit pas un zéro de P.

On pourrait étendre la définition de la multiplicité aux polynômes nuls en disant qu'elle vaut $+\infty$ pour tout $k \in \mathbb{K}$.

Exemple

Considérons le polynôme $P = X^3 - 2X^2 - 2X - 3$ de $\mathbb{Q}[X]$.

Il admet 3 comme zéro simple, c'est-à-dire de multiplicité 1.

En effet, $X - 3$ divise P mais $(X - 3)^2$ ne divise pas P. On a $P = (X^2 + X + 1)(X - 3)$.

En effectuant la division euclidienne de P par $(X - 3)^2$, on obtient $P = (X + 4)(X - 3)^2 + 13X - 39$.

La condition pour être un zéro d'un polynôme donnée par cette définition est équivalente à l'annulation de sa fonction polynomiale induite.

Proposition

Soient $P \in \mathbb{K}[X]$ et $k \in \mathbb{K}$. Le nombre k est un zéro de P si et seulement si $P(k) = 0$.

Preuve

Effectuons la division euclidienne de P par $X - k$:

$$P = Q(X - k) + R, \text{ avec } Q, R \in \mathbb{K}[X] \text{ et } \deg(R) < 1.$$

Nécessairement, R est un polynôme constant $c \in \mathbb{K}$.

En évaluant les deux membres de cette égalité en k, on obtient $P(k) = c$.

Mais par définition, k est un zéro de P si et seulement si $R = 0$. D'où la conclusion. □

Lien entre la multiplicité et les dérivées

Théorème

Supposons que $\mathbb{K}$ est égal à $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

Soient $P \in \mathbb{K}[X]$ non nul, $k \in \mathbb{K}$ et $\alpha \in \mathbb{N}$.

Le nombre k est un zéro de multiplicité α de P si et seulement si $P(k) = 0,\ \mathrm{D}\,P(k) = 0,\ \ldots,\ \mathrm{D}^{\alpha-1}\,P(k) = 0$ et $\mathrm{D}^{\alpha}\,P(k) \neq 0$.

Exemple

Considérons le polynôme $P = X^3 - 2X^2 - 2X - 3$ de $\mathbb{Q}[X]$.

Nous avons vu qu'il admet 3 comme zéro simple.

On a bien que

$$P(3) = 3^3 - 2 \cdot 3^2 - 2 \cdot 3 - 3 = 27 - 18 - 6 - 3 = 0.$$

On calcule $\mathrm{D}\,P = 3X^2 - 4X - 2$ et on a bien aussi que

$$\mathrm{D}\,P(3) = 3 \cdot 3^2 - 4 \cdot 3 - 2 = 27 - 12 - 2 = 13 \neq 0.$$

Polynômes à coefficients complexes et théorème fondamental de l'algèbre

Théorème fondamental de l'algèbre

Tout polynôme de $\mathbb{C}[X]$ non constant de degré d possède exactement d zéros (complexes) lorsque ceux-ci sont comptés avec leurs multiplicités.

Ainsi, si $k_1, \ldots, k_m$ sont les zéros de P de multiplicités $\alpha_1, \ldots, \alpha_m$ respectivement, alors

$$\alpha_1 + \cdots + \alpha_m = d$$

et

$$P = p(X - k_1)^{\alpha_1} \cdots (X - k_m)^{\alpha_m},$$

où p est le coefficient dominant de P.

Corollaire

Supposons que $\mathbb{K}$ est $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

1. Deux polynômes de $\mathbb{K}[X]$ ayant les mêmes zéros complexes avec les mêmes multiplicités sont égaux à une constante non nulle multiplicative près.
2. Deux polynômes de $\mathbb{K}[X]$ de même degré d prenant les mêmes valeurs en $d+1$ arguments sont égaux.
3. Deux polynômes de $\mathbb{K}[X]$ sont égaux si et seulement si leurs fonctions polynomiales induites (de $\mathbb{K}$ dans $\mathbb{K}$) sont égales.

Preuve

1. Deux polynômes de $\mathbb{K}[X]$ ayant les mêmes zéros complexes avec les mêmes multiplicités sont égaux à une constante non nulle multiplicative près.

S'il s'agit de deux polynômes constants, alors nécessairement ils sont soit tous les deux nuls soit tous les deux non nuls. La propriété est évidente dans ce cas.

Si l'un des deux est constant et l'autre non, il ne peuvent avoir les mêmes zéros complexes par le théorème fondamental de l'algèbre (et il n'y a rien à montrer).

Enfin, si les deux polynômes sont non-constants, cela découle de la factorisation donnée par le théorème fondamental de l'algèbre.

2. Deux polynômes de $\mathbb{K}[X]$ de même degré d prenant les mêmes valeurs en $d+1$ arguments sont égaux.

Si $P, Q \in \mathbb{K}[X]$ sont de même degré d et sont égaux en $d+1$ valeurs, alors le polynôme $P-Q$ est de degré au plus d et s'annule en $d+1$ valeurs.

Ainsi, $P-Q$ possède $d+1$ zéros.

Puisque $\mathbb{K} \subseteq \mathbb{C}$, on obtient par le théorème fondamental de l'algèbre que $P-Q$ est un polynôme constant.

Le seul polynôme constant qui possède au moins un zéro étant le polynôme nul, on obtient $P = Q$.

3. Deux polynômes de $\mathbb{K}[X]$ sont égaux si et seulement si leurs fonctions polynomiales induites (de $\mathbb{K}$ dans $\mathbb{K}$) sont égales.

Clairement, si deux polynômes sont égaux, alors ils prennent la même valeur en tout élément de $\mathbb{K}$.

Montrons la réciproque. Soient $P, Q \in \mathbb{K}[X]$ des polynômes tels que leurs fonctions polynomiales induites sont égales.

Alors $P - Q$ possède une infinité de zéros (en fait la fonction induite par $P - Q$ est la fonction nulle).

Comme dans le point précédent, le théorème fondamental de l'algèbre impose $P = Q$.

□

Équivalence des notions de polynômes formels et de fonction polynomiales dans les cas où $\mathbb{K}$ est $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

Le troisième point du corollaire précédent montre l'équivalence des notions de polynômes et de fonction polynomiales dans les cas où $\mathbb{K}$ est $\mathbb{C}$, $\mathbb{R}$ ou $\mathbb{Q}$.

Cela permet d'utiliser la méthode d'identification des coefficients pour la résolutions d'équations polynomiales.

Remarque

Le théorème fondamental de l'algèbre ne fournit pas d'algorithme pour trouver les zéros d'un polynôme !

Cependant, il existe des méthodes pour obtenir les zéros d'un polynôme de degré au plus 4.

Pour un polynôme de degré supérieur à 5, aucune méthode n'existe !

Néanmoins, plusieurs méthodes relevant de l'analyse numérique permettent de fournir des approximations aussi fines que souhaitées des zéros d'un polynôme d'un degré quelconque.

C'est l'un des objets du cours "Introduction à l'algorithmique numérique".

Polynômes à coefficients réels

Lemme 1

Soit $P \in \mathbb{R}[X]$. Si $c \in \mathbb{C}$ est un zéro de P, alors son conjugué $\bar{c}$ est aussi un zéro de P.

Preuve

Notons $P = p_0 + p_1 X + \cdots + p_d X^d$.

Soit $c \in \mathbb{C}$ un zéro de P.

Alors

$$P(c) = p_0 + p_1 c + \cdots + p_d c^d = 0.$$

Puisque les coefficients de P sont réels, on obtient

$$P(\bar{c}) = p_0 + p_1 \bar{c} + \cdots + p_d \bar{c}^d = \overline{P(c)} = \bar{0} = 0.$$

Ceci montre que $\bar{c}$ est un zéro de P.

Lemme 2

Pour tout $c \in \mathbb{C}$, on a $(X - c)(X - \bar{c}) \in \mathbb{R}[X]$.

Preuve

Soit $c \in \mathbb{C}$. On a $c = a + ib$ avec $a, b \in \mathbb{R}$. En distribuant le produit, on obtient que

$$(X - c)(X - \bar{c}) = X^2 - (c + \bar{c})X + c\bar{c} = X - 2aX + (a^2 + b^2) \in \mathbb{R}[X].$$

□

Exemple

Soit $c = 3 + i$. On a

$$\begin{aligned}(X - c)(X - \bar{c}) &= (X - 3 - i)(X - 3 + i) \\ &= X^2 - (3 - i + 3 + i)X + (3 + i)(3 - i) \\ &= X^2 - 6X + 10.\end{aligned}$$

On a bien $c + \bar{c} = 3 + i + 3 - i = 6$ et $c\bar{c} = (3 + i)(3 - i) = 10$.

Proposition

Tout polynôme P de $\mathbb{R}[X]$ se factorise dans $\mathbb{R}[X]$ sous la forme

$$P = p(X - r_1) \cdots (X - r_m) Q_1 \cdots Q_n,$$

où p est le coefficient dominant de P, $r_1, \ldots, r_m$ sont les zéros réels de P et $Q_1, \ldots, Q_n \in \mathbb{R}[X]$ sont des polynômes du second degré avec un réalisant $\Delta < 0$.

Preuve

Soit $P \in \mathbb{R}[X]$. Par le lemme 1, les zéros de P sont de la forme

$$r_1, \ldots, r_k, c_1, \ldots, c_\ell, \overline{c}_1, \ldots, \overline{c_\ell},$$

avec $r_1, \ldots, r_k \in \mathbb{R}$ et $c_1, \ldots, c_\ell \in \mathbb{C} \setminus \mathbb{R}$.

Par le théorème fondamental de l'algèbre, on obtient

$$\begin{aligned} P &= p(X - r_1) \cdots (X - r_k)(X - c_1)(X - \overline{c}_1) \cdots (X - c_\ell)(X - \overline{c}_\ell) \\ &= p(X - r_1) \cdots (X - r_k) Q_1 \cdots Q_\ell, \end{aligned}$$

où p est le coefficient dominant de P et où on a posé $Q_i = (X - c_i)(X - \overline{c_i})$ pour tout $i \in \{1, \ldots, \ell\}$.

Par le lemme 2, nous savons que les polynômes Q_i sont à coefficients réels.

De plus, ces polynômes ont un réalisant $\Delta < 0$ puisqu'ils ne possèdent pas de zéro réel. □