Polynômes

Thomas Huber

Actualisé: 30 avril 2018
vers. 1.1.0

Table des matières

1 Notions de base

Un *polynôme* p en une *variable* x est de la forme

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Les a_i sont appelés les *coefficients* de p et peuvent être des nombres entiers, rationnels, réels ou complexes. Si $a_n \neq 0$ alors a_n est appelé le *coefficient dominant*. Si $a_n = 1$ alors p est appelé *unitaire*. Les polynômes de la forme $p(x) = c$ sont appelés *constants*, $p(x) = 0$ est aussi appelé le *polynôme nul*. On peut aussi considérer des polynômes en plusieurs variables : un exemple en trois variables est

$$x^3 + y^3 + z^3 - 3xyz.$$

Soient maintenant $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ et $q(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_0$ deux polynômes. La *somme* (différence) de p et q est obtenue en additionnant (soustrayant) les coefficients correspondants :

$$p(x) \pm q(x) = (a_n \pm b_n) x^n + (a_{n-1} \pm b_{n-1}) x^{n-1} + \ldots + (a_0 \pm b_0).$$

Si c est une constante, alors on peut multiplier p par c :

$$c \cdot p(x) = (c \cdot a_n) x^n + (c \cdot a_{n-1}) x^{n-1} + \ldots + (c \cdot a_0).$$

Plus généralement on peut multiplier des polynômes arbitraires en distribuant les termes, puis en les regroupant selon les puissances de x :

$$p(x) \cdot q(x) = (a_n b_n) x^{2n} + (a_n b_{n-1} + a_{n-1} b_n) x^{2n-1} + \ldots + \left(\sum_{i=0}^{k} a_{k-i} b_i \right) x^k + \ldots + (a_0 b_0).$$

Par exemple on a

$$\begin{aligned} (x^3 - 2x^2 + 5)(2x^2 - 3) &= 2x^5 - 3x^3 - 4x^4 + 6x^2 + 10x^2 - 15 \\ &= 2x^5 - 4x^4 - 3x^3 + 16x^2 - 15. \end{aligned}$$

Le plus grand nombre k tel que $a_k \neq 0$ est appelé le *degré* de p et est noté $\deg(p)$. On définit de plus le degré du polynôme nul comme $\deg(0) = -\infty$. Ainsi on a toujours les formules

$$\begin{aligned} \deg(p \pm q) &\leq \max\{\deg(p), \deg(q)\}, \\ \deg(p \cdot q) &= \deg(p) + \deg(q). \end{aligned}$$

1.1 Coefficients

Exemple 1 (Bélarus 94)**.** *Trouver toutes les paires (P, Q) de polynômes réels unitaires tels que*

$$P(Q(x)) = x^{1994}.$$

Démonstration. On utilise le résultat général suivant. Si $P(x) = a_m x^m + \ldots + a_r x^r$ et $Q(x) = b_n x^n + \ldots + b_s x^s$ sont deux polynômes avec $a_m \neq 0, a_r \neq 0$ et $b_n \neq 0$, $b_s \neq 0$ (les cas $m = r$ et $n = s$ sont possibles), alors $P(Q(x))$ est de la forme

$$P(Q(x)) = c_{mn} x^{mn} + \ldots + c_{rs} x^{rs}$$

avec $c_{mn} \neq 0$ et $c_{rs} \neq 0$. On peut voir ceci directement en utilisant la formule pour $P(Q(x))$. Celle-ci donne plus exactement $c_{mn} = a_m b_n^m$ et $c_{rs} = a_r b_s^r$.

Dans notre cas on veut avoir $P(Q(x)) = x^{1994}$. Ceci ne peut être le cas que si $P(x) = x^m$ et $Q(x) = x^n$ sont deux monômes avec $m \cdot n = 1994$. La décompostion en facteurs premiers de $1994 = 2 \cdot 997$ les seules possibilités sont $(m, n) = (1, 1994), (2, 997), (997, 2)$ et $(1994, 1)$. □

Exemple 2. *Écrire $x^5 + x + 1$ comme produit de deux polynômes non constants à coefficients entiers.*

Démonstration. Cherchons une factorisation de la forme

$$x^5 + x + 1 = (x^3 + ax^2 + bx + c)(x^2 + rx + s).$$

On peut choisir deux facteurs unitaires sans perte de généralité car le produit des coefficients dominants de droite doit être le coefficient dominant de gauche, donc 1. Ainsi les deux valent 1 ou les deux valent -1 ; dans le deuxième cas on peut remplacer les deux facteurs par leur opposé. En multipliant les deux facteurs et en comparant les coefficients on obtient le système d'équations suivant :

$$\begin{aligned} a + r &= 0 \\ b + ar + s &= 0 \\ c + br + as &= 0 \\ bs + cr &= 1 \\ cs &= 1 \end{aligned}$$

La dernière équation implique que $c = s = \pm 1$ et en introduisant ces valeurs dans les autres équations on trouve l'unique solution $a = -1, b = 0, c = 1, r = 1, s = 1$. Cela nous donne

$$x^5 + x + 1 = (x^3 - x^2 + 1)(x^2 + x + 1).$$

□

De temps en temps il faut construire des polynômes qui doivent prendre certaines valeurs à certains endroits. Ceci est toujours possible si le degré du polynôme vaut au plus le nombre de valeurs données moins un. Cette affirmation est l'énoncé du théorème suivant.

Proposition 1.1. *Soit n un nombre naturel et soient $a_0, \ldots, a_n$, $b_0, \ldots, b_n$ des nombres réels (ou complexes) fixés, deux à deux différents. Alors il existe exactement un polynôme P de degré $\leq n$ avec*

$$P(a_k) = b_k \qquad \text{pour } 0 \leq k \leq n.$$

On appelle les points du plan (a_k, b_k) les noeuds et P le polynôme d'interpolation passant par les noeuds (a_k, b_k). Si les noeuds sont tous rationnels (resp. réels), alors P a des coefficients rationnels (resp. réels).

Preuve. On prouve d'abord l'existence d'un tel polynôme. Pour cela on introduit les polynômes de Lagrange. Soit

$$L_k(x) = \prod_{i \neq k} \frac{x - a_i}{a_k - a_i},$$

où i parcourt les indices $0, \ldots, n$ à l'exception de $i = k$. D'après cette construction on a $L_k(a_l) = 0$ si $k \neq l$ et $L_k(a_k) = 1$. Le polynôme

$$P(x) = \sum_{k=0}^{n} b_k \cdot L_k(x)$$

satisfait alors toutes les conditions demandées. De plus les L_k n'ont que des coefficients rationnels (resp. réels) si tous les a_k sont rationnels (resp. réels). L'unicité sera prouvée plus tard en tant que conséquence immédiate du théorème 1.10.

□

Il faut remarquer que P n'a pas nécessairement des coefficients *entiers* si tous les a_k, b_k sont entiers. Un contre-exemple est le polynôme $P(x) = x(x+1)/2$, qui n'a pas de coefficients entiers mais $P(a) \in \mathbb{Z}$ pour tout $a \in \mathbb{Z}$.

Exemple 3. *Soit P un polynôme de degré $\leq n$, tel que*

$$P(k) = \binom{n+1}{k}^{-1}, \qquad k = 0, 1, \ldots, n.$$

Trouver la valeur de $P(n+1)$.

Solution. La construction avec le polynôme de Lagrange nous donne

$$P(x) = \sum_{k=0}^{n} \prod_{i \neq k} \left(\frac{x - i}{k - i} \right) P(k).$$

Or on a

$$\begin{aligned}\prod_{i\neq k}\left(\frac{n+1-i}{k-i}\right) =& \frac{n+1}{k}\cdot\frac{n}{k-1}\cdots\frac{n-k+2}{1}\cdot\frac{n-k}{-1}\cdots\frac{1}{k-n}\\ =&(-1)^{n-k}\binom{n+1}{k}.\end{aligned}$$

Il s'ensuit donc

$$P(n+1)=\sum_{k=0}^{n}(-1)^{n-k}=\begin{cases}0 \text{ pour n impair}\\ 1 \text{ pour n pair.}\end{cases}$$

□

Mais le chemin qui passe par les polynômes de Lagrange n'est pas toujours le chemin le plus simple. Souvent il est plus simple de poser un système d'équations pour les coefficients cherchés.

Exemple 4. *Trouver un polynôme P de degré 3 avec $P(n)=2^{n-1}$ pour $n=1,2,3,4$.*

Solution. On pose $P(x)=ax^3+bx^2+cx+d$ pour obtenir le système d'équations

$$\begin{aligned}a+b+c+d=&P(1)=1\\ 8a+4b+2c+d=&P(2)=2\\ 27a+9b+3c+d=&P(3)=4\\ 64a+16b+4c+d=&P(4)=8\end{aligned}$$

avec comme unique solution $a=1/6$, $b=-1/2$, $c=4/3$ et $d=0$.

□

1.2 Divisibilité

Dans cette section tous les polynômes sont des polynômes à coefficents dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. La lettre K représente toujours un des ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Un nombre $a\in K$ est appelé une *unité* si a est inversible dans K, c'est-à-dire s'il existe un nombre $b\in K$ avec $ab=1$. Clairement ±1 sont les seules unités dans $\mathbb{Z}$ tandis que pour $K=\mathbb{Q},\mathbb{R},\mathbb{C}$ tous les éléments non nuls sont des unités. Cette petite différence entre $\mathbb{Z}$ et les autres ensembles mentionnés est la source de beaucoup de problèmes et finalement la raison pour laquelle beaucoup des résultats suivants diffèrent dans le cas $K=\mathbb{Z}$ on n'y sont valables que pour des polynômes unitaires. Deux polynômes $p,q\in K[x]$ sont appelés *équivalents* s'il existe une unité $a\in K$ avec $p=a\cdot q$.

Soient $p,q\in K[x]$ deux polynômes arbitraires. On dit que p est divisible par q dans K s'il existe un polynôme $a\in K[x]$ avec $p=a\cdot q$. Un polynôme $p\in K[x]$ est appelé *irréductible*

dans $K[x]$ s'il n'est pas une unité et si pour toute représentation de la forme $p = a \cdot b$ dans $K[x]$ on a que a ou b est une unité. Il est essentiel de savoir dans quel ensemble on considère les coefficients de p. Le polynôme $2x-4$ est par exemple irréductible sur $\mathbb{Q}$ mais pas irréductible sur $\mathbb{Z}$, car on a $2x-4 = 2(x-2)$ et aucun des deux facteurs n'est une unité dans $\mathbb{Z}$. Un autre exemple est le polynôme $p(x) = x^4 - 2$. On peut facilement calculer que p est irréductible sur $\mathbb{Z}$ et $\mathbb{Q}$ (on peut par exemple utiliser le critère d'Eisenstein, voir plus bas). D'autre part on peut factoriser p sur $\mathbb{R}$ resp. $\mathbb{C}$ comme ceci :

$$p(x) = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Comme pour les entiers, pour les polynômes on a aussi une division avec reste. On va énoncer le théorème suivant seulement pour le cas de la division de p par un polynôme q unitaire. Pour $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ c'est sans importance car le coefficient dominant est toujours une unité dans K. Plus précisément : On peut diviser p et q par le coefficient dominant de q et on est dans la situation désirée. Pour $K = \mathbb{Z}$ ce n'est pas possible et le théorème est en général faux pour des polynômes non unitaires q. On insiste sur ce point car il est la source de beaucoup des difficultés qu'on aura dans le cas $K = \mathbb{Z}$.

Proposition 1.2 (Division avec reste)**.** *Soit $p(x) \in K[x]$ un polynôme arbitraire et $q(x) \in K[x]$ un polynôme unitaire. Alors il existe dans $K[x]$ des polynômes $d(x)$ et $r(x)$ uniquement déterminés avec $\deg(r) < \deg(q)$ tels que*

$$p(x) = d(x) \cdot q(x) + r(x).$$

$r(x)$ est appelé le reste *de la division par $q(x)$. On a $r(x) = 0$ si et seulement si p est divisible par q.*

Comme pour les nombres entiers, la division avec reste est le point de départ pour toute l'arithmétique des polynômes. Ainsi il est peu surprenant que tous les résultats de la première section du script de théorie des nombres sont aussi valables pour les polynômes. Nous énonçons ici les résultats sans les prouver. Souvent la preuve est analogue au cas des entiers. Comme pour les entiers, il existe une "décomposition en facteurs premiers" pour les polynômes :

Théorème 1.3. *Soit $p \in K[x]$ un polynôme non nul. Alors il existe des polynômes non équivalents irréductibles $p_1, \ldots, p_r \in K[x]$ et des nombres naturels $a_1, \ldots, a_r$ avec*

$$p = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Les nombres a_i sont uniquement déterminés, les polynômes p_i sont uniques à équivalence près.

Un défaut mineur de cet énoncé est que les facteur irréductibles p_i n'y soient uniques qu'à équivalence près. Toutefois on peut facilement se débarrasser de ce défaut. Dans le cas $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ tout polynôme est équivalent à un unique polynôme unitaire. On peut alors se restreindre aux polynômes unitaires et le théorème 1.3 prend ainsi la forme suivante :

Théorème 1.4. *Soit $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ et soit $p \in K[x]$ un polynôme non nul. Alors il existe des polynômes unitaires irréductibles distincts $p_1, \ldots, p_r \in K[x]$, des nombres naturels $a_1, \ldots, a_r$ et une unité $u \in K$ avec*

$$p = u \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Les a_i, les p_i et l'unité u sont uniquement déterminés.

Dans le cas $K = \mathbb{Z}$ la situation est légèrement différente. Les seules unités dans $\mathbb{Z}$ sont ± 1. Ainsi tout polynôme est équivalent à un seul polynôme avec coefficient dominant positif. On peut donc choisir les polynôme irréductibles à coefficient dominant positif comme système de représentants des polynômes irréductibles. Le théorème 1.3 devient alors

Théorème 1.5. *Soit $p \in \mathbb{Z}[x]$ un polynôme non nul. Alors il existe des polynômes irréductibles $p_1, \ldots, p_r \in K[x]$ distincts avec coefficient dominant positif, des nombres naturels $a_1, \ldots, a_r$ et un signe $\epsilon = \pm 1$ avec*

$$p = \epsilon \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}.$$

Les a_i, les p_i et le signe ϵ sont uniquement déterminés.

Bien sûr on peut se demander comment décrire tous les polynômes irréductibles sur K. On va donner une réponse complète à cette question pour $K = \mathbb{R}$ et $\mathbb{C}$ dans le théorème 1.14. Pour $K = \mathbb{Z}$ et $\mathbb{Q}$ le problème est beaucoup plus compliqué. Par exemple tous les nombres premiers sont des polynômes constants irréductibles dans $\mathbb{Z}[x]$. On va d'abord montrer le fait surprenant que l'irréductibilité sur $\mathbb{Z}$, resp. sur $\mathbb{Q}$ est essentiellement la même chose. Pour ceci on a besoin de deux résultats qui sont très utiles mais qui ne sont pas faciles à prouver.

Proposition 1.6 (Gauss)**.** *Soit $p \in \mathbb{Z}[x]$ un polynôme unitaire et supposons $p = a \cdot b$ avec des polynômes unitaires $a, b \in \mathbb{Q}[x]$. Alors a et b ont automatiquement des coefficients entiers.*

Pour le résultat suivant on a besoin de la notion de primitivité d'un polynôme. Soit $p(x) = a_n x^n + \ldots + a_1 x + a_0$ un polynôme. Alors p est appelé *primitif* si tous les coefficients sont entiers et si l'on a $\operatorname{pgcd}(a_n, \ldots, a_1, a_0) = 1$. Par exemple tout polynôme unitaire à coefficients entiers est primitif. Remarque : Tout polynôme à coefficients rationnels est équivalent à un polynôme primitif. On peut simplement le multiplier par le plus petit commun multiple des dénominateurs de ses coefficients.

Proposition 1.7. *Soit $p \in \mathbb{Z}[x]$ un polynôme. Alors p est irréductible sur $\mathbb{Z}$ si et seulement si une des conditions suivantes est satisfaite :*

1. *p est au signe près un nombre premier.*
2. *p est primitif et irréductible sur $\mathbb{Q}$.*

Dans ce qui suit on va se restreindre à des polynômes non constants et primitifs. Un critère d'irréductibilité très utile est le critère d'Eisenstein.

Proposition 1.8 (Eisenstein). *Soit $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polynôme primitif de degré $n > 0$. De plus soit p un nombre premier avec*

$$p \nmid a_n, \qquad p \mid a_i \text{ pour } i < n, \qquad p^2 \nmid a_0.$$

Alors f est irréductible sur $\mathbb{Z}$.

Pour illustrer ceci on va montrer l'irréductibilité d'une famille importante de polynômes dont on va parler plus tard. Cet exemple montre entre autres que sur $\mathbb{Z}$ il existe des polynômes irréductibles de degré arbitrairement grand.

Exemple 5. *Soit p un premier. Prouver que le polynôme $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ est irréductible sur $\mathbb{Z}$.*

Solution. Au lieu de considérer $f(x)$ on considère $f(x+1)$. Clairement les deux se factorisent de la même façon, il suffit donc de montrer que le deuxième est irréductible. À l'aide des suites géométriques on trouve

$$\begin{aligned} f(x+1) =& \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x} \\ =& x^{p-1} + \binom{p}{1} x^{p-2} + \ldots + \binom{p}{p-2} x + \binom{p}{p-1}. \end{aligned}$$

L'irréductibilité suit directement du critère d'Eisenstein : tous les coefficients sauf le premier sont divisibles par p et comme le terme constant vaut p, il n'est pas divisible par p^2. □

1.3 PGCD et PPCM

Grâce à la division avec reste toute la section correspondante du script de théorie des nombres peut être recopiée ici. Toutefois dans le cas $K = \mathbb{Z}$ l'algorithme d'Euclide ne marche plus en général.

1.4 Les zéros d'un polynôme

Soit $p \in K[x]$ un polynôme quelconque et $a \in K$ un nombre. On dit que a est un *zéro* de p si $p(a) = 0$. La division avec reste de p par le polynôme linéaire $(x - a)$ nous donne deux polynômes uniquement déterminés d et r tels que $p(x) = d(x) \cdot (x - a) + r$, où le degré de r est plus petit que le degré de $(x - a)$, autrement dit avec r constant. En évaluant le polynôme en $x = a$, il s'ensuit que $r = p(a)$. Cela nous donne le résultat suivant important.

Proposition 1.9. *Soit $p \in K[x]$ un polynôme et soit $a \in K$ un nombre. Il existe alors un polynôme uniquement déterminé $d(x) \in K[x]$ tel que*

$$p(x) = d(x) \cdot (x - a) + p(a).$$

En particulier a est un zéro de $p(x)$ si et seulement si le polynôme linéaire $(x-a)$ est un facteur de $p(x)$.

Il peut bien sûr arriver que p soit non seulement divisible par $(x-a)$ mais également par une plus grande puissance de ce facteur linéaire. Dans ces cas-là on doit compter a plusieurs fois comme zéro. On dit que a est un *zéro k-tuple* de p (ou un zéro de *multiplicité* k) si p est divisible par $(x-a)^k$, mais pas par $(x-a)^{k+1}$. Avec ces définitions on peut formuler l'estimation suivante pour le nombre de zéros d'un polynôme :

Théorème 1.10 (Théorème de l'identité)**.**

1. *Soit $p \in K[x]$ un polynôme de degré $n \geq 0$. Alors p admet au plus n zéros dans K, en comptant avec multiplicité. De plus p possède exactement n zéros dans K si p se décompose sur K en facteurs linéaires (autrement dit si p est un produit de polynômes de degré ≤ 1 avec coefficients dans K).*
2. *Si p est un polynôme de degré $\leq n$ et s'il possède au moins $n+1$ zéros (avec multiplicités), alors p est le polynôme identiquement nul.*
3. *Si p et q sont deux polynômes de degré $\leq n$ et s'ils prennent la même valeur en au moins $n+1$ points, alors $p = q$.*

Preuve. Supposons que p admette les zéros $a_1, \ldots, a_r \in K$ avec multiplicités respectives $m_1, \ldots, m_r$. D'après la proposition 1.9 il existe un polynôme $d \in K[x]$ avec

$$p(x) = (x-a_1)^{m_1} \cdots (x-a_r)^{m_r} \cdot d(x).$$

Comme $p \neq 0$ on a également $d \neq 0$. Soit donc $m := \deg d \geq 0$. En comparant les degrés des deux côtés de l'équation, on obtient $\sum m_i = n - m \leq n$, ce qui démontre (a). L'affirmation (b) est une conséquence directe car si p n'était pas nul, il y aurait contradiction avec (a). Pour finir (c) s'ensuit de (b) en appliquant ce dernier au polynôme $p - q$.

□

Exemple 6 (Espagne 2000)**.** *Considérons les polynômes*

$$\begin{aligned} P(x) =& x^4 + ax^3 + bx^2 + cx + 1, \\ Q(x) =& x^4 + cx^3 + bx^2 + ax + 1, \end{aligned}$$

où a, b, c sont des nombres réels avec $a \neq c$. Trouver des conditions sur a, b, c pour que P et Q aient au moins deux zéros communs et trouver dans ces cas tous les zéros de P et Q.

Solution. Chaque zéro commun de P et Q est également un zéro de leur différence. Comme

$$P(x) - Q(x) = (a-c)x(x^2-1)$$

et $a \neq c$, les seules possibilités pour les zéros sont $x = 0, 1, -1$. Mais comme $x = 0$ n'est jamais un zéro de P ou de Q on doit avoir $x = \pm 1$ comme zéros communs. Les équations

$P(1) = P(-1) = 0$ nous donnent les conditions $a+b+c+2 = -a+b-c+2 = 0$, autrement dit $a = -c$ et $b = -2$. Or dans ce cas-là on obtient

$$\begin{aligned} P(x) =& x^4 - 2x^2 + 1 + a(x^3 - x) = (x^2-1)^2 + ax(x^2-1) = (x^2 + ax - 1)(x^2-1), \\ Q(x) =& x^4 - 2x^2 + 1 - a(x^3 - x) = (x^2-1)^2 - ax(x^2-1) = (x^2 - ax - 1)(x^2-1). \end{aligned}$$

Les zéros de P sont donc $x = 1, -1, (-a + \sqrt{a^2+4})/2, (-a - \sqrt{a^2+4})/2$, les zéros de Q sont $x = 1, -1, (a + \sqrt{a^2+4})/2, (a - \sqrt{a^2+4})/2$. En particulier P et Q admettent vraiment deux zéros communs qui sont $x = \pm 1$. □

Pour des polynômes à coefficients entiers (ou rationnels) les zéros *rationnels* sont faciles à trouver. Le lemme suivant réduit fortement les possibilités pour de tels zéros.

Lemme 1.11. *Soit $p(x) = a_n x^n + \ldots + a_1 x + a_0$ un polynôme à coefficients entiers avec $a_n, a_0 \neq 0$. Si u est un zéro rationnel de p et si on écrit $u = r/s$ avec r, s premiers entre eux, alors $r \mid a_0$ et $s \mid a_n$.*

Preuve. Par hypothèse on a $a_n u^n + \ldots + a_1 u + a_0 = 0$. En multipliant l'équation par s^n, on obtient

$$a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0.$$

Comme s divise tous les termes à part le premier et que la somme vaut zéro, on doit avoir $s \mid a_n r^n$. Etant donné que s et r sont premiers entre eux, on obtient en effet $s \mid a_n$. De façon analogue on peut conclure que $r \mid a_0 s^n$ et donc $r \mid a_0$.

□

Le *conjugué* d'un nombre complexe $z = x+iy$ est défini par $\overline{z} = x-iy$ (il s'agit de l'image de z par la symétrie par rapport à l'axe réel). Dans le cas d'un polynôme réel les zéros non réels apparaissent toujours par couples conjugués ; c'est l'énoncé de la proposition suivante.

Proposition 1.12. *Soient $p \in \mathbb{R}[x]$ un polynôme réel et $a \in \mathbb{C}$ un nombre complexe. On a alors $p(\overline{a}) = \overline{p(a)}$. En particulier si a est un zéro de multiplicité n de p, alors $\overline{a}$ est également un zéro de multiplicité n de p.*

Preuve. Soit $p(x) = a_n x^n + \ldots + a_1 x + a_0$. On a

$$\begin{aligned} p(\overline{a}) =& a_n \cdot (\overline{a})^n + \ldots + a_1 \cdot \overline{a} + a_0 = \overline{a_n} \cdot \overline{(a^n)} + \ldots + \overline{a_1} \cdot \overline{a} + \overline{a_0} \\ =& \overline{a_n \cdot a^n + \ldots + a_1 \cdot a + a_0} = \overline{p(a)}. \end{aligned}$$

Il s'ensuit clairement que a est un zéro de p si et seulement si $\overline{a}$ est également un zéro. Dans ce cas on a $p(x) = (x-a)(x-\overline{a}) \cdot p_1(x)$. Comme $(x-a)(x-\overline{a}) = x^2 - 2\Re(a)x + |a|^2$ est un polynôme réel, les coefficients de p_1 doivent également être réels. Si maintenant a est un zéro de p_1, on peut mettre en évidence un facteur supplémentaire $(x-a)(x-\overline{a})$. En répétant ce procédé, on remarque que les multiplicités des zéros a et $\overline{a}$ doivent être les mêmes. □

Nous avons déjà beaucoup parlé des zéros des polynômes, mais la question de l'existence de tels zéros est restée jusqu'ici ouverte.

Théorème 1.13 (Théorème fondamental de l'algèbre)**.** *Tout polynôme complexe non constant admet un zéro complexe.*

Par la mise en évidence successive des facteurs linéaires il s'ensuit directement que tout polynôme complexe de degré $n \geq 1$ possède exactement n zéros complexes, comptés avec multiplicité. Nous sommes enfin en mesure de classifier les polynômes irréductibles réels et complexes.

Proposition 1.14. *1. Les polynômes complexes irréductibles sont précisément les polynômes linéaires.*

2. Tout polynôme réel irréductible est soit linéaire, soit quadratique de la forme $ax^2 + bx + c$ avec un discriminant négatif $D = b^2 - 4ac < 0$.

Preuve. (a) est une conséquence directe du théorème 1.13. Soit maintenant p un polynôme réel irréductible. De nouveau par le théorème 1.13 le polynôme p admet un zéro complexe u. Si u est réel, alors p admet un facteur linéaire et doit donc lui-même être linéaire. Si u n'est pas réel, alors par la proposition 1.12 le polynôme p admet comme facteur réel $(x-u)(x-\overline{u})$. Par conséquent p doit être un multiple scalaire de $(x-u)(x-\overline{u})$. Comme les zéros d'un polynôme quadratique sont donnés par $(-b \pm \sqrt{D})/(2a)$, le seul cas dans lequel les zéros ne sont pas réels (et donc le polynôme est irréductible sur $\mathbb{R}$) est quand $D < 0$.

□

Exemple 7. *Soit P un polynôme réel tel que pour tout $x \in \mathbb{R}$ on a $P(x) \geq 0$. Montrer qu'il existe deux polynômes réels Q_1 et Q_2 avec $P = Q_1^2 + Q_2^2$.*

Solution. Le coefficient dominant c de P doit être positif, sinon on aurait $P(x) < 0$ pour des x très grands. D'après la proposition 1.14 il existe des nombres réels $a_1, \ldots, a_r$ et $b_1, \ldots, b_s$, $c_1, \ldots, c_s$ avec $b_i^2 - 4c_i < 0$ et

$$P(x) = c \prod_{i=1}^{r} (x - a_i) \prod_{i=1}^{s} (x^2 + b_i x + c_i).$$

Comme P est partout non négatif, les zéros réels a_i doivent tous être de multiplicité paire. Ainsi le premier produit est le carré d'un polynôme réel. On a de plus que $c = (\sqrt{c})^2$ est également le carré d'un polynôme réel, il suffit donc de montrer que le dernier produit est la somme de deux carrés de polynômes réels. Chaque facteur s'écrit comme

$$x^2 + b_i x + c_i = \left(x + \frac{b_i}{2}\right)^2 + \left(c_i - \frac{b_i^2}{4}\right),$$

et vu que $c_i > b_i^2/4$, le deuxième terme est positif, donc il est bien le carré d'un nombre réel. Par conséquent chaque terme du dernier produit est la somme de deux carrés, donc

leur produit l'est également car nous avons la formule d'Euler bien connue

$$(X^2+Y^2)(Z^2+U^2) = (XZ+YU)^2 + (XU-YZ)^2.$$

□

Exemple 8. *Trouver tous les polynômes P qui satisfont l'égalité*

$$P(x)P(x+1) = P(x^2).$$

Solution. Le polynôme identiquement nul est clairement une solution, de même que le polynôme constant $P = 1$. Nous allons désormais supposer que $P \neq 0$. Soit α un zéro complexe de P. En évaluant le polynôme en α on obtient $P(\alpha^2) = 0$, donc α^2 est également un zéro. En répétant le procédé on voit que $\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots$ sont tous des zéros de P. Comme P n'est pas identiquement nul, il ne peut avoir qu'un nombre fini de zéros. Il s'ensuit que $\alpha = 0$ ou $|\alpha| = 1$. En évaluant P en $x = \alpha - 1$, on obtient de manière similaire que $(\alpha-1)^2$ est aussi un zéro de P. Par l'argument qu'on vient d'invoquer on a $\alpha - 1 = 0$ ou $|\alpha - 1| = 1$ également. Nous allons désormais supposer que $\alpha \neq 0, 1$ et nous allons montrer que cela nous conduit à une contradiction.

Nous devrions donc avoir $|\alpha| = |\alpha - 1| = 1$, c'est-à-dire que les deux nombres se trouvent sur le cercle unité et leur distance horizontale vaut 1. A l'aide d'un dessin on voit facilement que ce n'est le cas que pour $\alpha_1 = e^{i\pi/3}$ et $\alpha_2 = e^{i5\pi/3}$. Or par la première partie de notre raisonnement α_1^2, resp. α_2^2 sont également des zéros. Etant donné que $\alpha_1^2 = e^{i2\pi/3} \neq \alpha_1, \alpha_2, 0, 1$ et $\alpha_2^2 = e^{i4\pi/3} \neq \alpha_1, \alpha_2, 0, 1$, nous avons la contradiction cherchée.

Les seuls zéros possibles de P sont donc 0 et 1. Par conséquent les polynômes cherchés sont de la forme $P(x) = cx^m(x-1)^n$ avec un nombre complexe $c \neq 0$ et des entiers non-négatifs m, n. En substituant dans l'équation on obtient

$$c^2(x+1)^m x^{m+n}(x-1)^n = cx^{2m}(x^2-1)^n.$$

En appliquant l'identité $x^2 - 1 = (x-1)(x+1)$ et en comparant les facteurs linéaires et les coefficients dominants des deux côtés, on voit que $c = 1$ et $m = n$. Les solutions sont donc $P = 0$ et pour $n \geq 1$ les polynômes

$$P(x) = x^n(x-1)^n.$$

□

2 Polynômes symétriques

2.1 Polynômes symétriques élémentaires

Dans cette section nous allons parler de polynômes en n variables $x_1, \ldots, x_n$. Un tel polynôme s'appelle *symétrique* s'il ne change pas quand on permute les variables. D'une

façon un peu plus formelle on peut dire que $P(x_1, \ldots, x_n)$ est symétrique si pour toute permutation π de $\{1, 2, \ldots, n\}$ on a

$$P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = P(x_1, \ldots, x_n).$$

Voici quelques exemples de polynômes symétriques en trois variables x, y, z :

$$x^n + y^n + z^n + xyz, \qquad xy + yz + zx - 4, \qquad (x-y)^{2n} + (y-z)^{2n} + (z-x)^{2n}.$$

Les polynômes symétriques les plus simples sont les *polynômes symétriques élémentaires* $s_1, \ldots, s_n$. Ils sont définis de la façon suivante :

$$s_k = \sum_{i_1 < i_2 < \ldots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}, \qquad 1 \leq k \leq n.$$

En d'autres termes, s_k est la somme de tous les termes possibles obtenus en multipliant k des n variables différentes entre elles. Pour rendre cela un peu plus clair voici les polynômes symétriques élémentaires pour les cas $n = 2, 3$ explicitement. Pour $n = 2$ on a (pour les variables x, y)

$$u = s_1 = x + y, \qquad v = s_2 = xy.$$

Pour $n = 3$ on a (pour les variables x, y, z)

$$u = s_1 = x + y + z, \qquad v = s_2 = xy + yz + zx, \qquad w = s_3 = xyz.$$

Les désignations u, v, w sont dans ces cas-là usuelles.

Un fait très important est que *tout* polynôme symétrique s'écrit de manière unique comme un polynôme ayant pour variables les polynômes symétriques élémentaires.

Théorème 2.1. *Soit P un polynôme symétrique en n variables $x_1, \ldots, x_n$. Alors il existe exactement un polynôme Q en n variables tel que*

$$P(x_1, x_2, \ldots, x_n) = Q(s_1, s_2, \ldots, s_n).$$

Nous n'allons pas entrer dans les détails de la preuve car elle est plutôt technique, mais remarquons que l'existence du polynôme Q est assurée par une méthode de construction explicite. Cette dernière n'est malheureusement pas très commode à utiliser, voici tout de même quelques exemples de la façon dont on procède avec un polynôme symétrique donné pour construire Q. La règle de base est : 'Toujours commencer par les puissances pures !'

Exemple 9. *Factoriser le polynôme*

$$x^3 + y^3 + z^3 - 3xyz.$$

Solution. Nous allons exprimer le polynôme en fonction de u, v, w. Pour commencer on a $u^2 = x^2 + y^2 + z^2 + 2(xy + yz + zx)$ et donc $x^2 + y^2 + z^2 = u^2 - 2v$. Il s'ensuit alors que $u \cdot (u^2 - 2v) = (x+y+z)(x^2+y^2+z^2) = (x^3+y^3+z^3)+(x^2y+x^2z+y^2x+y^2z+z^2x+z^2y)$. D'un autre côté on a $uv = (x^2y + x^2z + y^2x + y^2z + z^2x + z^2y) + 3xyz$. En combinant ces deux résultats on obtient

$$x^3 + y^3 + z^3 = u(u^2 - 2v) - (uv - 3w) = u^3 - 3uv + 3w$$

et pour finir

$$\begin{aligned} x^3 + y^3 + z^3 - 3xyz =& (u^3 - 3uv + 3w) - 3w = u(u^2 - 3v) \\ =& (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx). \end{aligned}$$

□

Exemple 10. *Soit $n \geq 0$ un nombre entier et soit $P_n = x^n + y^n + z^n$. Montrer pour $n \geq 2$ la formule de récurrence suivante :*

$$P_{n+1} = uP_n - vP_{n-1} + wP_{n-2}.$$

A l'aide de cette formule, exprimer P_n comme polynôme en u, v, w pour $n \leq 5$.

Solution. La formule de récurrence est une conséquence du calcul suivant :

$$\begin{aligned} uP_n =& (x + y + z)(x^n + y^n + z^n) \\ =& (x^{n+1} + y^{n+1} + z^{n+1}) + (x^n y + x^n z + y^n x + y^n z + z^n x + z^n y) \\ =& P_{n+1} + (xy + yz + zx)(x^{n-1} + y^{n-1} + z^{n-1}) - (x^{n-1}yz + y^{n-1}zx + z^{n-1}xy) \\ =& P_{n+1} + vP_{n-1} - wP_{n-2}. \end{aligned}$$

De plus on a $P_0 = 3$, $P_1 = u$ et $P_2 = u^2 - 2v$. On obtient ainsi dans l'ordre

$$\begin{aligned} P_3 =& uP_2 - vP_1 + wP_0 = u^3 - 3uv + 3w, \\ P_4 =& uP_3 - vP_2 + wP_1 = u^4 - 4u^2v + 2v^2 + 4uw, \\ P_5 =& uP_4 - vP_3 + wP_2 = u^5 - 5u^3v + 5uv^2 + 5u^2w - 5vw. \end{aligned}$$

□

Comme le dernier exemple le montre, ces calculs peuvent très vite devenir compliqués.

2.2 Les formules de Viète

Dans cette section nous allons parler des formules de Viète qui jouent un rôle très important dans l'étude des polynômes. Considérons dans un premier temps un polynôme $P(x) = a_n x^n + \ldots + a_1 x + a_0$ en *une* variable. Ce polynôme admet exactement n zéros complexes $\alpha_1, \ldots, \alpha_n$ (comptés avec multiplicité). Ces zéros sont bien sûr uniquement

déterminés par les coefficients du polynôme, mais il est toutefois très difficile (et même pour $n \geq 5$ impossible en général) de les calculer explicitement. Le sens opposé, c'est-à-dire retrouver les coefficients à partir des zéros du polynôme, est très simple, comme la proposition suivante le montre.

Proposition 2.2 (Viète)**.** *Soit $P(x) = a_n x^n + \ldots + a_1 x + a_0$ un polynôme avec $a_n \neq 0$. Soient $\alpha_1, \ldots, \alpha_n$ les zéros complexes de P (comptés avec multiplicité), et soit s_k le kième polynôme symétrique élémentaire en les α_i. Alors*

$$s_k := s_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \cdot \frac{a_{n-k}}{a_n}, \qquad \text{pour } 1 \leq k \leq n.$$

Preuve. Nous avons par hypothèse

$$P(x) = a_n x^n + \ldots + a_1 x + a_0 = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

En effectuant la multiplication du côté droit, on obtient par la définition des polynômes symétriques élémentaires s_k

$$\prod_{k=1}^{n}(x - \alpha_k) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - + \ldots + (-1)^n s_n.$$

En substituant dans la première équation et en comparant les coefficients des deux côtés, l'affirmation s'ensuit. □

Les formules de Viète nous permettent donc d'exprimer les polynômes symétriques élémentaires en les zéros à travers les coefficients sans devoir connaître les zéros eux-mêmes. En combinant ceci avec le théorème 2.1 on obtient ainsi *tous* les polynômes symétriques en $\alpha_1, \ldots, \alpha_n$. C'est une observation très importante qui peut être appliquée dans de nombreux cas.

Exemple 11. *(Canada 96) Soient α, β et γ les zéros du polynôme $x^3 - x - 1$. Trouver la valeur de*

$$A = \frac{1-\alpha}{1+\alpha} + \frac{1-\beta}{1+\beta} + \frac{1-\gamma}{1+\gamma}.$$

1ère solution. On utilise la notation habituelle $u = \alpha + \beta + \gamma$, $v = \alpha\beta + \beta\gamma + \gamma\alpha$ et $w = \alpha\beta\gamma$. Un calcul simple montre que

$$\begin{aligned} A =& \frac{(1-\alpha)(1+\beta)(1+\gamma) + (1-\beta)(1+\gamma)(1+\alpha) + (1-\gamma)(1+\alpha)(1+\beta)}{(1+\alpha)(1+\beta)(1+\gamma)} \\ =& \frac{3 + u - v - 3w}{1 + u + v + w}. \end{aligned}$$

Les formules de Viète nous donnent alors

$$u = 0, \qquad v = -1, \qquad w = 1,$$

et ainsi $A = 1$. □

2e solution. La solution se simplifie si on calcule directement avec $\alpha' = 1+\alpha$, $\beta' = 1+\beta$ et $\gamma' = 1+\gamma$. Il est clair que ces nombres seront les zéros du polynôme $(x-1)^3-(x-1)-1 = x^3-3x^2+2x-1$. Soient u', v', w' les polynômes symétriques élémentaires correspondants en α', β', γ'. On a

$$A = \frac{2-\alpha'}{\alpha'} + \frac{2-\beta'}{\beta'} + \frac{2-\gamma'}{\gamma'} = \frac{2v'}{w'} - 3.$$

Les formules de Viète donnent dans ce cas-ci $v' = 2$ et $w' = 1$ et on obtient de nouveau $A = 1$. □

Exemple 12 (APMO 03). *Soient a, b, c, d, e, f des nombres réels tels que les zéros du polynôme*

$$p(x) = x^8 - 4x^7 + 7x^6 + ax^5 + bx^4 + cx^3 + dx^2 + ex + f$$

sont tous réels et positifs. Trouver toutes les valeurs possibles de f.

Solution. Soient $\alpha_1, \ldots, \alpha_8 > 0$ les huit zéros réels de p. Par Viète on a d'un côté

$$s_1 = \sum_{k=1}^{8} \alpha_k = 4, \qquad s_2 = \sum_{1 \le k < l \le 8} \alpha_k \alpha_l = 7.$$

D'un autre côté l'inéquation de McLaurin (ou AM-GM) donne de faç con générale

$$\left(\frac{s_1}{8}\right)^2 \ge \frac{s_2}{28}.$$

A cause de $s_1 = 4$ et $s_2 = 7$ on a même l'égalité dans cette inéquation, mais ce n'est le cas que si $\alpha_1 = \ldots = \alpha_8$. Du fait que $s_1 = 4$, il s'ensuit que tous les α_k prennent la valeur $\frac{1}{2}$. En appliquant Viète encore une fois on obtient comme seule valeur possible $f = (\frac{1}{2})^8 = \frac{1}{256}$. □

Exemple 13 (USA 77). *Soient a et b deux zéros distincts du polynôme $x^4 + x^3 - 1$. Montrer que ab est un zéro du polynôme $x^6 + x^4 + x^3 - x^2 - 1$.*

Solution. On désigne les quatre zéros de $p(x) = x^4 + x^3 - 1$ par a, b, c, d. Un calcul simple montre que ces zéros sont tous différents car p et p' n'ont pas de zéros communs. De plus aucun d'entre eux ne vaut 0. Par Viète on a alors

$$\begin{aligned} a + b + c + d &= -1, \\ ab + ac + ad + bc + bd + cd &= 0, \\ abc + bcd + cda + dab &= 0, \\ abcd &= -1. \end{aligned}$$

Posons $r = ab$, $s = cd$, $u = a + b$, $v = c + d$. Les équations ci-dessus deviennent

$$\begin{aligned} u + v &= -1, \\ r + s + uv &= 0, \\ rv + su &= 0, \\ rs &= -1. \end{aligned}$$

De la première équation on conclut que $v = -1 - u$, et de la quatrième que $s = -1/r$. En remplaçant ceci dans la troisième équation il s'ensuit que $-r(1+u) - u/r = 0$, et donc $u = -r^2/(1+r^2)$. En remplaçant le résultat trouvé dans la deuxième équation on obtient

$$\begin{aligned} & r - \frac{1}{r} + \frac{-r^2}{1+r^2} \cdot \frac{-1}{1+r^2} = 0 \\ \iff & (r^2-1)(r^2+1)^2 + r^3 = 0 \\ \iff & r^6 + r^4 + r^3 - r^2 - 1 = 0, \end{aligned}$$

ce qu'il fallait démontrer. □

Exercices

1. (CH 04) Les nombres réels a, b, c, d satisfont les relations

$$\begin{aligned} a &= \sqrt{45 - \sqrt{21-a}}, \qquad & b &= \sqrt{45 + \sqrt{21-b}}, \\ c &= \sqrt{45 - \sqrt{21+c}}, \qquad & d &= \sqrt{45 + \sqrt{21+d}}. \end{aligned}$$

   Montrer que $abcd = 2004$.

2. (Hongrie 83) Soit $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1$ un polynôme à coefficients entiers positifs. Supposons que P possède n zéros réels. Montrer que

$$P(2) \geq 3^n.$$

3. (OMI 88) Montrer que l'ensemble des nombres réels x qui satisfont l'équation

$$\sum_{k=1}^{70} \frac{k}{x-k} \geq \frac{5}{4}$$

   est une réunion d'intervalles disjoints, telle que la somme de toutes les longueurs d'intervalle vaut 1988.