POFM 2020 — 21 - Cours par correspondance : Polynomes

Groupe C

Yaël Dillies

6 décembre 2020

La phrase du jour

Les polynomes sont nos amis.

Je ne sais qui

Sommaire

Définition formelle

Un *polynome* est une suite $(a_0, a_1, a_2, \ldots)$ telle que seulement un nombre fini de a_n est non nul.

Définition formelle

Un *polynome* est une suite $(a_0, a_1, a_2, \dots)$ telle que seulement un nombre fini de a_n est non nul.

$(1, 3, 0, 0, \dots)$ est un polynome

$(1, 1, \dots)$ **n'**est **pas** un polynome

Définition formelle

Un *polynome* est une suite $(a_0, a_1, a_2, \dots)$ telle que seulement un nombre fini de a_n est non nul.

$$(1, 3, 0, 0, \dots) \text{ est un polynome}$$

$$(1, 1, \dots) \textbf{ n'}\text{est } \textbf{pas} \text{ un polynome}$$

Cette définition est **AUSTÈRE**. Que fait vraiment un polynome ?

Définition compréhensible

Un polynome P est une expression de la forme

$$P = a_n X^n + a_{n-1} X^{n-1} + \dots a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$$

Définition compréhensible

Un polynome P est une expression de la forme

$$P = a_n X^n + a_{n-1} X^{n-1} + \dots a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i$$

Pour le moment, on suppose que les a_i sont réels, mais un polynome peut être défini de façon beaucoup plus générale.

Définition compréhensible

Un polynome P est une expression de la forme

$$P = a_nX^n + a_{n-1}X^{n-1} + \dots a_1X + a_0 = \sum_{i=0}^{n} a_iX^i$$

Pour le moment, on suppose que les a_i sont réels, mais un polynome peut être défini de façon beaucoup plus générale. Le plus grand k tel que $a_k \neq 0$ est appelé le *degré* de P et on l'écrit $\deg P$. Exemples :

$$\deg(X^2 + X) = 2, \deg(3) = 0$$

Et $P = 0$? On a par convention $\deg 0 = -\infty$.

Que fait un polynome ?

Que peut-on faire d'un polynome ?

Que fait un polynome ?

Que peut-on faire d'un polynome ?

- On peut l'**évaluer** :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

où x est un réel. *Dans la définition, X est une variable, un symbole.*

Que fait un polynome ?

Que peut-on faire d'un polynome ?

- On peut l'**évaluer** :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  où x est un réel. *Dans la définition, X est une variable, un symbole.*

- On peut les additionner. Si $P = \sum_{i=0}^{n} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$, alors

$$P+Q = (p_n+q_n)x^n + \dots (p_1+q_1)x + (p_0+q_0) = \sum_{i=0}^{n} (p_i+q_i) X^i$$

Que fait un polynome ?

Que peut-on faire d'un polynome ?

- On peut l'**évaluer** :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

où x est un réel. *Dans la définition, X est une variable, un symbole.*

- On peut les additionner. Si $P = \sum_{i=0}^{n} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$, alors

$$P+Q = (p_n+q_n)x^n + \dots (p_1+q_1)x + (p_0+q_0) = \sum_{i=0}^{n} (p_i+q_i) X^i$$

- On peut les multiplier. Si $P = \sum_{i=0}^{n} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$, alors

$$PQ = (p_n+q_n)x^n + \dots (p_1+q_1)x + (p_0+q_0) = \sum (p_i+q_i) X^i$$

Que fait un polynome ?

Que peut-on faire d'un polynome ?

- On peut l'**évaluer** :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  où x est un réel. *Dans la définition, X est une variable, un symbole.*

- On peut les additionner. Si $P = \sum_{i=0}^{n} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$, alors

$$P+Q = (p_n+q_n)x^n + \dots (p_1+q_1)x + (p_0+q_0) = \sum_{i=0}^{n} (p_i+q_i) X^i$$

- On peut les multiplier. Si $P = \sum_{i=0}^{n} p_i X^i$ et $Q = \sum_{i=0}^{n} q_i X^i$, alors

$$PQ = (p_n+q_n)x^n + \dots (p_1+q_1)x + (p_0+q_0) = \sum_{i=0}^{n} (p_i+q_i) X^i$$

Exercices

Évaluer $P(1)$ et $P(-2)$ lorsque

- $P = X - 3$
- $P = 4$
- $P = X^2 + 5X + 13$

Calculer

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

Plus d'exercices

Calculer

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

Plus d'exercices

Calculer

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

On remarque que

$$\deg(PQ) = \deg P + \deg Q$$

et que

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

avec égalité si $\deg P \neq \deg Q$.

Définition d'une racine

Un réel r tel que $P(r) = 0$ est appelé *racine* de P.

Lemme

Si r est une racine de P, alors il existe un polynome Q tel que

$$P = (X - r)Q$$

Preuve

On peut écrire

$$P = (X - r)Q + R$$

avec $\deg R < \deg(X - r) = 1$. Donc R est constant et en évaluant en r on obtient

$$0 = P(r) = (r - r)Q(r) + R(r) = R(r)$$

Donc $R = 0$.

Exercices

Déterminer

- $\frac{X^2+2X+1}{X+1}$
- $\frac{X^3+5X-42}{X-3}$

Conseils pour trouver les racines

Si $\frac{p}{q}$ est racine de $P = a_n X^n + a_{n-1} X^{n-1} + \ldots a_1 X + a_0$, alors $p \mid a_0$ et $q \mid a_n$, donc on a peu de cas à tester.
Si $a_n = a_0, a_{n-1} = a_1, \ldots,$ alors r est racine de P ssi $\frac{1}{r}$ l'est

Polynomes en plusieurs variables

On peut avoir des polynomes en deux ou plus de variables. Par exemple,

$$P = X^2Y + XY + Y^2 + 2$$

Un polynome est *symétrique* si on peut échanger ses variables n'importe comment sans changer le polynome.

$$X^2Y + XY + Y^2 + 2 \text{ n'est pas symétrique}$$

$$X^2 + XY + Y^2 + 2 \text{ est symétrique}$$

Relations de Viète

On peut écrire un polynome $P = x^n + \cdots + a_1 x + a_0$ comme

$$P = (x - r_1) \dots (x - r_n)$$

où $r_1, \dots, r_n$ sont les racines de P (comptées avec multiplicité). En développant, on trouve

$$-a_{n-1} = r_1 + \cdots + r_n, a_{n-2} = r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n, (-1)^n a_0 = r_1 \dots$$

On appelle ces expressions les *polynomes symétriques élémentaires*.

Caractérisation des polynomes symétriques

Tout polynome symétrique est une combinaison linéaire de polynomes symétriques élémentaires.

Relations de Newton

Écrire sous forme de combinaison linéaire de polynomes symétriques élémentaires

- $x^2 + y^2 + z^2$
- $x^3 + y^3 + z^3$

Trouver rapidement les racines rationnelles d'un polynome à coefficients entiers

Essayons de trouver les racines de $P = X^3 + 2X - 3$.
Supposons que $P\left(\frac{p}{q}\right) = 0$ et que p, q premiers entre eux. On a $p^3 + 2pq^2 - 3q^3 = q^3 P\left(\frac{p}{q}\right) = 0$, donc $p \mid 3q^3$ et $q \mid p^3$. Donc $p = \pm 1, \pm 3$ et $q = \pm 1$ (si $c \mid ab$ et c est premier avec b, alors $c \mid a$).
Il suffit donc de tester $x = \pm 1, \pm 3$.

Polynomes à coefficients "symétriques"

Supposons que $a_n = a_0, a_{n-1} = a_1$. Si $x \neq 0$, alors $P\left(\frac{1}{x}\right) = a_n x^{-n} + \cdots + a_1 x^{-1} + a_0 = \frac{a_n + \cdots + a_1 x^{n-1} + a_0 x^n}{x^n} = \frac{a_0 + \cdots + a_{n-1} x^{n-1} + a_n x^n}{x^n} = \frac{P(x)}{x^n}$. Donc les racines de P vont par paire de la forme $x, \frac{1}{x}$ (et $P(0) = a_0 = a_n \neq 0$ donc 0 n'est pas une racine) sauf éventuellement 1 et -1.
On peut utiliser cette remarque en posant $z = x + \frac{1}{x}$ et en remarquant que $Px^{-\frac{n}{2}}$ est un polynome de degré $\left\lceil \frac{n}{2} \right\rceil$ en z.

Un polynome de degré n a au plus n racines

Faisons-le par récurrence sur n :

- **Initialisation :** Clair pour degré 0.
- **Hérédité :** Si r est une racine de P, alors on peut écrire $P = (X - r)Q$. On a $\deg Q = \deg P - \deg(X - r) = n - 1$. Or $P(x) = 0 \iff x - r = 0$ ou $Q(x) = 0$. Donc les racines de P sont r (une racine) et les racines de Q (au plus $n - 1$ racines). Donc P a au plus n racines.

Attention : Ne marche pas modulo un composé. Par exemple, $X^2 - 1$ admet $1, 3, 5, 7$ comme racines modulo 8.

Racines multiples

Il peut s'avérer que $P = (X-r)^m Q$ avec $m > 1$ et Q un polynome. Le plus grand m tel que c'est vrai est la *multiplicité* de r.
On voit alors que
$P' = (X-r)^m Q' + m(X-r)^{m-1}Q = (X-r)^{m-1}R$. Donc la multiplicité de r dans P' est (au moins, mais en fait exactement) $m-1$ et donc par récurrence
$P(r) = P'(r) = \cdots = P^{(m-1)}(r) = 0$. Et on a fait aussi
$P^{(m)}(r) \neq 0$.

Racines multiples

Exemple : Trouver les racines doubles de $P = X^3 + 8X^2 + 21X + 18$. Solution : Calculer le pgcd de P et $P' = 3X^2 + 16X + 21$ à coup d'Euler :

$$\begin{aligned} 3P - XP' &= 2 \cdot (4X^2 + 21X + 27) \\ 4P' - 3 \cdot (4X^2 + 21X + 27) &= X + 3 \\ (4X^2 + 21X + 27) - (4X + 9)(X + 3) &= 0 \end{aligned}$$

On trouve $X + 3$, donc la seule racine double éventuelle est -3

Exemple d'utilisation

Exercice

Soient P et Q deux polynomes tels que P a les mêmes racines que Q (mais pas forcément même multiplicité) et $P-1$ les mêmes racines que $Q-1$ (mais pas forcément même multiplicité). Montrer que $P=Q$.

Indice : La dérivée d'un polynome de degré n est un polynome de degré $n-1$.

Exemple d'utilisation

Solution

Si on regarde $P - Q = (P-1) - (Q-1)$, on voit qu'il a toutes les racines de P et toutes les racines de $P-1$. Or ces racines sont distinctes puisque $P(r) = 0 \implies P(r) - 1 \neq 0$.

Si on note a, b le nombre de racines distinctes de P et de $P-1$ respectivement, alors on voit que $P - Q$ a au moins $a + b$ racines. On veut donc montrer

$a + b > \max(\deg P, \deg Q) \geq \deg(P - Q)$ (on suppose par symétrie que $n = \deg P > \deg Q$).

Exemple d'utilisation

Solution

L'idée est maintenant de regarder $D_0 = \gcd(P, P')$ et $D_1 = \gcd(P - 1, P')$. $\deg D_0 = n - a$ et $\deg D_1 = n - b$. Or D_0, D_1 sont premiers entre eux et divisent tous deux P'. Du coup, $D_0 D_1 \mid P'$ et $\deg D_0 + \deg D_1 \leq \deg P' = n - 1$. En mettant tout bout à bout,
$a + b = 2n - \deg D_0 - \deg D_1 \geq n + 1 > n$.
Autrement dit, P et $P - 1$ ont en tout $2n$ racines comptées avec multiplicité et P' n'en annule par multiplicité qu'au plus $n - 1$ et il en reste donc au moins $n + 1$ distinctes.

Interpolation de Lagrange

Formule d'interpolation de Lagrange

Si $x_1, \ldots, x_n$ sont des réels distincts et $y_1, \ldots, y_n$ des réels arbitraires, alors il existe un unique polynome P de degré inférieur à $n-1$ tel que $P(x_i) = y_i$ pour tout $i \in [\![1, n]\!]$.

Essence de la preuve

L'idée est de remarquer que $\prod_{j \neq i} \frac{X - x_j}{x_i - x_j}$ vaut 1 en x_i et 0 en x_j pour tout $j \neq i$.
Pour l'unicité, si P et Q respectent tous deux les conditions, alors $P - Q$ a comme racines $x_1, \ldots, x_n$ et est de degré au plus $n-1$. Donc $P - Q = 0$ et $P = Q$.

Expansion de Taylor

Expansion de Taylor

$$P(a+x) = P(a) + xP'(a) + \frac{x^2}{2}P''(a) + \cdots = \sum_{k=0}^{n+1} \frac{x^k}{k!}P^{(k)}(a)$$

Essence de la preuve

On peut écrire $P(a+x) = \sum_{k=0}^{n+1} \frac{c_k}{k!}x^k$. En dérivant k fois les deux côtés et en évaluant en a, on trouve $c_k = P^{(k)}(a)$.

Réduire le modulo

Un polynome modulo ab est entièrement caractérisé par un polynome modulo a et un polynome modulo b si a, b sont premiers entre eux. Cela permet de transférer toutes les questions sur les polynomes modulo n à des questions modulo p^α pour p premier. Ensuite, le lemme de Hensel permet de faire un pont entre modulo p et modulo p^α sous certaines conditions.

Hensel

Lemme de Hensel

Si r est une racine simple de P modulo un premier p, alors il existe un unique r' modulo p^α racine de P et tel que $r' \equiv r \mod p$.

Exemple

$X^2 + 1$ a deux racines modulo 5 : $2, 3$ et les deux sont simples. Donc il en a aussi deux modulo 25 : $7 \equiv 2 \mod 5$ et $18 \equiv 3 \mod 5$.

Hensel

Essence de la preuve

Par récurrence sur α. Supposons que r est unique modulo p^α. Alors $P(r+kp^\alpha) = P(r) + kp^\alpha P'(r) + k^2p^{2\alpha}P''(r)/2 + \cdots \equiv P(r) + kp^\alpha P'(r)[p^{\alpha+1}]$ car $2\alpha \geq \alpha + 1$.
Donc $p^{\alpha+1} \mid P(r+kp^\alpha) \iff k \equiv -\frac{P(r)}{p^\alpha P'(r)} \mod p$, ce qui donne une unique solution.

Suites récurrentes linéaires

On sait résoudre les suites récurrentes linéaires, mais que se passe-t-il si au lieu de

$$a_k x_{n+k} + \cdots + a_0 x_0 = 0$$

on a

$$a_k x_{n+k} + \cdots + a_0 x_0 = P(n)$$

avec P un polynome ? Eh bien on peut tuer le polynome en remarquant que $P(n+1) - P(n)$ est un polynome de degré plus petit que P. Concrètement,

$$a_k x_{n+k+1} + (a_{k-1} - a_k) x_{n+k} + \cdots + (a_0 - a_1) x_1 - a_0 x_0 = Q(n)$$

où $\deg Q < \deg P$. En répétant l'opération, on se sera effectivement débarrassé du polynome à droite. Ainsi, x_n est une suite récurrente linéaire de polynome caractéristique $(a_k X^k + \cdots + a_0)(X-1)^{\deg P + 1}$.