Notas sobre polinomios

Glenier Bello

1. Definiciones y conceptos básicos

1.1. Un *polinomio* es una función $f : \mathbb{C} \to \mathbb{C}$ del tipo

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

donde n es un entero no negativo y los coeficientes a_j están en $\mathbb{C}$, con $a_n \neq 0$. Diremos que n es el *grado* de f y lo denotaremos por $\deg f$.

Al polinomio idénticamente 0 le llamaremos *polinomio nulo*. A este polinomio no le asociaremos ningún grado.

1.2. Al conjunto de todos los polinomios con coeficientes complejos lo denotaremos por $\mathbb{C}[x]$. Notar que la variable x sólo tiene un valor simbólico, podríamos haber puesto igualmente $\mathbb{C}[z]$. De hecho, quizá resulte más natural usar la variable z para valores complejos y la variable x para valores reales. Sin embargo, en la gran mayoría de los problemas de olimpiadas se suele usar la variable x incluso para valores complejos. Por ello, usaremos siempre como variable la letra x.

A veces, en vez de trabajar con coeficientes complejos, nos interesará trabajar con coeficientes en otros cuerpos como $\mathbb{R}$ o $\mathbb{Q}$, o incluso en anillos como $\mathbb{Z}$ o $\mathbb{Z}_n$ (enteros módulo n). Denotaremos a estas familias de polinomios por $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$ y $\mathbb{Z}_n[x]$, respectivamente.

1.3. Si A es un anillo conmutativo con unidad (como por ejemplo todos los casos considerados en 1.1) entonces $A[x]$ también es un anillo conmutativo con unidad. (Las operaciones de suma y producto en $A[x]$ son las "usuales", no entraremos en detalles.)

El elemento neutro y la unidad en $A[x]$ son precisamente el elemento neutro y la unidad en A.

Sin embargo, $A[x]$ no es un cuerpo, ya que el polinomio $1 - x$ no tiene inverso.

1.4 Ejercicio. Comprobar que el polinomio $1 - x$ no tiene inverso en $\mathbb{C}[x]$.

Ya hemos visto que $\mathbb{C}[x]$ no es un cuerpo. Sin embargo, sí podemos hacer una *división con resto*. Más precisamente, se cumple el siguiente resultado.

1.5 Teorema. *Si $f, g \in \mathbb{C}[x]$, entonces existen $q, r \in \mathbb{C}[x]$ únicos tales que*

$$f(x) = g(x)q(x) + r(x),$$

donde $\deg r < \deg g$ o bien $r = 0$.

Notar que el teorema funciona igualmente si cambiamos $\mathbb{C}$ por cualquier otro cuerpo, como $\mathbb{R}$ o $\mathbb{Q}$.

1.6. A los polinomios q y r les llamaremos *cociente* y *resto* de la división de f entre g, respectivamente. Si $r = 0$, entonces diremos que g divide a f y lo denotaremos por $g \mid f$.

1.7 Ejercicio. Demostrar el Teorema 1.5.

1.8 Ejercicio. Hacer la división con resto de $f(x) = x^7 - 1$ entre $g(x) = x^3 + x + 1$.

1.9. Sea $f \in \mathbb{C}[x]$. Diremos que $a \in \mathbb{C}$ es una *raíz* o un *cero* de f si $f(a) = 0$.

El siguiente resultado es inmediato usando la división con resto.

1.10 Lema. *Si $f \in \mathbb{C}[x]$, entonces $a \in \mathbb{C}$ es una raíz de f si y sólo si $f(x) = (x-a)q(x)$ para cierto $q \in \mathbb{C}[x]$.*

Usando este lema e inducción, deducimos fácilmente el siguiente teorema.

1.11 Teorema. *Si $f \in \mathbb{C}[x]$ es un polinomio de grado n y $a_1, \ldots, a_n \in \mathbb{C}$ son raíces de f, entonces $f(x) = c(x-a_1)\cdots(x-a_n)$, para cierta constante $c \in \mathbb{C}$.*

1.12 Ejercicio. Demostrar el Lema 1.10 y el Teorema 1.11.

1.13. Sea $f \in \mathbb{C}[x]$ un polinomio y $a \in \mathbb{C}$ una raíz de f. Diremos que a es una *raíz de multiplicidad* $m \in \mathbb{N}$ si $f(x) = (x-a)^m q(x)$ para cierto polinomio q tal que $q(a) \neq 0$.

1.14 Teorema. *Sea $f \in \mathbb{C}[x]$ un polinomio y $a \in \mathbb{C}$ una raíz de f. Entonces a es una raíz de multiplicidad m si y sólo si*

$$f(a) = f'(a) = f''(a) = \cdots = f^{(m-1)}(a) = 0, \quad f^{(m)}(a) \neq 0.$$

1.15 Ejercicio. Demostrar el Teorema 1.14.

1.16 Teorema. *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Si $p/q \in \mathbb{Q}$ es una raíz de f con p y q coprimos, entonces $p \mid a_0$ y $q \mid a_n$.*

1.17 Ejercicio. Demostrar el Teorema 1.16.

1.18. Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ y sea $a \in \mathbb{C}$. Poniendo $x = a + (x-a)$ obtenemos que f se puede escribir de la forma

$$f(x) = c_n(x-a)^n + \cdots + c_1(x-a) + c_0,$$

para ciertas constantes $c_j \in \mathbb{C}$.

2. Raíces de la unidad

2.1. Sea $n \in \mathbb{N}$ y pongamos

$$\omega = e^{i\frac{2\pi}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Es inmediato comprobar que $\omega, \omega^2, \ldots, \omega^n = 1$ son raíces del polinomio $x^n - 1$. A estas n raíces se les llama *raíces n-ésimas de la unidad.*

También es fácil comprobar que son los vértices de un n-ágono regular inscrito en la circunferencia unidad centrada en el origen. Notar que uno de los vértices siempre será el punto $(1, 0)$.

Si $\gcd(k, n) = 1$, entonces las potencias ω^k también nos dan las n raíces de la unidad.

Las soluciones de algunos problemas de olimpiada se basan en el uso de las raíces de la unidad.

2.2 Ejemplo.

(a) ¿Para qué naturales n se cumple que $x^2 + x + 1 \mid x^{2n} + x^n + 1$?

(b) Probar que si $n \equiv 0$ ó $n \equiv 1$ módulo 3, entonces $37 \mid 1\underbrace{0\ldots0}_{n}1\underbrace{0\ldots0}_{n}1$.

2.3 Ejemplo. Probar que $x^4 + x^3 + x^2 + x + 1 \mid x^{44} + x^{33} + x^{22} + x^{11} + 1$.

3. Ecuaciones recíprocas

3.1. Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. Diremos que f es un *polinomio recíproco* si $a_j = a_{n-j}$ para $j = 0, \ldots, n$.

Si f es un polinomio recíproco, entonces a la ecuación $f(x) = 0$ la llamaremos *ecuación recíproca.*

3.2 Teorema. *Si $f \in \mathbb{C}[x]$ un polinomio recíproco de grado $2n$, entonces se puede escribir de la forma $f(x) = x^n g(z)$, donde $z = x + 1/x$ y $g(z)$ es un polinomio en z de grado n.*

3.3 Ejercicio.

(a) Si $f \in \mathbb{C}[x]$ tiene grado n y $a_0 \neq 0$, entonces f es un polinomio recíproco si y sólo si
$$x^n f\left(\frac{1}{x}\right) = f(x).$$

(b) Todo polinomio recíproco de grado impar es divisible por $x + 1$ y el cociente es un polinomio recíproco de grado par.

(c) Si $a \in \mathbb{C}$ es un cero de la ecuación recíproca $f(x) = 0$, entonces $1/a$ también es un cero de esta ecuación.

4. Polinomios simétricos y fórmulas de Vieta

4.1. Los *polinomio simétricos* en las variables $x_1, \ldots, x_n$ son polinomios que no cambian al permutar las variables $x_1, \ldots, x_n$. Por ejemplo,

$$f(x, y) = x^5 + y^5 + 3x^2y + 3xy^2 - x - y + 2$$

es un polinomio simétrico en las variables x, y.

Los *polinomios simétricos elementales* son $\sigma_k(x_1, \ldots, x_n) = \sum x_{i_1} \cdots x_{i_k}$, donde la suma es sobre subconjuntos de k elementos $\{i_1, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$. Por ejemplo,

$$\sigma_1(x, y, z) = x + y + z, \quad \sigma_2(x, y, z) = xy + yz + zx, \quad \sigma_3(x, y, z) = xyz.$$

4.2 Teorema. *Sea $\sigma_k = \sigma_k(x_1, \ldots, x_n)$ y sea $s_k = x_1^k + \cdots + x_n^k$. Entonces*

$$k\sigma_k = s_1\sigma_{k-1} - s_2\sigma_{k-2} + \cdots + (-1)^k s_{k-1}\sigma_1 + (-1)^k s_k.$$

4.3 Teorema. *Todo polinomio simétrico en $x_1, \ldots, x_n$ se puede expresar como un polinomio en $\sigma_1, \ldots, \sigma_n$.*

4.4 Teorema (Fórmulas de Vieta). *Sean $\alpha_1, \ldots, \alpha_n$ y $c_1, \ldots, c_n$ números complejos tales que*

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n.$$

Entonces $c_k = (-1)^k \sigma_k(\alpha_1, \ldots, \alpha_n)$ para $k = 1, \ldots, n$.

5. Otros teoremas

5.1 Teorema. *La ecuación cuadrática $ax^2 + bx + c = 0$, con $a, b, c \in \mathbb{R}$ y $a \neq 0$ tiene soluciones*

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

El discriminante *D de la ecuación cuadrática se define como $D := b^2 - 4ac$. Si $D < 0$, entonces las soluciones son complejas y conjugadas. Si $D = 0$, entonces la soluciones degeneran en una única solución real. Si $D > 0$, entonces la ecuación tiene dos soluciones reales distintas.*

5.2 Teorema (Binomio de Newton). *Para cualesquiera $x, y \in \mathbb{C}$ y $n \in \mathbb{N}$ se cumple*

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

5.3 Teorema (Teorema fundamental del Álgebra). *Todo polinomio no constante en $\mathbb{C}[x]$ tiene una raíz compleja.*

5.4 Corolario. *Todo polinomio en $\mathbb{C}[x]$ de grado n tiene exactamente n raíces complejas (contando la multiplicidad).*

5.5. Si $f \in \mathbb{R}[x]$ y $a \in \mathbb{C}$ es una raíz de f, entonces el conjugado de a también es raíz de f.

5.6. Sea A un anillo conmutativo con unidad. Un polinomio en $A[x]$ es *irreducible* en $A[x]$ si no se puede expresar como producto de dos polinomios $g, h \in A[x]$ ambos de grado mayor o igual que 1.

5.7 Teorema (Criterio de Eisenstein). *Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Si existen un primo p y un entero $k \in \{0, 1, \ldots, n-1\}$ tales que $p \mid a_j$ para $j = 0, 1, \ldots, k$, $p \nmid a_{k+1}$ y $p^2 \nmid a_0$, entonces f tiene un factor irreducible g de grado mayor o igual que $k+1$. En particular, si podemos elegir p de manera que $k = n-1$, entonces f es un polinomio irreducible.*

6. Problemas

6.1. Sea $f \in \mathbb{Z}[x]$ un polinomio mónico de grado n y sean $k, p \in \mathbb{N}$. Probar que si ninguno de los números $f(k), f(k+1), \ldots, f(k+p)$ es divisible por $p+1$ entonces f no tiene raíces racionales.

6.2. Probar que el polinomio $1 + x + x^2/2! + \cdots + x^n/n!$ no tiene raíces múltiples.

6.3. Sea $f \in \mathbb{Z}[x]$. Probar que si existen $a, b, c, d \in \mathbb{Z}$ distintos tales que $f(a) = f(b) = f(c) = f(d) = 5$, entonces no existe ningún $k \in \mathbb{Z}$ tal que $f(k) = 8$.

6.4. Probar que $a^2 + ab + b^2 \geq 3(a + b - 1)$ para todos $a, b \in \mathbb{R}$.

6.5. ¿Para qué valores de $a \in \mathbb{R}$ es mínima la suma de los cuadrados de las raíces del polinomio $x^2 - (a-2)x - a - 1$?

6.6. Sean $a, b, c \in \mathbb{R}$ tales que $a + b + c > 0, ab + bc + ca > 0$ y $abc > 0$. Probar que $a, b, c > 0$.

6.7. El polinomio $ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ cumple que ad es impar y bc es par. Probar que el polinomio tiene al menos una raíz que no es racional.

6.8. Sean a, b y c números distintos. La ecuación cuadrática

$$\frac{(x-a)(x-b)}{(c-a)(c-b)} + \frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)} = 1$$

tiene soluciones $x_1 = a, x_2 = b$ y $x_3 = c$. ¿Qué se deduce de este hecho?