Polinomios con coeficientes en un cuerpo

ALGEBRA Y GEOMETRIA ANALITICA

Facultad de Cs. Exactas y Naturales y Agrimensura - UNNE

Esp. Prof. Liliana Noemí Caputo

Año Lectivo 2017

CONJUNTOS DE POLINOMIOS

Definición axiomática

Sean $(\mathbb{K}, +, .)$ un cuerpo (es decir, $\mathbb{K} = \mathbb{Q}$, $\mathbb{K} = \mathbb{R}$ ó $\mathbb{K} = \mathbb{C}$) V un conjunto tal que $V \cap \mathbb{K} = \varnothing$. El conjunto $\mathbb{K}[V]$ en el cual se han definido dos operaciones ($\oplus$, suma) y ($\otimes$, producto) es el conjunto de polinomios con coeficientes en $\mathbb{K}$, si, y sólo si, se cumplen los siguientes axiomas:

<u>Axiomas de construcción</u>

C1) $\mathbb{K} \subset \mathbb{K}[V]$

C2) $V \subset \mathbb{K}[V]$

C3) Si $p, q \in \mathbb{K}[V]$, entonces: $p \oplus q \in \mathbb{K}[V] \wedge p \otimes q \in \mathbb{K}[V]$

C4) Si $p, q \in \mathbb{K}$, entonces: $p \oplus q = p + q \wedge p \otimes q = p.q$

C5) Los únicos elementos de $\mathbb{K}[V]$ son los construibles por C1, C2, C3 y C4.

En virtud del axioma C4, no hay ambigüedad si en vez de escribir $p \oplus q$ y $p \otimes q$, escribimos $p + q$ y $p.q$, respectivamente.

<u>Axiomas de operatividad</u>: Si $p, q, s \in \mathbb{K}[V]$, entonces:

O1) $p + (q + s) = (p + q) + s$

O2) $p + q = q + p$

O3) $p + 0 = p$, siendo 0 el neutro de la suma en $\mathbb{K}$

O4) $p.(q.s) = (p.q).s$

O5) $p.(q + s) = p.q + p.s$

O6) $p.q = q.p$

O7) $1.p = p$, siendo 1 el neutro del producto en $\mathbb{K}$.

O8) $0.p = 0$.

Primeras Observaciones:

1) Al polinomio 0 se lo denomina "polinomio nulo".
2) El opuesto de 1 es decir, -1, es un polinomio por C1.
3) Dado un polinomio $p \in \mathbb{K}[V]$, $(-1).p \in \mathbb{K}[V]$ (por observación 2 y C3) lo denotamos con $-p$ y lo llamaremos el polinomio opuesto de p o, simplemente, el opuesto de p, pues $p + (-1).p =^{1} 1.p + (-1).p =^{2} (1 - 1).p =^{3} 0.p =^{4} 0$
4) Si $p, -q \in \mathbb{K}[V]$, entonces a la suma de p y de $-q$, la denotamos con $p - q$.

Potencias de un polinomio: Sean $p \in \mathbb{K}[V] - \{0\}$ y $n \in \mathbb{N}$. Entonces:

1. $p^0 = 1$
2. $p^n = p.p^{n-1}$

Vemos que cualquier potencia entera y no negativa de un polinomio no nulo p es un polinomio: Si $p \in \mathbb{K}[V] - \{0\}$ y $n \in \mathbb{N}$, se tiene que:

$p^0 = 1 \in \mathbb{K} \subset \mathbb{K}[V]$, por axioma C1.

$p^1 =^{5} p.p^{1-1} = p.p^0 =^{6} p.1 =^{7} p \in \mathbb{K}[V] - \{0\} \subset \mathbb{K}[V]$

---

[1] Por O7.
[2] Por O5.
[3] Por ser 1 y -1 opuestos en $\mathbb{K}$.
[4] Por O8.
[5] Por 2. de la definición de potenciación.
[6] Por 1. de la definición de potenciación.
[7] Por axiomas O6 y O7.

Supongamos que $p^n \in \mathbb{K}[V]$ (HI) y veamos que p^{n+1} también es un polinomio con coeficientes en $\mathbb{K}$. En efecto, por definición de potenciación tenemos que:

$p^{n+1} = p.p^n \in \mathbb{K}[V]$ por HI y axioma C3.

Luego, hemos probado que si $p \neq 0$, $\forall n \in \mathbb{N}_0$: $p^n \in \mathbb{K}[V]$.

Además, en $\mathbb{K}$ - por ser un cuerpo - se cumple que

$$\forall m \in \mathbb{N}: 0^m = 0 \in \mathbb{K} \subset \mathbb{K}[V] \text{ (por axioma C1)}$$

Polinomios en una indeterminada x

Sea ahora $V = \{x\}$. En ese caso, se acostumbra denotar al conjunto de polinomios $\mathbb{K}[V]$ mediante $\mathbb{K}[x]$ y se dice que es el conjunto de polinomios con coeficientes en $\mathbb{K}$, en una indeterminada.

Entonces, por el axioma C2, x es un polinomio con coeficientes en $\mathbb{K}$ y también lo será x^n, cualquiera sea $n \in \mathbb{N}$. Ahora bien, como $V \cap \mathbb{K} = \emptyset$, $x \notin \mathbb{K}$, de donde, $x \neq 0$ y, en consecuencia, $x^0 = 1$.

Luego, $\forall a \in \mathbb{K}$, $\forall\ n \in \mathbb{N}_0$: $a.x^n \in \mathbb{K}[x]$, por axioma C3. Por lo general, cualesquiera sean $a \in \mathbb{K}$ y $n \in \mathbb{N}_0$, al polinomio $a.x^n$ se lo llama **monomio**.

Luego, por los axiomas C3 y O1, la suma de monomios es un polinomio. En particular, a la suma de dos monomios se la llama **binomio**. En consecuencia, es usual representar a un polinomio $p \in \mathbb{K}[x]$ como sigue:

$$p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

con $n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Nótese que el polinomio nulo es tal que $a_i = 0$, $\forall i \in \mathbb{N}_0$. (*)

En ese caso, los a_i se llaman **coeficientes** de p. Al coeficiente a_0 es común llamarlo **término independiente**. Vemos, además, que si n = 0, $p(x) = a_0 \in \mathbb{K}$.

Se llama **grado de p** – y se denota con gr(p) -al máximo i, tal que $a_i \neq 0$. Es decir, si $a_n \neq 0$, gr(p) = n. En ese caso, diremos que a_n es el **coeficiente principal** de p. Un polinomio cuyo coeficiente principal es 1, se dice que es **mónico.**

De (*), se deduce que no existe el grado del polinomio nulo. En consecuencia, todo polinomio de grado cero, es un elemento no nulo de $\mathbb{K}$.

Veamos algunos ejemplos de polinomios con coeficientes complejos, en una indeterminada x:

$p(x) = 2x^5 - 4x^3 - 2x + 10$. Si bien, los coeficientes son todos enteros, como sabemos que $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $p \in \mathbb{C}[x]$, gr(p) = 5, su coeficiente principal es 2 y su término independiente es 10.

$q(x) = \frac{2}{5}x^4 + 0x^8 - x$. Se puede observar que todos los coeficientes de q son racionales, pero como $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $q \in \mathbb{C}[x]$, gr(q) = 4, su coeficiente principal es $\frac{2}{5}$ y su término independiente es 0.

$s(x) = -\sqrt{3} + 2x$. Vemos que 2, $-\sqrt{3} \in \mathbb{R} \subset \mathbb{C}$, de donde $s \in \mathbb{C}[x]$, gr(r) = 1, su coeficiente principal es 2 y su término independiente es $-\sqrt{3}$.

$t(x) = x^7 - 5 + i$. Como $1, -5 + i \in \mathbb{C}$, resulta que $t \in \mathbb{C}[x]$, $gr(t) = 7$, t es mónico y su término independiente es $-5 + i$.

Relación de igualdad en $\mathbb{K}[x]$

Dados, $p, q \in \mathbb{K}[x]$, tales que sus coeficientes son $a_1, \ldots, a_n$ y $b_{1, \ldots,} b_m$, respectivamente, $m, n \in \mathbb{N}_0$ tales que $n \leq m$. Entonces:

$$p = q \Leftrightarrow gr(p) = gr(q) \wedge a_i = b_i, \forall\ i = 0, \ldots, n.$$

Operaciones en $\mathbb{K}[x]$

Suma y multiplicación

Dados, $p, q \in \mathbb{K}[x]$, tales que $gr(p) = n$ y $gr(q) = m$ y, además:

$$p(x) = \sum_{i=0}^{n} a_i x^i \text{ y } q(x) = \sum_{k=0}^{m} b_k x^k$$

Acordaremos que $(p + q)(x) = p(x) + q(x)$ y que $(p.q)(x) = p(x).q(x)$.

Usando los axiomas de operatividad, puede concluirse que:

$$(p + q)(x) = \sum_{j=0}^{h} (a_j + b_j) x^j$$

donde $gr(p + q) = h = \text{máx}\,\{gr(p), gr(q)\}$.

Análogamente, usando los axiomas antes mencionados, se verifica que:

$$(p.q)(x) = \sum_{j=0}^{n+m} c_j x^j$$

donde, para cualquier $0 \leq j \leq n + m$, c_j está dado por la suma siguiente:

$$c_j = \sum_{t=0}^{j} a_{j-t} b_t$$

siendo, además, $gr(p.q) = gr(p) + gr(q)$.

Por otra parte, si $gr(q) = 0$ (es decir, $q \in \mathbb{K} - \{0\}$), el producto p.q es:

$$(pq)(x) = \sum_{i=0}^{n} q a_i x^i$$

con $gr(pq) = gr(p)$, obviamente.

<u>Teorema 1</u>: Los únicos polinomios invertibles en $\mathbb{K}[x]$, son los de grado cero.

Demostración: Sea $p \in \mathbb{K}[x] - \{0\}$. Supongamos que existe $q \in \mathbb{K}[x] - \{0\}$, tal que $p.q = 1$.

Entonces, $gr(p.q) = gr(1) = 0$ es decir, $gr(p) + gr(q) = 0$, de donde resulta que $gr(p) = -gr(q)$.

Como $gr(p), gr(q) \in \mathbb{N}_0$, $gr(p) \geq 0$ y $-gr(q) \leq 0$. Luego: $0 \leq gr(p) = -gr(q) \leq 0$ de donde debe ser $gr(p) = 0$, por propiedad antisimétrica del orden en $\mathbb{R}$.

Potencias n – ésimas de un binomio

Sean dos monomios $p(x) = ax^n$ y $q(x) = bx^m$, con $a, b \in \mathbb{K}$ y $m,n \in \mathbb{N}_0$, entonces, por el teorema del binomio de Newton, se tiene que $\forall\ h \in \mathbb{N}$:

$$(p+q)^h = \sum_{k=0}^{h} \binom{h}{k} p^{h-k} q^k$$

División de polinomios

Dados, $p, q \in \mathbb{K}[x]$, tales que $q \neq 0$, $gr(p) = n$ y $gr(q) = m$ y, además:

$$p(x) = \sum_{i=0}^{n} a_i x^i \text{ y } q(x) = \sum_{k=0}^{m} b_k x^k$$

Entonces, existen y son únicos dos polinomios $c, r \in \mathbb{K}[x]$ tales que $p = cq + r$, con $r = 0 \vee gr(r) < gr(q)$. En general, a p se lo llama dividendo, a q divisor, a c cociente y a r resto, de la división de p por q (Nótese la similitud de esta proposición con el algoritmo de la división en $\mathbb{Z}$. Precisamente, esta proposición se conoce con el nombre de algoritmo de la división en $\mathbb{K}[x]$).

Si bien no haremos la demostración formal del algoritmo, veamos cómo utilizarlo para hallar el cociente y el resto de la división de p por q. Para ello, distingamos dos casos:

1) Si $gr(p) < gr(q)$. En ese caso, $p =$[8] $0 + p =$[9]$0.q + p$. Como $gr(p) < gr(q)$, haciendo $c = 0$ y $r = p$, hemos obtenido el cociente y el resto buscados.

2) Si $gr(p) = n \geq gr(q)$ y p y q son los polinomios dados al presentar los polinomios suma y producto, entonces, disponemos ambos polinomios, ordenando sus términos en orden decreciente de los subíndices de sus coeficientes, en una disposición similar a la de la división de números enteros:

$$\begin{array}{l|l} a_n x^n + a_{n-1} \quad x^{n-1} + \ldots + a_{n-m}\, x + a_0 & b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0 \\ \hline & \frac{a_n}{b_m} x^{n-m} \end{array}$$

Como $gr(q) = m \leq n = gr(p)$, $b_m \neq 0 \neq a_n$, luego $\frac{a_n}{b_m} \in \mathbb{K} - \{0\}$ y $\frac{a_n}{b_m}\, x^{n-m} \in \mathbb{K}[x]$.

Luego, si $c_1(x) = \frac{a_n}{b_m}\, x^{n-m}$, calculamos $c_1.q$ y $r_1 = p - c_1.q = p + c(-q)$. Si resulta que $r_1 = 0 \vee gr(r_1) < gr(q)$, c_1 y r_1 son el cociente y el resto buscados.

[8] Por axioma O2
[9] Poe axioma O8

En caso contrario ($r_1 \neq 0 \wedge gr(r_1) \geq gr(q)$), iteramos el procedimiento (usando como dividendo a r) k veces, hasta hallar c_k y r_k tales que $r_k = 0 \vee gr(r_k) < gr(q)$. En ese caso, $c_1 + .. + c_k$ y r_k son el cociente y el resto, respectivamente, buscados.

Vemos que, en este caso, el coeficiente principal de c es $\frac{a_n}{b_m} \neq 0$ y que gr(c) = = gr(p) – gr(q).

Veamos a continuación ejemplos: Sean $p(x) = 3x^4 - 2x + 1$, $q(x) = 2x^2 + 4x - 2$ y $s(x) = x - 3$.

Si queremos hallar el cociente y el resto de s dividido p, como gr(s) < gr(p), tenemos que c = 0 y r = s.

Busquemos ahora el cociente y resto de dividir p por q: por lo que dijimos antes, $c_1(x) = \frac{3}{2}x^2$, de donde, $c_1(x).q(x) = 3x^4 + 6x^3 - 3x^2$. Finalmente, obtenemos $r_1(x) = p(x) - c_1(x).q(x) = -6x^3 + 3x^2 - 2x + 1$.

Como $gr(r_1) > gr(q)$, se halla $c_2(x) = -3x$. Luego, $c_2(x).q(x) = -6x^3 - 12x^2 + 6x$. Se tiene pues, que $r_2(x) = r_1(x) - c_2(x).q(x) = 15x^2 - 8x + 1$.

Como $gr(r_2) = gr(q)$, hallamos $c_3(x) = \frac{15}{2}$ con lo cual $c_3(x).q(x) = 15x^2 + 30x - 15$ y $r_3(x) = r_2(x) - c_3(x).q(x) = -38x + 16$.

Como $gr(r_3) < gr(q)$, podemos afirmar que $c(x) = c_1(x) + c_2(x) + c_3(x)$ es decir, que $c(x) = \frac{3}{2}x^2 - 3x + \frac{15}{2}$ y que $r(x) = r_3(x) = -38x + 16$.

En cambio, si dividimos q por s, se obtiene que c(x) = 2x + 10 y r = 28.

Cuando como en el ejemplo anterior, el divisor es de grado 1, al hacer la división de p por q, se obtiene que gr(c) = gr(p) – 1. Además, como el algoritmo afirma que $r = 0 \vee gr(r) < gr(q) = 1$, en este caso resulta $r = 0 \vee gr(r) = 0$.

Si el divisor q, además es mónico, tal que $q(x) = x + b_0$, el coeficiente principal de c es a_n es decir, el coeficiente principal del dividendo (p). Luego: $p(x) = c(x).(x + b_0) + r$, con $r \in \mathbb{K}$.

Esto es lo que dio origen a una regla, llamada **regla de Ruffini**, que permite obtener el cociente y el resto de la división, en forma más sencilla, en el caso particular en que el divisor es mónico y de grado 1.

Si los coeficientes del polinomio cociente, c, son $c_{n-1}, c_{n-2}, \ldots, c_0$. Entonces:

1) Se escriben en una misma fila todos los coeficientes del dividendo (aún los que sean 0), ordenándolos en forma decreciente como al hacer la división.

2) Se traza un ángulo recto y se escribe el opuesto del término independiente del divisor, tal como se indica a continuación:

$$\begin{array}{c|lllll} & a_n & a_{n-1} & \ldots\ldots\ldots & a_k & \ldots\ldots\ldots \; a_0 \\ -b_0 & & & & & \\ \hline & & & & & \end{array}$$

3) En la primera columna, debajo de la recta horizontal, se coloca c_{n-1}, que ya dijimos que es $c_{n-1} = a_n$, como se indica a continuación:

$$\begin{array}{c|lllll} & a_n & a_{n-1} & \ldots\ldots\ldots & a_k & \ldots\ldots\ldots \; a_0 \\ -b_0 & & & & & \\ \hline & a_n = c_{n-1} & & & & \end{array}$$

4) Para $0 \leq k < n - 1$, se calcula $c_k = a_{k+1} - b_0.c_{k+1}$. Es decir, se tiene que:

$$
\begin{array}{r|cccccc}
 & a_n & a_{n-1} & \ldots\ldots\ldots\ldots\ldots\ldots.. & a_{k+1} & \ldots\ldots\ldots\ldots\ldots. & a_1 \quad a_0 \\
-b_0 & & -b_0.c_{n-1} & \ldots\ldots\ldots\ldots\ldots & -b_0.c_{k+1} & \ldots\ldots\ldots\ldots & -b_0.c_1 \\
\hline
 & c_{n-1} & c_{n-2} = a_{n-1} - b_0.c_{n-1} & \ldots\ldots c_k = a_{k+1} - b_0.c_{k+1} & \ldots & c_0 = a_1 - b_0.c_1 &
\end{array}
$$

5) Finalmente, se halla $r = a_0 - b_0.c_0.$

6) Luego, el cociente es $c(x) = a_n x^{n-1} + c_{n-2} x^{n-2} + \ldots + c_0.$

Para ejemplificar el uso de la regla, usemos los polinomios q y s dados como ejemplos anteriormente: $q(x) = 2x^2 + 4x - 2$ y $s(x) = x - 3$.

Entonces:

Disponemos en una fila los coeficientes de q y en el ángulo el opuesto del término independiente de s.

$$
\begin{array}{r|ccc}
 & 2 & 4 & -2 \\
3 & & & \\
\hline
 & & &
\end{array}
$$

Como el cociente es de grado gr(q) – 1, el coeficiente principal es $c_1 = 2$ y el término independiente $c_0 = 2.3 + 4 = 10$.

$$
\begin{array}{r|ccc}
 & 2 & 4 & -2 \\
3 & & 6 & \\
\hline
 & 2 & 10 &
\end{array}
$$

Finalmente, se calcula el resto de la división, haciendo $r = 10.3 - 2 = 28$. Es usual recuadrar el resto, al usar la regla, tal como se ve a continuación.

$$
\begin{array}{r|ccc}
 & 2 & 4 & -2 \\
3 & & 6 & 30 \\
\hline
 & 2 & 10 & \boxed{28}
\end{array}
$$

Entonces, se tiene que $c(x) = 2x + 10$ y el resto es $r = 28$.

Finalmente, decimos que si el resto de la división de p por $q \neq 0$ es el polinomio nulo, **q divide a p** o, lo que es lo mismo, **q es un divisor de p**. En este caso, utilizamos la misma notación que en el de los números enteros: $q|p$.

Funciones polinómicas

Sea $p \in \mathbb{K}[x]$ de grado $n \in \mathbb{N}_0$ y coeficientes $a_n, \ldots, a_0$. Definimos la **función polinómica asociada a p, de grado n**, como sigue:

$$f_p : \mathbb{K} \longrightarrow \mathbb{K} / f_p(k) = \sum_{i=0}^{n} a_i k^i$$

Por leyes de cierre de la suma y del producto en $\mathbb{K}$, cualquiera sea $p \in \mathbb{K}[x]$, f_p es función.

Observaciones:

1) La función lineal f: $\mathbb{R} \to \mathbb{R}$ / $f(x) = ax + b$, donde a y b son números reales fijos es una función polinómica de grado 1, si $a \neq 0$ o de grado 0, si $a = 0$ (función constante).

2) La función cuadrática g: $\mathbb{R} \to \mathbb{R}$ / $g(x) = ax^2 + bx + c$, donde a, b y c son números reales fijos y $a \neq 0$ es una función polinómica de grado 2.

Para cada $k \in \mathbb{K}$, a $f_p(k)$ lo llamamos **valor numérico de p en k**, o **especialización de p en k**. Al valor numérico de p en $k \in \mathbb{K}$ se lo denotará, simplemente, con p(k) en vez de con $f_p(k)$.

Es trivial que el valor numérico de un polinomio p de grado cero en cualquier $k \in \mathbb{K}$, es $p \in \mathbb{K}$ y que el valor numérico del polinomio nulo en todo $k \in \mathbb{K}$, es cero.

Dados los polinomios p, q, s, t, w, $v \in \mathbb{K}[x]$ tales que $p = t$, $p = q+s$ y $p = vw$, las funciones polinómicas asociadas f_p, f_t, f_{q+s} y f_{vw} son iguales, de donde se tiene que $p(k) = t(k)$, $p(k) = q(k) + s(k)$ y $p(k) = v(k).w(k)$, $\forall k \in \mathbb{K}$.

Teorema del Resto

Sean p, $q \in \mathbb{K}[x]$ tales que $q(x) = x + a$. Entonces, el resto de la división de p por q es $r = p(-a)$.

Demostración: Sean p, $q \in \mathbb{K}[x]$ tales que $q(x) = x + a$. Luego, por algoritmo de división, $p(x) = c(x).(x + a) + r$, con $gr(c) = gr(p) – 1$ y $gr(r) = 0$.

Entonces: $p(-a) = c(-a).(-a + a) + r = c(-a).0 + r = 0 + r = r$.

Observación MUY importante:

A partir de este momento, podemos trabajar con tres objetos matemáticos muy diferentes:

1) **Un polinomio** con coeficientes en un cuerpo $\mathbb{K}$, que es un elemento de $\mathbb{K}[x]$, que cumple los axiomas de construcción dados al principio de este capítulo. Por ejemplo, el polinomio $p \in \mathbb{C}[x]$ tal que $p(x) = x^3 – 2x + 5$.

2) **Una función polinómica asociada a un polinomio p**, a la que denotamos con f_p NO es un polinomio, sino una función. Por ejemplo, la función real de una variable real f_p: $\mathbb{R} \to \mathbb{R}$ / $f_p(t) = t^3 – 8$ es la función polinómica de grado 3 asociada al polinomio $p(x) = x^3 – 8$.

3) **Una ecuación polinómica** $p(k) = f_p(k) = a \in \mathbb{K}$, que es una igualdad en la cual se desconoce el valor de la o las preimágenes de a por la función f_p. Para el ejemplo dado, es una ecuación polinómica de tercer grado la igualdad siguiente: $f_p(t) = t^3 – 8 = 0$. Dado que es una función real de variable real, existe una única preimagen de 0 que es 2 (puesto que $2^3 – 8 = 8 – 8 = 0$). Luego la

ecuación tiene una única solución real, y su conjunto solución es S = {2} $\subset \mathbb{R}$. En cambio, si consideramos la función f_p como una función compleja de una variable compleja, la misma admite tres soluciones complejas: las raíces cúbicas de 8 (las cuales pueden calcularse de la forma indicada al estudiar números complejos), de donde, el correspondiente conjunto solución está dado por S = {<2, 0>, <2, $\frac{2}{3}\pi$>, <2, $\frac{4}{3}\pi$>}

Raíces de un polinomio

Sean p $\in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Decimos que α es raíz de p si, y sólo si, $p(\alpha) = 0$.

Así pues, hallar las raíces de un polinomio p es equivalente a hallar los valores de $\alpha \in \mathbb{K}$ tales que $p(\alpha) = f_b(\alpha) = 0$, que es lo que se suele llamar "resolver la ecuación polinómica $p(\alpha) = 0$".

Ejemplos:

1) Dado $p(x) = x^4 - 1 \in \mathbb{C}[x]$, vemos que p(i) = p(-i) = p(1) = p(-1) = 0, con lo cual, -i, i, -1 y 1 son cuatro raíces de p. El conjunto solución de la ecuación polinómica $x^4 - 1 = 0$ es pues, S = {-i, i, -1, 1}.
2) Si $q(x) = x^2 - 5 \in \mathbb{C}[x]$, vemos que sus raíces son $+\sqrt{5}$ y $-\sqrt{5}$, puesto que $q(+\sqrt{5}) = (+\sqrt{5})^2 - 5 = 5 - 5 = 0 = 5 - 5 = (-\sqrt{5})^2 - 5 = q(-\sqrt{5})$.
3) Sea $s(x) = x^3 + 3x^2 + 3x + 1 =$[10]$(x + 1)^3 \in \mathbb{C}[x]$. Entonces, -1 es raíz de s puesto que s(-1) = 0.
4) Si $t(x) = 2x^2 + 6x = 2x.(x + 3) \in \mathbb{C}[x]$, es obvio que 0 y -3 son raíces de t.
5) Las únicas raíces del polinomio $w(x) = x^2 + 1$, son i y – i.

<u>Teorema 2</u>: Sean p $\in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Entonces:

$$p(\alpha) = 0 \Leftrightarrow (x - \alpha) | p(x)$$

<u>Demostración</u>: Sean p $\in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$. Entonces:

Si $p(\alpha) = 0$, por el teorema del resto, el resto de dividir p por $x - \alpha$ es el polinomio nulo, de donde, por definición, $x - \alpha$ es un divisor de p.

Recíprocamente, si $(x - \alpha)|p(x)$, el resto de dividir p por $x - \alpha$ es el polinomio nulo, de donde, por el teorema del resto, $p(\alpha) = p(-(-\alpha)) = 0$.

Raíces múltiples de un polinomio

Sean p $\in \mathbb{K}[x]$, k $\in \mathbb{N}$ y $\alpha \in \mathbb{K}$. Decimos que α es raíz múltiple de orden de multiplicidad k de p si, y sólo si, $(x - \alpha)^k | p \wedge (x - \alpha)^{k+1} \nmid p$.

En el ejemplo 3, -1 es raíz múltiple de orden 3 de p.

Cuando el orden de multiplicidad de una raíz α es 1, se dice que α es raíz simple, y si dicho orden es 2, que es una raíz doble.

[10] Por el teorema del binomio de Newton

Proposición: Todo polinomio $p \in \mathbb{K}[x]$ de grado n tiene, a lo sumo, n raíces distintas.

Aceptaremos esta proposición como verdadera, sin demostrarla.

Polinomios con coeficientes complejos

A partir de este momento, todos los polinomios con los que trabajaremos son polinomios con coeficientes complejos.

Enunciado del Teorema Fundamental del Algebra (TFA)

Todo polinomio con coeficientes complejos, admite en $\mathbb{C}$ al menos una raíz.

Este teorema, que admitimos sin demostración, nos permite afirmar que $\mathbb{C}$ es un cuerpo **algebraicamente cerrado**, característica que no tienen los cuerpos $\mathbb{R}$ y $\mathbb{Q}$, lo cual se pone en evidencia al analizar los siguientes ejemplos:

Ya vimos que el polinomio del ejemplo 2 admite como raíces a las raíces cuadradas de 5, que son números irracionales, a pesar de que sus coeficientes son números racionales (1 y 5). Por ello, $\mathbb{Q}$ no es algebraicamente cerrado.

De la misma manera, en el ejemplo 5 observamos que las únicas raíces de $w(x) = x^2 + 1$ son i y –i, con lo cual, a pesar de que sus coeficientes son reales, w no admite ninguna raíz real; por ello $\mathbb{R}$ tampoco es algebraicamente cerrado.

Teorema de Gauss

Sean s un polinomio con coeficientes enteros $a_n, \ldots, a_0$, $n > 0$ y $a_n \neq 0 \neq a_0$. **Si** s admite como raíz a $\frac{p}{q} \in \mathbb{Q}$, con p y q coprimos, **entonces**, $p|a_0 \wedge q|a_n$.

Demostración: Sean $\frac{p}{q} \in \mathbb{Q}$ y s un polinomio de coeficientes enteros tal que

$$s(x) = \sum_{i=0}^{n} a_i x^i$$

con $a_n \neq 0 \neq a_0$ y $s(\frac{p}{q}) = 0$. Entonces, por propiedad distributiva de la potenciación con respecto al producto de números reales:

$$s\left(\frac{p}{q}\right) = \sum_{i=0}^{n} a_i \frac{p^i}{q^i} = 0$$

de donde, multiplicando ambos miembros por q^n resulta:

$$q^n \sum_{i=0}^{n} a_i \frac{p^i}{q^i} = \sum_{i=0}^{n} a_i p^i q^{n-i} = 0 \ (*)$$

con lo cual se tiene, por un lado:

$$\sum_{i=1}^{n} a_i p^i q^{n-i} = -a_0 q^n$$

de donde, por propiedad distributiva del producto con respecto a la suma en $\mathbb{Z}$:

$$p\sum_{i=1}^{n} a_i p^{i-1} q^{n-i} = -a_0 q^n$$

Por cierre de la suma y el producto en $\mathbb{Z}$, la suma que multiplica a p, en el primer miembro, es un cierto número entero h. Luego: $p.h = -a_0.q^n$. Ahora bien, tenemos pues que $p|-a_0.q^n$, pero como p y q son coprimos, $p \nmid q^n$ de donde, debe ser $p|-a_0$ y, en consecuencia, p divide a a_0.

Por otra parte, de (*) se tiene que:

$$\sum_{i=0}^{n-1} a_i p^i q^{n-i} = -a_n p^n$$

Razonando en forma similar, resulta que existe $h' \in \mathbb{Z}$ tal que $q.h' = -a_n.p^n$. Es decir, que hemos probado que $q|-a_n.p^n$; nuevamente, como p y q son coprimos, q no puede ser un divisor de p^n, luego debe ser divisor de $-a_n$ y de a_n.

<u>Teorema 3</u>: Todo polinomio con coeficientes reales, si admite como raíz a un número complejo, también admite como raíz a su conjugado.

<u>Demostración</u>: Sea p un polinomio de coeficientes reales y de grado n > 0, tal que admite como raíz a $z \in \mathbb{C}$. Entonces:

$$p(z) = \sum_{i=0}^{n} a_i z^i = 0 \; (**)$$

Luego, se tiene que:

$$p(\overline{z}) = \sum_{i=0}^{n} a_i \overline{z}^i =^{11} \sum_{i=0}^{n} a_i \overline{z^i} =^{12} \sum_{i=0}^{n} \overline{a_i}\,\overline{z^i} =^{13} \sum_{i=0}^{n} \overline{a_i z^i} =^{14} \overline{\sum_{i=0}^{n} a_i z^i} =^{**} \overline{0} =^{15} 0$$

Factorización de polinomios con coeficientes complejos

Factorizar un polinomio es, sencillamente, expresarlo como el producto de dos o más factores.

Existen diversas técnicas para factorizar un polinomio, a las que tracionalmente se las llamó **casos de factoreo.** Veamos sucintamente, de que se tratan:

[11] El conjugado de la potencia n - ésima de un número complejo, es su conjugado a la n.
[12] Todo número real es igual a su conjugado.
[13] El conjugado del producto de dos números complejos, es el producto de sus conjugados.
[14] El conjugado de la suma de dos números complejos, es la suma de los conjugados.
[15] Todo número real coincide con su conjugado.

Sean $n, m \in \mathbb{N}$, con $m > 1$, $p, p_o, p_1, p_2, \ldots p_m, q, r, s, t, k, a^n \in \mathbb{C}[x]$, tales que p_i es un monomio, para todo $i = 0, 1, \ldots, m$, $t = p_1 + p_2$, $s = p_1 - p_2$ y, finalmente, r es:

$$r = \sum_{i=0}^{m} p_i$$

Se presentan distintos casos:

<u>Caso 1</u> (Factor común): Si p es tal que:

$$p = \sum_{i=0}^{m} qp_i \ =^{16} q \sum_{i=0}^{m} p_i \ = qr$$

<u>Ejemplo</u>: $p(x) = 12x^5 – 4x^3 + 10x = 2x.(6x^4 – 2x^2 + 5)$

<u>Caso 2</u> (Factor común por grupos): Si p es tal que:

$$p = \sum_{i=0}^{m} qp_i + \sum_{i=0}^{m} kp_i =^{11} q \sum_{i=0}^{m} p_i + k \sum_{i=0}^{m} p_i =^{11} (q+k) \sum_{i=0}^{m} p_i = (q+k).s$$

<u>Ejemplo</u>: $q(x) = x^5 + x^3 + 4x^2 + 4 = x^3.(x^2 + 1) + 4.(x^2 + 1) = (x^2 + 1)(x^3+ 4)$.

<u>Caso 3</u> (Trinomio del cuadrado perfecto): Si p es tal que:

$$p = p_1^2 + 2p_1p_2 + p_2^2 = ^{17}(p_1 + p_2)^2 = t^2 = t.t$$

<u>Ejemplo</u>: $s(x) = x^6 – 6x^3 + 9 = (x^3)^2 + 2.(-3)x^3 + (-3)^2 = (x^3 – 3)^2$.

<u>Caso 4</u> (Cuatrinomio del cubo perfecto): Si p es tal que:

$$p = p_1^3 + 3p_1^2p_2 + 3p_1p_2^2 + p_2^3 =^{17} (p_1 + p_2)^3 = t^3 = t.t.t$$

<u>Ejemplo</u>: $t(x) = x^6 + 6x^5 + 12x^4 + 8x^3 = (x^2)^3 + 3.2.x^4.x + 3.4.x^2.x^2 + 2^3.x^3 =$
$= (x^2)^3 + 3(x^2)^2(2x) + 3.2^2.x^2.x^2 + 2^3.x^3 = (x^2)^3 + 3(x^2)^2(2x) + 3.(2.x)^2.x^2 + (2x)^3 =$
$= (x^2 + 2x)^3$

<u>Caso 5</u> (Diferencia de cuadrados): Si p es tal que: $p = p_1^2 - p_2^2$, entonces, vemos que $p = p_1^2 - p_2^2 = p_1^2 + p_1.p_2 - p_1.p_2 - p_2^2 = p_1(p_1 + p_2) - p_2(p_1 + p_2) =$
$= (p_1 + p_2). (p_1 - p_2) = s.t.$

<u>Ejemplo</u>: $v(x) = x^4 – 4 = (x^2)^2 – 2^2 = x^4 + 2x^2 – 2x^2 – 4 = x^2(x^2 + 2) - 2(x^2 + 2) =$
$= (x^2 + 2) (x^2 - 2) = (x^2 + 2).(x^2 - \left(\sqrt{2}\right)^2) = (x^2 + 2)(x + \sqrt{2})(x - \sqrt{2})$

<u>Caso 6</u> (Divisibilidad por la suma o diferencias de las bases):

Si p es tal que: $p = p_1^n - a^n$, p es divisible por la diferencia de las bases es decir, por $p_1 – a$.

[16] Axioma O5.
[17] Teorema del binomio de Newton.

En cambio, si p es tal que: $p = p_1^n + a^n$, $p_1 + a|\ p$, sólo si n es impar. En efecto, si $p(x) = x^2 + 16$, se tiene que el resto de dividir p por x + 2 es 20[18] es decir, $x + 2 \nmid p$.

Teorema de descomposición factorial

Hemos visto que existen polinomios (como $x^2 + 16$), que no pueden ser factorizados por ninguno de estos métodos. Así pues, como el TFA nos asegura que todo polinomio p de coeficientes complejos admite, al menos, una raíz en $\mathbb{C}$ (α), por el Teorema 2, $(x - \alpha)|\ p$. Si c_1 es tal que $p(x)= c_1(x).(x - \alpha)$, como a su vez, c_1 es un polinomio de coeficientes complejos, nuevamente por el TFA, existe $\beta \in \mathbb{C}$, raíz de c_1, de donde $(x - \beta)|c_1$. Luego, si $c_2 \in \mathbb{C}[x]$ es tal que $c_1(x) = c_2(x). (x - \beta)$, se tiene que $p(x)= c_1(x).(x - \alpha) = c_2(x). (x - \beta).(x - \alpha)$. Si se sigue factorizando c_2, se obtiene un cociente c_3 que, nuevamente, puede ser factorizado, y así sucesivamente.

Por ello, enunciamos el siguiente teorema: Sean p un polinomio de coeficientes complejos, de grado $n \in \mathbb{N}$ y de coeficiente principal a_n. Si los números complejos $\alpha_1, \ldots, \alpha_n$ son n raíces - no necesariamente distintas - de p, entonces, p se puede factorizar como sigue:

$$p(x) = a_n \prod_{i=1}^{n} (x - \alpha_i)$$

Veamos entonces, cómo factorizar el polinomio $p(x) = x^2 + 16$.

En principio, buscamos $z \in \mathbb{C}$ tal que $z^2 + 16 = 0$. Es decir, debemos hallar las raíces cuadradas de -16. Una de dichas raíces es 4i. Entonces, por el Teorema 3 - como s es un polinomio de coeficientes reales - también admite como raíz a -4i, de donde:

$$p(x) = (x - 4i).(x + 4i)$$

Podemos ver que este teorema es, prácticamente, una “fábrica” de polinomios, con sólo fijar de antemano su grado, su coeficiente principal y sus raíces, pueden hallarse los polinomios que se deseen. Veamos algunos ejemplos:

Proponer un polinomio p tal que:

1) Sea de coeficientes reales, mónico, de grado 5 y que admita una raíz doble y una compleja no real.

Entonces, $a_5 = 1$ y, como se pide que sea de coeficientes reales y admita una raíz compleja no real, por el Teorema 3, debe admitir también a su conjugada. Se fija una raíz compleja no real, por ejemplo, 1 + 2i, cuyo conjugado es 1 – 2i. Como se pide, además, una raíz doble, se fija un número cualquiera, por ejemplo, -3. Vemos que, hasta el momento, p tiene 4 raíces. Se elige otra raíz, por ejemplo, 8 y se escribe el polinomio factorizado como sigue:

$$p(x) = (x - 1 - 2i).(x - 1 + 2i).(x + 3)^2.(x - 8)$$

2) Su coeficiente principal sea 2i, admita dos raíces racionales y dos irracionales.

[18] Por el teorema del resto y por ser p(-2) = 20.

En este caso, el grado de p debe ser, como mínimo, 4. Como 1 y 2 son números racionales, $+\sqrt{3}$ y $-\sqrt{5}$ son irracionales, podemos factorizar p como sigue: $p(x) = 2i.(x - 1).(x - 2).(x - \sqrt{3}).(x + \sqrt{5})$. Como no se fija el grado de p, podríamos también escribir: $p(x) = 2i.(x - 1)^2.(x - 2).(x - \sqrt{3}).(x + \sqrt{5})\ (x - 2i)$, por ejemplo (al no ser p de coeficientes reales, no necesariamente $p(-2i) = 0$).

Consideraciones finales

Al definir el conjunto de polinomios con coeficientes en un cuerpo, establecimos que V debe ser un conjunto disjunto con $\mathbb{K}$.

Supongamos ahora que $V = \{x, y\}$; luego, como $V \subset \mathbb{K}[V]$, x e y son dos polinomios. De la misma manera, valen en $\mathbb{K}[V]$ todos los axiomas de construcción y de operatividad, así como también la definición de potenciación dados al inicio de este capítulo.

Además, $x, y \notin \mathbb{K}$, de donde, $x \neq 0 \neq y$; luego, por definición de potenciación, $x^0 = y^0 = 1$ y serán polinomios x^n, y^m, $a.x^n.y^m$ (por axiomas C1, C3 y definición de potenciación), cualesquiera sean n, m $\in \mathbb{N}_0$ y a $\in \mathbb{K}$. Dichos polinomios se llaman, como en el caso de una sola indeterminada, monomios.

Llamemos al último monomio $p(x, y) = a\,.\,x^n.\,y^m$.

Entonces, si a = 0, p es el polinomio nulo; en caso contrario, definimos el grado de p como gr(p) = n + m.

Sean $p_1, \ldots, p_k \in \mathbb{K}[V]$ monomios no nulos . Entonces, podemos expresar a $p \in \mathbb{K}[V]$, como sigue:

$$p(x, y) = \sum_{i=1}^{k} p_i\,(x, y)$$

donde $gr(p) = máx\,\{gr(p_i)\ /\ i = 1, \ldots, k\}$.

<u>Ejemplos</u>: Consideremos los siguientes polinomios en $\mathbb{C}[V]$

$p(x, y) = 2x^2\,y^3 + ix^5 + 4\,x^2\,y^2 - 2 + 5i$. Entonces, gr(p) = 5.

$q(x, y) = 4ix^2 + 2xy - y^2$. Luego, gr(q) = 2.

$s(x, y) = 5xy + 3x^2\,y^2 + 1 - i$; se tiene que gr(s) = 4.

$(p + s)(x, y) = 2x^2\,y^3 + ix^5 + 7x^2\,y^2 + 5xy - 1 + 4i$.

Vemos que gr(p + s) = máx {0, 2, 4, 5} = 5 = máx {gr(p), gr(s)}

$(p.q)(x,y) = -4x^7+2ix^6y - ix^5\,y^2+8ix^4y^3+4x^3y^4 - 2x^2y^5+16ix^4y^2+ 8x^3y^3-4x^2y^4 - (20 + 8i)x^2 - (4 - 10i)xy + (2 - 5i)y^2$.

Puede observarse que gr(p.q) = 7 = 5 + 2 = gr(p) + gr(q).

De la misma manera que lo hecho en $\mathbb{K}[x]$, a cada polinomio $p \in \mathbb{K}[V]$ se lo puede asociar con una función polinómica f_p de $\mathbb{K}^2$ en $\mathbb{K}$. Así pues, para cada elemento $k \in \mathbb{K}$, puede hallarse el valor numérico del polinomio en dicho par, calculando su imagen por la correspondiente función polinómica.

Ejemplos: Sea $p \in \mathbb{C}[V]$ / $p(x, y) = 2x^2 y^3 + ix^5 + 4x^2y^2 – 2 + 5i$. Busquemos su valor numérico en (1, 2):

$$p(1, 2) = 2.1^2.2^3 + i1^5 + 4.1^2.2^2 – 2 + 5i = 16 + i + 16 – 2 + 5i= 30 + 6i.$$

De igual manera, hallemos el valor numérico de p en (2, i):

$$p(2, i) = 2.1^2i^3 +i.2^5 + 4.2^2.i^2 – 2 + 5i = -2i + 32i – 16 – 2 + 5i = -18 + 35i$$

Entonces, una ecuación polinómica con dos incógnitas será una igualdad del tipo $f_p(k, h) = a \in \mathbb{K}$. Resolverla consiste, simplemente, en hallar todos los pares $(k, h) \in \mathbb{K}^2$ que hacen que se cumpla la igualdad.

Dada la ecuación: $x^2 – 4x + y^2 – 2y + 1 = 0$ (1) que proviene de la función polinómica f_p: $\mathbb{R}^2 \to \mathbb{R}$ / $f_p(x, y) = x^2 – 4x + y^2 – 2y + 1$, vemos que, sumando y restando 4 en el primer miembro de (1), se obtiene:

$$x^2 – 4x + 4 + y^2 – 2y + 1 - 4 = 0$$

utilizando el teorema del binomio de Newton, resulta: $(x – 2)^2 + (y – 1)^2 – 4 = 0$. De donde, sumando 4 a ambos miembros, se tiene que: $(x – 2)^2 + (y – 1)^2 = 4$.

Así pues, si consideramos las coordenadas de todos los puntos de la circunferencia con centro en c = (2, 1) y radio 2, todos ellos verifican la igualdad (1) es decir, todos ellos son soluciones de dicha ecuación. Diremos entonces, que la ecuación admite infinitas soluciones y que su conjunto solución es la circunferencia $C(c, 2) \subset \mathbb{C}$, con c = 2 + i (que representamos con el punto de coordenadas (2, 1)).

Bibliografía consultada

Figallo,A.V. (1993). Polinomios y funciones polinómicas. Memorias del 5º Seminario Nacional de Matemática. Nivel Medio. Facultad de Filosofía, Humanidades y Artes de la Universidad Nacional de San Juan. San Juan, Argentina. pp 39 – 48.

De Nápoli, P. (2007). Notas de Algebra I. Polinomios. Versión 0.8.5. Departamento de Matemática de la Facultad de Ciencias Exactas y Naturales – UBA. CABA. Argentina. Disponible en:
http://mate.dm.uba.ar/~pdenapo/apuntes-algebraI/polinomios.pdf

Lezama, O. (2014). Cuadernos de Algebra Nº2. Anillos. Departamento de Matemática. Facultad de Ciencias de la Universidad Nacional de Colombia. Bogotá, Colombia. Disponible en:
http://ciencias.bogota.unal.edu.co/fileadmin/content/seminarios/sac2/cuadernos/anillos.pdf