Álgebra I. 525140 - DIM - CFM
5 de julio de 2021
Prof.: Isabel Donoso, Anahí Gajardo, Jorge Moya, Alejandra Pérez
Cinthya Rivas, Mónica Selva, Filip Thiele, Gladis Torres

Polinomios en $\mathbb{R}$ y $\mathbb{C}$

La solución de ecuaciones cuadráticas (de la forma $a\,x^2 + b\,x + c = 0$ con a, b, $c \in \mathbb{R}$), cúbicas (de la forma $a\,x^3 + b\,x^2 + c\,x + d = 0$ con a, b, c, $d \in \mathbb{R}$), cuárticas, ... fue objeto de estudio por más de 300 años.

Ya sabemos que las soluciones a la ecuación $a\,x^2 + b\,x + c = 0$ con a, b, $c \in \mathbb{R}$ son

$$\frac{-b + \sqrt{b^2 - 4\,a\,c}}{2\,a}, \tag{1}$$

donde $\sqrt{b^2 - 4\,a\,c}$ representa el conjunto de los números complejos z que satisfacen $z^2 = b^2 - 4\,a\,c$.

Los valores en (1) pueden determinarse realizando operaciones aritméticas entre los coeficientes de la ecuación y calculando raíces cuadradas de números complejos. Fórmulas similares se encuentran para las ecuaciones cúbicas y cuárticas, pero no para, por ejemplo, ecuaciones de la forma

$$a\,x^5 + b\,x^4 + c\,x^3 + d\,x^2 + e\,x + f = 0, \qquad \text{con } a \in \mathbb{R}, a \neq 0. \tag{2}$$

Este resultado fue demostrado por Niels Abel (1802 – 1829), un matemático noruego, que murió de tubercolosis a los 27 años de edad. Lo que Abel demostró es que no es posible calcular las soluciones de una ecuación como (2) realizando sólo operaciones aritméticas entre sus coeficientes y calculando radicales. Sin embargo, esto no significa que ninguna ecuación de grado 5 pueda resolverse de esta forma, por ejemplo, ya sabemos cuáles son las soluciones, en $\mathbb{C}$, de la ecuación $x^5 = 1$. Galois fue quién logró caracterizar qué tipo de ecuaciones como (2) son tales que sus soluciones pueden encontrarse realizando operaciones aritméticas entre los coeficientes y calculando radicales.

Una función que a cada $x \in \mathbb{C}$ le haga corresponder el número complejo $a\,x^2 + b\,x + c$, se denomina polinomio de grado menor o igual que 2.

Estas funciones son cruciales en ingeniería ya que son las únicas que se pueden representar en un computador, y todas las demás funciones se calculan por medio de aproximaciones basadas en sumas y multiplicaciones.

Funciones como ésta son el objeto de estudio de este capítulo.

Definición 1. Polinomio y polinomio nulo. Sean $n \in \mathbb{N} \cup \{0\}$ y $a_0, a_1, \ldots, a_n \in \mathbb{K}$, donde $\mathbb{K}$ denota ya sea $\mathbb{R}$ o $\mathbb{C}$.

1. Un *polinomio con coeficientes en* $\mathbb{K}$ es una función $p : \mathbb{K} \longrightarrow \mathbb{K}$ definida por

$$\forall\, x \in \mathbb{K} : \quad p(x) = a_0 + a_1\, x + a_2\, x^2 + \ldots + a_n\, x^n = \sum_{k=0}^{n} a_k\, x^k, \tag{3}$$

   donde $a_0, a_1, \ldots, a_n \in \mathbb{K}$ son constantes.

   Es decir, el valor de $p(x)$, para cada $x \in \mathbb{K}$, $p(x)$ se puede escribir como suma de potencias naturales de x multiplicadas por constantes más un término constante.

   Los números a_0, a_1, $\ldots$, a_n se denominan coeficientes de p, de los cuales

   - al que no está multiplicado por x (o multiplicado por x^0), que se ha denotado por a_0, se le llama *término independiente*, *término libre* o *constante*,
   - El *grado* del polinomio corresponde a la potencia de x más grande presente el el polinomio y se denota $\mathrm{gr}(p)$, es decir:

$$\mathrm{gr}(p) = \text{máx}\{i \in \{0, \ldots, n\} \;:\; a_i \neq 0\} \quad \text{o} \quad gr(p) = -\infty \text{ si } p \equiv 0.$$

     El coeficiente que acompaña a la potencia más grande se denomina *coeficiente principal*, por ejemplo, si $a_n \neq 0$ entonces $\mathrm{gr}(p) = n$ y a_n es el coeficiente principal de p.

2. Al conjunto de todos los polinomios con coeficientes en $\mathbb{K}$ se le representa por $\mathcal{P}(\mathbb{K})$. Además denotaremos por $\mathcal{P}_n(\mathbb{K})$ con $n \in \mathbb{N} \cup \{0\}$ al conjunto formado por todos los polinomios de grado menor o igual que n y coeficientes en $\mathbb{K}$.

3. El *polinomio nulo* es aquel que vale 0 en todas partes, cuyos coeficientes son todos nulos. A este polinomio lo denotaremos por la letra griega θ, es decir, la función $\theta : \mathbb{K} \to \mathbb{K}$ definida por $\theta(x) = 0$, para todo $x \in \mathbb{K}$, es denominado polinomio nulo.

   Como vimos arriba su grado se considera como $-\infty$. Asignar este símbolo será conveniente, como veremos más abajo, si es que adoptamos las siguientes convenciones para su interacción con los números enteros.

   - $-\infty = -\infty$
   - $\forall i \in \mathbb{Z}, -\infty < i$
   - $-\infty - \infty = -\infty$
   - $\forall i \in \mathbb{Z}, i - \infty = -\infty + i = -\infty$

   No deben interpretarse estas convenciones con sentido numérico, si no como meros artilugios para facilitar la escritura de los teoremas y reglas de cálculo que aprenderemos en este capítulo.

Ejemplo 2. 1. La función $p : \mathbb{R} \longrightarrow \mathbb{R}$ tal que $\forall x \in \mathbb{R} \ : \ p(x) = 2\,x + 1$ es un polinomio en $\mathcal{P}(\mathbb{R})$, $\mathrm{gr}(p) = 1$, su coeficiente principal es 2 y su término libre es 1.

2. La función $u : \mathbb{C} \longrightarrow \mathbb{C}$ tal que $\forall x \in \mathbb{C} \ : \ u(x) = 2\,x + 1$ es un polinomio en $\mathcal{P}(\mathbb{C})$, $\mathrm{gr}(p) = 1$, su coeficiente principal es 2 y su término libre es 1.

3. La función $q : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $q(x) = 5\,i$ para todo $x \in \mathbb{C}$ cumple que $q \in \mathcal{P}(\mathbb{C})$ y $\mathrm{gr}(q) = 0$, de donde se puede afirmar que $q \in \mathcal{P}_0(\mathbb{C})$. Su coeficiente principal es $5i$ y coincide con su término libre: $5i$.

   Este polinomio es una función constante idénticamente igual a $5i$ al igual que todas las funciones del conjunto $\mathcal{P}_0(\mathbb{C})$.

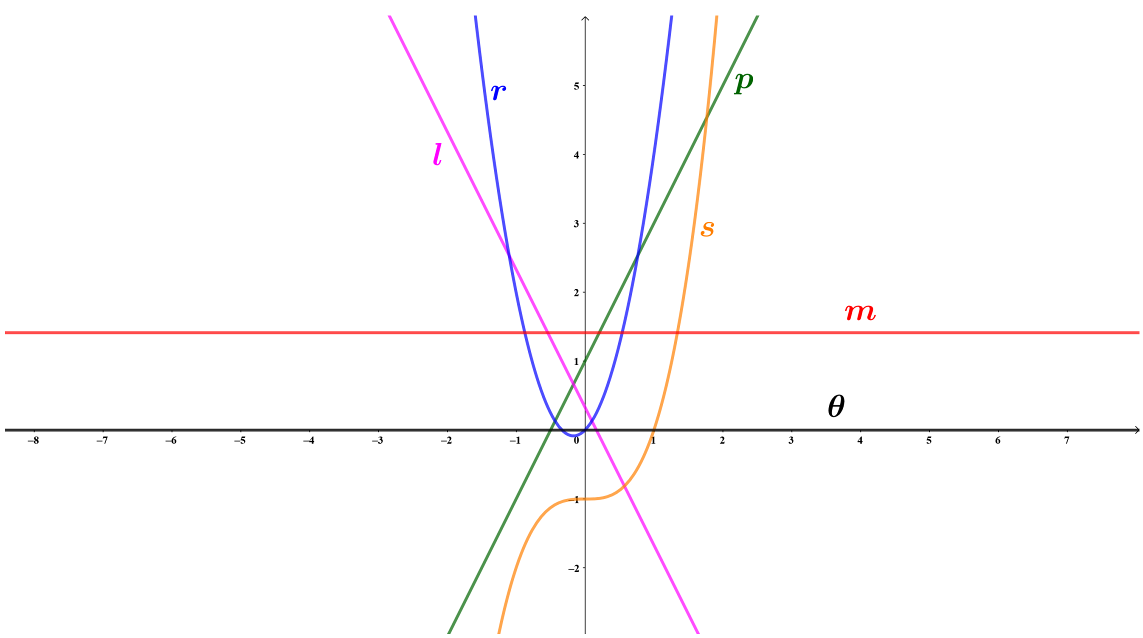
4. La función $t : \mathbb{C} \longrightarrow \mathbb{C}$ tal que para cada $x \in \mathbb{C}$, $t(x) = x + 5\,x^7 - x^2$ es un polinomio de grado 7 con coeficientes complejos. El coeficiente principal de t es 5 y su término libre es 0. Si quisiéramos llevarlo a su forma estándar lo escribiríamos como sigue:

$$t(x) = 0 + 1x - 1x^2 + 0x^3 + 0x^4 + 0x^5 + 0x^6 + 5\,x^7,$$

   en otras palabras: $a_0 = 0$, $a_1 = 1$, $a_2 = -1$, $a_3 = 0$, $a_4 = 0$, $a_5 = 0$, $a_6 = 0$ y $a_7 = 5$.

5. La función que a cada $x \in \mathbb{R} - \{0\}$ le hace corresponder el número $v(x) = \dfrac{1}{x} + x^2 + 3$ no es un polinomio, pues $\dfrac{1}{x}$ no es una potencia positiva de x.

En la figura siguiente se muestran, de todos los polinomios mencionados en este ejemplo, los que son elementos de $\mathcal{P}(\mathbb{R})$. Además allí se grafican las funciones $m : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $m \equiv \sqrt{2}$, $l : \mathbb{R} \longrightarrow \mathbb{R}$, definida por $l(x) = \dfrac{1}{3} - 2x$, y $r : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $r(x) = 3x^2 + x$ y $s(x) = x^3 - 1$.



Operaciones aritméticas en $\mathcal{P}(\mathbb{K})$ y sus propiedades

Definición 3. Suma y producto de polinomios. Dados dos polinomios $p, g \in \mathcal{P}(\mathbb{K})$.

$$p : \mathbb{K} \to \mathbb{K}, \qquad g : \mathbb{K} \to \mathbb{K}.$$

La suma y el producto de polinomios es la misma que la suma y el producto de funciones, es decir, $p + g$ y $p \cdot g$ son las funciones

$$p + g : \mathbb{K} \to \mathbb{K}, \qquad p \cdot g : \mathbb{K} \to \mathbb{K}$$

definidas por:

$$\forall\, x \in \mathbb{K} \ : \ (p + g)(x) = p(x) + g(x), \qquad y \qquad (p \cdot g)(x) = p(x) \cdot g(x).$$

Las funciones resultantes de suma r o multiplicar polinomios también son polinomios, y podemos precisar si grado, tal como establecen los siguientes resultados.

Lema 4. Grado de la suma de polinomios. Sean $p, g \in \mathcal{P}(\mathbb{K})$.

$$p : \mathbb{K} \to \mathbb{K}, \qquad g : \mathbb{K} \to \mathbb{K}$$

Se verifica que $p + q : \mathbb{K} \longrightarrow \mathbb{K}$ es un polinomio de $\mathcal{P}(\mathbb{K})$ y además:

a) Si $\mathrm{gr}(p) \neq \mathrm{gr}(g)$, entonces $\mathrm{gr}(p + g) = \max\{\mathrm{gr}(p),\, \mathrm{gr}(g)\}$.

b) Si $\mathrm{gr}(p) = \mathrm{gr}(g)$, pero la suma de sus coeficientes principales no es cero, entonces $\mathrm{gr}(p + g) = \mathrm{gr}(p) = \mathrm{gr}(g) = \max\{\mathrm{gr}(p),\, \mathrm{gr}(g)\}$.

c) Si $\mathrm{gr}(p) = \mathrm{gr}(g)$, pero la suma de sus coeficientes principales es cero, entonces $\mathrm{gr}(p + g) < \max\{\mathrm{gr}(p),\, \mathrm{gr}(g)\}$.

Demostración. En lo que sigue, sean $n = \mathrm{gr}(p)$ y $m = \mathrm{gr}(g)$, $n,\, m \in \mathbb{N} \cup \{0\}$.

a) Podemos asumir, sin pérdida de generalidad, que $n > m$. Por definición de polinomio, existen escalares $a_0,\, a_1, \cdots, a_n,\, b_0, \cdots,\, b_m \in \mathbb{K}$, con $a_n,\, b_m \neq 0$ tales que,

$$\forall\, x \in \mathbb{K} \ : \ p(x) = a_0 + a_1\, x + \cdots + a_n\, x^n, \qquad \forall\, x \in \mathbb{K} \ : \ q(x) = b_0 + b_1\, x + \cdots + b_m\, x^m.$$

En tal caso, $p + g : \mathbb{K} \to \mathbb{K}$, aplicando asociatividad y conmutatividad de la suma en $\mathbb{K}$, podemos concluir que es el polinomio definido por

$$(p + g)(x) = (a_0 + b_0) + (a_1 + b_1)\, x + \cdots + (a_m + b_m)\, x^m + a_{m+1}\, x^{m+1} + \cdots + a_n\, x^n,$$

y como $a_n \neq 0$, se concluye que $\mathrm{gr}(p + g) = n = \max\{n,\, m\}$.

b) Asumamos que $n = m$. Entonces, procediendo de manera similar a lo anterior, se deduce que

$$(p+g)(x) = (a_0 + b_0) + (a_1 + b_1)\,x + \cdots + (a_n + b_n)\,x^n, \tag{4}$$

y como $a_n + b_n \neq 0$ (a_n no es el inverso aditivo de b_n), se concluye que $\mathrm{gr}(p+g) = n = m = \text{máx}\{n,\, m\}$.

c) En este caso tenemos que $a_n + b_n = 0$, $\mathrm{gr}(p+g) < n = \text{máx}\{n,\, m\}$.

Finalmente, si uno de los polinomios fuera el polinomio nulo, y el otro no, estaríamos en el caso a), y se cumpliría que la suma es igual al polinomio no nulo y su grado también es igual al de este polinomio. Lo cual, dado que hemos definido que $-\infty$ es menor que cualquier número entero, coincide con el máximo de los grados.

Por otro lado, si ambos polinomios son nulos su suma es también el polinomio nulo y su grado es $-\infty$, que es igual a $\text{máx}\{-\infty, -\infty\}$. $\square$

Para la multiplicación podemos especificar de manera más exacta el grado.

Proposición 5. Grado de la multiplicación de polinomios. Sean $p, g \in \mathcal{P}(\mathbb{K})$.

$$p : \mathbb{K} \to \mathbb{K}, \qquad g : \mathbb{K} \to \mathbb{K}$$

Se verifica que $p \cdot q : \mathbb{K} \longrightarrow \mathbb{K}$ es un polinomio de $\mathcal{P}(\mathbb{K})$ y además:

$$\mathrm{gr}(p \cdot g) = \mathrm{gr}(p) + \mathrm{gr}(g).$$

Demostración. En lo que sigue, sean $n = \mathrm{gr}(p)$ y $m = \mathrm{gr}(g)$, $n,\, m \in \mathbb{N} \cup \{0\}$. Al igual que antes, asumimos que existen escalares $a_0,\, a_1, \cdots, a_n,\, b_0, \cdots, b_m \in \mathbb{K}$, con $a_n,\, b_m \neq 0$ tales que,

$$\forall\, x \in \mathbb{K} \ : \ p(x) = a_0 + a_1\,x + \cdots + a_n\,x^n, \qquad \forall\, x \in \mathbb{K} \ : \ q(x) = b_0 + b_1\,x + \cdots + b_m\,x^m.$$

Entonces para cada $x \in \mathbb{K}$,

$$\begin{aligned}(p \cdot g)(x) &= (a_0 + a_1\,x + \cdots + a_n\,x^n) \cdot (b_0 + b_1\,x + \cdots + b_m\,x^m) \\ &= a_0 \cdot (b_0 + b_1\,x + \cdots + b_m\,x^m) + \cdots + a_n\,x^n \cdot (b_0 + b_1\,x + \cdots + b_m\,x^m) \\ &= a_0b_0 + a_0b_1\,x + \cdots + a_0b_m\,x^m + a_1b_0\,x + \cdots + a_nb_0\,x^n + a_nb_1\,x^{n+1} + \cdots + a_nb_m\,x^{n+m},\end{aligned}$$

con lo que

$$\mathrm{gr}(p \cdot g) = \mathrm{gr}(p) + \mathrm{gr}(g).$$

En caso que uno de los dos polinomios fuera el polinomio nulo (o ambos), tendríamos que el resultado de la multiplicación es también sería el polinomio nulo, con lo cual se cumpliría que su grado es igual a $-\infty$ lo cual coincide con definición que dimos para la suma en en caso que uno de los sumandos sea $-\infty$. $\square$

Ejemplo 6. Calculemos algunas sumas y productos de polinomios.

1. Sean $r : \mathbb{R} \longrightarrow \mathbb{R}$ y $l : \mathbb{R} \longrightarrow \mathbb{R}$ los polinomios definidos por

$$r(x) = 3\,x^2 + x, \qquad l(x) = -\,2\,x + \frac{1}{3}, \qquad \forall\, x \in \mathbb{R}.$$

Calculemos $l \cdot r$. Para cada $x \in \mathbb{R}$,

$$(l \cdot r)(x) = (-\,2\,x + 1/3)\,(3\,x^2 + x) = -\,6\,x^3 - x^2 + \frac{1}{3}\,x.$$

Notar que el producto también es un polinomio y es de grado 3 ($= \mathrm{gr}(r) + \mathrm{gr}(l)$).

Calculemos $l + r$. Para cada $x \in \mathbb{R}$,

$$(l + r)(x) = (-\,2\,x + 1/3) + (3\,x^2 + x) = 3\,x^2 -\, x + 1/3$$

También es un polinomio y es de grado 2 ($= \max\{\mathrm{gr}(r) + \mathrm{gr}(l)\}$).

¿Qué pasa con el coeficiente principal de la suma? ¿ de la multiplicación? ¿qué pasa con el término libre de la multiplicación?

Ejercicio 7. Consideremos $p \in \mathcal{P}(\mathbb{R})$ definido como $p(x) = 3\,x^3 + 5\,x + 2$.

Determinemos, si es posible, un polinomio $g \in \mathcal{P}(\mathbb{R})$ de modo que

1. $\mathrm{gr}(p + g) = 10$,
2. $\mathrm{gr}(p + g) = 1$,
3. $gr(pg) = -\infty$,
4. $\mathrm{gr}(p\,g) = 2$,
5. $\mathrm{gr}(p\,g) = 5$.

1. Basta elegir cualquier g cuyo grado sea 10, pues en tal caso, como $\mathrm{gr}(p) \neq \mathrm{gr}(g)$, necesariamente $\mathrm{gr}(p + g) = \max\{\mathrm{gr}(p),\, \mathrm{gr}(g)\} = 10$.

2. Basta elegir cualquier polinomio de la forma $g(x) = -3\,x^3 + a\,x + b$, con $a, b \in \mathbb{R}$, $a \neq -5$.

3. $g = \theta$.

4. No existe tal polinomio, pues necesariamente $\mathrm{gr}(p\,g) = \mathrm{gr}(p) + \mathrm{gr}(g) \geq 3$.

5. Basta elegir cualquier g cuyo grado sea 2, pues en tal caso $\mathrm{gr}(p\,g) = \mathrm{gr}(p) + \mathrm{gr}(g) = 2 + 3 = 5$.

La suma y producto entre polinomios satisfacen propiedades similares a la suma y producto de números reales o números complejos, pero tienen una diferencia importante y es que, no es cierto que para cada $p \in \mathcal{P}(\mathbb{K}) - \{\theta\}$ exista un inverso multiplicativo.

Sean $p,\, q,\, r \in \mathcal{P}(\mathbb{K})$ tales que $p : \mathbb{K} \to \mathbb{K}, \quad q : \mathbb{K} \to \mathbb{K}, \quad r : \mathbb{K} \to \mathbb{K}$. Entonces se cumple

1. La suma y el producto de polinomios son operaciones conmutativas, es decir,

$$p + q = q + p \qquad \text{y} \qquad p\,q = q\,p.$$

La igualdad $p + q = q + p$ es cierta si y solo si para cada $x \in \mathbb{K}$ se cumple que $(p + q)(x) = (q + p)(x)$, pero esto es una consecuencia de la conmutatividad de la suma en $\mathbb{K}$ pues

$$(p + q)(x) = p(x) + q(x) = q(x) + p(x) = (q + p)(x).$$

De manera similar se puede demostrar que el producto también es una operación conmutativa.

2. Ambas operaciones son asociativas, $p + (q + r) = (p + q) + r$ y $p\,(q\,r) = (p\,q)\,r$.

Es una consecuencia de la asociatividad de la suma y el producto en $\mathbb{K}$ y puede demostrarse de modo similar a como se demostró la conmutatividad.

3. El polinomio nulo, $\theta : \mathbb{K} \to \mathbb{K}$, es el elemento neutro para la suma, es decir, $\forall\, p \in \mathcal{P}(\mathbb{K})$ se cumple $p + \theta = p$.

Esto es cierto pues para cada $x \in \mathbb{K}$ se cumple que $(p+\theta)(x) = p(x)+\theta(x) = p(x)+0 = p(x)$.

El polinomio θ es el único elemento neutro para la suma. Si existiera $\hat{\theta} \in \mathcal{P}(\mathbb{K})$ tal que para cada $p \in \mathcal{P}(\mathbb{K})$, $\hat{\theta} + p = \hat{\theta}$, entonces, si $p = \theta$

$$\hat{\theta} = \hat{\theta} + \theta$$

y esta suma es igual a θ.

4. Para todo $p \in \mathcal{P}(\mathbb{K})$, existe el inverso aditivo, que se denota por $-p$, y es el polinomio cuyos coeficientes son los inversos aditivos de los coeficientes de p. Por ejemplo, el inverso aditivo de $p(x) = 2\,x + 1$ es $-\,p(x) = -\,2\,x - 1$.

5. El polinomio constante e igual a 1 es el elemento neutro para el producto. Para cada $p \in \mathcal{P}(\mathbb{K})$ se cumple que $p \cdot 1 = p$ pues

$$\forall\, x \in \mathbb{K} \;:\; (p \cdot 1)(x) = p(x) \cdot 1(x) = p(x) \cdot 1 = p(x).$$

6. $p\,\theta = \theta$. Esto no es difícil de demostrar pues el polinomio $p\,\theta$ es igual a θ si y solo si para cada $x \in \mathbb{K}$ se cumple que $(p\theta)(x) = \theta(x) = 0$ y esto es cierto pues

$$\forall\, x \in \mathbb{K} \;: \quad (p\,\theta)(x) = p(x)\theta(x) = p(x)0 = 0.$$

7. Si $p \in \mathcal{P}(\mathbb{K})$, $p \neq \theta$, es tal que $\mathrm{gr}(p) \geq 1$, entonces p no tiene inverso multiplicativo. Supongamos que existe $q \in \mathcal{P}(\mathbb{K})$, $q \neq \theta$, tal que $p\,q = 1$. Entonces,

$$\mathrm{gr}(1) = \mathrm{gr}(p\,q) \quad \Rightarrow \quad 0 = \mathrm{gr}(p) + \mathrm{gr}(q) \quad \Rightarrow \quad \mathrm{gr}(q) = -\,\mathrm{gr}(p) \leq -1,$$

con lo cual q no es un polinomio, o bien, $q = \theta$, lo que claramente es una contradicción.

Por su parte, los polinomios constantes no nulos, los de grado 0, sí tiene inverso, por ejemplo el polinomio $m : \mathbb{R} \to \mathbb{R}$ definido por $m(x) = \sqrt{2}$, tiene inverso multiplicativo: $(m(x))^{-1} = \frac{1}{\sqrt{2}}$.

8. De manera similar a como ocurre en $\mathbb{R}$ y en $\mathbb{C}$, el producto de dos polinomios es el polinomio nulo si y solo si uno de los dos es el polinomio nulo, es decir,

$$p\,q = \theta \quad \Leftrightarrow \quad p = \theta \quad \vee \quad q = \theta.$$

Supongamos que $p \neq \theta$ y $p\,q = \theta$. Si q fuera distinto de θ, entonces $\mathrm{gr}(p) \geq 0$ y $\mathrm{gr}(q) \geq 0$. Por tanto, $\mathrm{gr}(p\,q) = \mathrm{gr}(p) + \mathrm{gr}(q) \geq 0$, lo cual no puede ocurrir pues $p\,q = \theta$.

Función racional impropia

En la sección anterior vimos cuándo una función es un polinomio y, si lo es, definimos cuál es su grado. La suma y el producto de polinomios se definen del mismo modo en que se definen la suma y el producto de funciones reales. Estas operaciones, que al realizarse entre polinomios dan como resultado un polinomio, tienen propiedades similares a la suma y el producto entre números complejos.

Definición 8. Función racional. Dado un cuerpo de números $\mathbb{K}$ y $p, g \in \mathcal{P}(\mathbb{K})$ no nulos, la función $h = \dfrac{p}{g}$ se denomina *función racional*, es decir, una función racional es la que resulta del cociente de dos polinomios y es tal que

$$h : \mathbb{K} - \{x \in \mathbb{K} \ : \ g(x) = 0\} \to \mathbb{K}, \qquad h(x) = \frac{p(x)}{g(x)}.$$

El polinomio p se denomina *dividendo* y el polinomio q, *divisor*.

Además,

- si $\mathrm{gr}(p)$ es mayor o igual que $\mathrm{gr}(g)$, entonces h es una *función racional impropia* (aquí necesariamente $p \neq \theta$).
- si $\mathrm{gr}(p)$ es menor que $\mathrm{gr}(g)$, entonces h es una *función racional propia*.

En lo que sigue de esta sección sólo trabajaremos con funciones racionales impropias.

Lema 9. Dados $p, g \in \mathcal{P}(\mathbb{K})$, $p, g \neq \theta$, entonces existen, **y son únicos**, polinomios $q, r \in \mathcal{P}(\mathbb{K})$ tales que

$$p = gq + r \quad \text{y} \quad \mathrm{gr}(r) < \mathrm{gr}(g) \quad (r \text{ puede ser igual a } \theta).$$

Esto significa que para cada $x \in \mathbb{K} - \{x \in \mathbb{K} \ : \ g(x) = 0\}$

$$\left(\frac{p}{g}\right)(x) = q(x) + \left(\frac{r}{g}\right)(x),$$

es decir, la función racional puede descomponerse en suma de un polinomio y una función racional propia

$$\frac{p}{g} = q + \frac{r}{g}.$$

Los polinomios q y r se denominan, respectivamente, *cuociente* y *resto* de $\dfrac{p}{g}$.

Demostración. Más adelante veremos que, de manera similar a como calculamos cuociente y resto de la división entre números naturales, podremos determinar los polinomios q y r que se mencionan en el lema. Con esto estaremos demostrando su existencia.

Demostremos ahora la unicidad de q y r. Supongamos existen polinomios q_1, q_2, r_1 y r_2 tales que $q_1 \neq q_2$, $r_1 \neq r_2$, $\mathrm{gr}(r_1) < \mathrm{gr}(g)$, $\mathrm{gr}(r_2) < \mathrm{gr}(g)$ y

$$\frac{p}{g} = q_1 + \frac{r_1}{g} = q_2 + \frac{r_2}{g}.$$

Si $q_1 + \dfrac{r_1}{g} = q_2 + \dfrac{r_2}{g}$, entonces, multiplicando esta igualdad por g, se tiene que

$$q_1\, g + r_1 = q_2\, g + r_2 \quad \Rightarrow \quad (q_1 - q_2)\, g = r_2 - r_1.$$

A ambos lados de la última igualdad tenemos dos polinomios. Si ellos son iguales, tienen que tener el mismo grado. Sin embargo,

$$\mathrm{gr}(r_2 - r_1) \leq \mathrm{máx}\{\mathrm{gr}(r_1), \mathrm{gr}(r_2)\} < \mathrm{gr}(g) \qquad \text{y} \qquad \mathrm{gr}(q_1 - q_2)\, g = \mathrm{gr}(q_1 - q_2) + \mathrm{gr}(g).$$

Si $q_1 \neq q_2$, se tiene que $\mathrm{gr}(q_1 - q_2) \geq 0$ y $\mathrm{gr}((q_1 - q_2)g) \geq \mathrm{gr}(g)$.

Los polinomios $(q_1 - q_2)g$ y $r_2 - r_1$ no pueden, por tanto, tener el mismo grado lo que significa que no pueden ser iguales.

Nuestra suposición inicial (existencia de dos cuocientes y dos restos distintos) es, por tanto, falsa.

□

Definición 10 (Divisibilidad)**.** Dados dos polinomios $p, g \in \mathcal{P}(K)$ no nulos, si el resto que resulta de dividir a p y g es el polinomio nulo, es decir, si $r = \theta$, entonces se dice que g *divide a* p, que p *es divisible por* g, o que g *es factor de* p. En este caso tenemos que existe un polinomio $q : \mathbb{K} \to \mathbb{K}$ tal que:

$$p = qg.$$

Por otra parte, al igual que en el caso de los números enteros, diremos que todo polinomio divide al polinomio nulo θ, y que todo polinomio es divisible por sí mismo, incluso θ. Sin embargo, definimos que θ solo se divide a sí mismo.

Veamos algunos ejemplos:

Ejemplo 11. Calculemos cuociente y resto de la división entre los siguientes polinomios p y g:

1. $p(x) = x^3 + 1$ y $g(x) = x + 1$. Dado que $x^3 + 1 = (x+1)\,(x^2 - x + 1)$, se tiene que el cuociente de $\dfrac{p}{g}$ es $q(x) = x^2 - x + 1$ y $r = \theta$. En este caso decimos que $x + 1$ y $x^2 - x + 1$ son factores de $x^3 + 1$, que $x^3 + 1$ es divisible por $x + 1$ o que $x + 1$ divide a $x^3 + 1$ y que $x^3 + 1$ es divisible por $x^2 - x + 1$ o que $x^2 - x + 1$ divide a $x^3 + 1$.

2. $p(x) = x^4 + 4\,x^2 + 4$ y $g(x) = x^2 + 2$. Dado que $x^4 + 4\,x^2 + 4 = (x^2+2)\,(x^2+2)$, se tiene que

$$\frac{x^4 + 4\,x^2 + 4}{x^2+2} = \frac{(x^2+2)\,(x^2+2)}{x^2+2} = x^2 + 2.$$

   Luego el cuociente es $q(x) = x^2 + 2$ y $r = \theta$. En este caso también decimos que p es divisible por $x^2 + 2$, o bien, que $x^2 + 2$ divide a p.

3. $p(x) = -\,3\,x^2 + 4\,x^4 + 1 - x$ y $g(x) = x^2 - 1$.
   En este caso no podemos factorizar p, y en situaciones como ésta, la aplicación del algoritmo para dividir polinomios nos permtirá determinar cociente y resto de la función racional impropia.

Algoritmo para dividir polinomios

Primero veremos ejemplos particulares de aplicación del algoritmo para dividir polinomios, la generalización del mismo al cálculo de cuociente y resto de la división entre dos polinomios p y g cualesquiera se ha dejado para un apéndice al final, pero no es necesario leerla si, con estos ejemplos, ya comprende cómo dividir dos polinomios cualesquiera.

Determinemos cuociente y resto de la división de $p(x) = -2\,x^2 + 4\,x^4 + 1 - x \quad \text{y} \quad g(x) = x^2 - 1$.

Dado que este algoritmo es similar al que utilizaba en el colegio para dividir números naturales, utilizaremos una notación similar.

Primero debemos ordenar los términos en dividendo y divisor de mayor a menor potencia, en este ejemplo p se debe reescribir como $p(x) = 4x^4 - 2x^2 - x + 1$ y g ya está ordenado.

$$(4x^4 - 2x^2 - x + 1) : (x^2 - 1) = \qquad (...)$$

Primero calculemos el cociente entre los términos principales de dividendo y divisor, es decir, $\dfrac{4\,x^4}{x^2} = 4\,x^2$.

Observe que ahora p puede escribirse como

$$p = 4x^2\left(x^2 - 1\right) + \left(p - 4x^2\left(x^2 - 1\right)\right).$$

El término $4x^2$ se escogió de modo que los términos principales de p y $4x^2\,(x^2 - 1)$ sean iguales y, así, el grado de $p - 4x^2\,(x^2 - 1)$ es estrictamente menor al grado de p. Siguiendo la notación que se usa para dividir números enteros, escribimos

$$\begin{array}{rrrrrl} & 4x^4 & +0x^3 & -2x^2 & -x & +1 : \; x^2 - 1 = \; 4x^2 \qquad (...) \\ - & 4x^4 & & -4x^2 & & \end{array}$$

Realizando la suma obtenemos

$$\begin{array}{rrrrrl}
4x^4 & +0x^3 & -2x^2 & -x & +1: & x^2-1 = \quad 4x^2 \qquad (...) \\
-\quad (4x^4 & & -4x^2) & & & \\
\hline
& & 2x^2 & -x & +1 &
\end{array}$$

Si llamamos q_1 al polinomio $4x^2$ y r_1 a $2x^2 - x + 1$, tenemos que

$$p = gq_1 + r_1 \quad \Rightarrow \quad \frac{p}{g} = q_1 + \frac{r_1}{g}$$

El algoritmo debe continuar, pues el grado de r_1 no es menor al grado de g. Procedemos de igual forma que en el paso anterior, pero ahora queremos determinar polinomios q_2 y r_2 de modo que $r_1 = q_2g + r_2$ y el grado de r_2 sea estrictamente menor que el grado de r_1.

De nuevo podemos calcular el cociente entre los términos principales de r_1 y g, $\dfrac{2\,x^2}{x^2} = 2$, y así, de la misma forma que en el paso anterior, tenemos que

$$r_1 = 2\left(x^2-1\right) + \left(r_1 - 2\left(x^2-1\right)\right)$$

que, usando la misma notación que para dividir números naturales, escribimos como

$$\begin{array}{rrrrrl}
4x^4 & +0x^3 & -2x^2 & -x & +1: & x^2-1 = \quad 4x^2+2 = q_2(x) \\
-\quad (4x^4 & & -4x^2) & & & \\
\hline
& & 2x^2 & -x & +1 & \\
& - & (2x^2 & & -2) & \\
\hline
& & & -x & +3 & = r_2(x)
\end{array}$$

Si llamamos q_2 al polinomio 2 y r_2 al polinomio $-x+3$, tenemos entonces que

$$p = q_1g + r_1 = q_1g + q_2g + r_2 = (q_1+q_2)g + r_2.$$

El grado de r_2 es estrictamente menor que el de r_1 y también estrictamente menor que el de g. En este momento ha terminado el algoritmo de división de polinomios, hemos determinado $q = q_1 + q_2$ y $r = r_2$ de modo que $p = qg + r$ con grado de r estrictamente menor que el grado de g y, por tanto,

$$\frac{4\,x^4-2\,x^2-x+1}{x^2-1} = 4\,x^2 + \frac{2\,x^2-x+1}{x^2-1} = 4\,x^2+2+\frac{-x+3}{x^2-1}.$$

Ejemplo 12. Determinemos cuociente y resto de la función racional impropia $\dfrac{p}{g}$ si $p(x) = 5x^4 + 4x^3 - x^2 + 6x$ y $g(x) = x^2+1$.

$$\begin{array}{rrrrrl}
5x^4 & +4x^3 & -x^2 & +6\,x & +0: & (x^2+1) = \quad 5x^2+4x-6 \\
-\quad (5x^4 & & +5x^2) & & & \\
\hline
& 4x^3 & +6x^2 & +6\,x & & \\
- & (4x^3 & & +4x) & & \\
\hline
& & -6x^2 & +2x & & \\
& - & (-6x^2 & & -6) & \\
\hline
& & & 2x & +6 &
\end{array}$$

Es decir, el cuociente de la división de $p(x) = 5\,x^4 + 4\,x^3 - x^2 + 6\,x$ por $g(x) = x^2 + 1$ es $q(x) = 5\,x^2 + 4x - 6$, y el resto es $r(x) = 2\,x + 6$.

Ejemplo 13. Determinemos cuociente y resto de la función racional propia $\dfrac{p}{g}$ si $p(x) = x^2 + 1$ y $g(x) = 5x^4 + 4x^3 - x^2 + 6x$.

En este caso, sea cual sea el polinomio $q \in \mathcal{P}(\mathbb{K})$ que multiplique a g, el resultado siempre tendrá grado mayor o igual que 4, y no podrá coincidir con p. Por lo tanto no queda más alternativa que tomar $q = \theta$, y entonces resulta $r = p$:

$$p = \theta \cdot g + p, \text{ como } \operatorname{gr}(p) < \operatorname{gr}(g) \text{ es posible tomar } p \text{ como resto.}$$

Observación 14. Si p, g son polinomios distintos del nulo, existen q y r tales que

$$\frac{p}{g} = q + \frac{r}{g}$$

con $\operatorname{gr}(r) < \operatorname{gr}(g)$.

Teorema del resto

Sea $p : \mathbb{K} \to \mathbb{K}$ un polinomio de grado mayor o igual que 1 y $g : \mathbb{K} \to \mathbb{K}$ el polinomio $g(x) = x - c$, con $c \in \mathbb{K}$. Entonces, aplicando el lema 9, sabemos que existen únicos polinomios q, r tales que

$$p(x) = q(x)(x - c) + r(x) \quad \text{ y } \quad \operatorname{gr}(r) < \operatorname{gr}(g) = 1,$$

es decir, $\operatorname{gr}(r) = 0$ o $-\infty$. Esto significa que r es un polinomio de la forma $r = r_0$ con $r_0 \in \mathbb{K}$ (r_0 puede ser cero, en cuyo caso r es el polinomio nulo). En tal caso,

$$p(x) = q(x)(x - c) + r_0.$$

Si ahora evaluamos p en $x = c$ obtenemos lo siguiente:

$$p(c) = q(c)(c - c) + r_0 = r_0,$$

es decir, el resto de la división de p por $x - c$ es igual a $p(c)$. Justo esto es lo que plantea el siguiente resultado llamado *Teorema del resto*.

Teorema 15. (Teorema del Resto) Sean $p \in \mathcal{P}(\mathbb{K})$ tal que $\operatorname{gr}(p) \geq 1$, $c \in \mathbb{K}$ y $\dfrac{p(x)}{x - c} = q(x) + \dfrac{r(x)}{x - c}$ con $\operatorname{gr}(r) < 1$. Entonces $r \equiv p(c)$.

Observe que si además $p(c) = 0$, entonces $r = \theta$ y por tanto p es divisible por $x - c$. A los valores c tales que $p(c) = 0$ se les da un nombre especial.

Definición 16 (Raíz de un polinomio.)**.** Sea $p \in \mathcal{P}(\mathbb{C})$. Se dice que $c \in \mathbb{C}$, *es una raíz de* p si y solo si $p(c) = 0$.

Corolario 17. Sean $p \in \mathcal{P}(\mathbb{K})$ tal que $\mathrm{gr}(p) \geq 1$, $c \in \mathbb{K}$, entonces se cumple que:

$$c \text{ es raíz de } p \Leftrightarrow \text{ el polinomio dado por } (x - c) \text{ divide a } p.$$

De esta manera al encontrar una raíz de p, encontramos también un factor de p. Por otra parte, si hemos factorizado p, sabemos que el conjunto de sus raíces es la unión de las raíces de sus factores.

Ejemplo 18.

1. El polinomio $m(x) = \sqrt{2}$ no tiene raíces.

2. El polinomio $l(x) = -2\,x + 1/3$ solo tiene como raíz a $x = 1/6$. El resto de dividir a l por $x - \frac{1}{6}$ es 0, mientras que, por ejemplo, el resto de dividir a l por x es $l(0) = \frac{1}{3}$. Además, dado que $l(x) = -2\left(x - \frac{1}{6}\right)$, el cociente de la división de l por $x - \frac{1}{6}$ es -2.

3. El polinomio $r(x) = 3\,x^2 + x = x\,(3\,x + 1)$ tiene dos raíces reales, 0 y $-1/3$. El resto de dividir a r, tanto por x como por $x + \frac{1}{3}$ es 0. La igualdad $r(x) = x\,(3\,x+1) = 3\,x\,\left(x + \frac{1}{3}\right)$ nos indica además que el cociente de la función racional impropia $\dfrac{r(x)}{x}$ es $3\,x + 1$, mientras que el cociente de $\dfrac{r(x)}{x + \frac{1}{3}}$ es $3\,x$.

4. El polinomio $s(x) = x^3 - 1 = (x - 1)\,(x^2 + x + 1)$ es tal que $s(1) = 0$, y por tanto, 1 es raíz de s. Para obtener las restantes debemos determinar para qué valores de x se cumple que $x^2 + x + 1 = 0$.

Ejemplo 19. Calculemos los valores de $x \in \mathbb{C}$ tales que $x^2+x+1 = 0$, completando cuadrados (por ejemplo) se tiene

$$\begin{aligned} x^2 + x + 1 &= x^2 + 2 \cdot \tfrac{1}{2}\,x + \tfrac{1}{4} + \tfrac{3}{4} \\ &= \left(x + \tfrac{1}{2}\right)^2 + \tfrac{3}{4} = 0 \\ &\Updownarrow \\ \left(x + \tfrac{1}{2}\right)^2 &= -\tfrac{3}{4} \\ &\Updownarrow \\ x + \tfrac{1}{2} &\in \sqrt{-\tfrac{3}{4}} \end{aligned}$$

Luego, las raíces de s son 1, $-\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}\,i$ y $-\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}\,i$.

5. Averigüemos si 1 es raíz de $p(x) = x^3 - 3\,x^2 + 4\,x - 2$.

   Solución: Dado que
   $$p(1) = 1 - 3 + 4 - 2 = 0,$$
   se tiene que 1 es raíz de p. Esto significa que si dividimos p por $x-1$ obtendremos resto igual al polinomio nulo, es decir, p es divisible por $x-1$. Si usamos el algoritmo para dividir polinomios, obtenemos que
   $$\frac{p}{x-1} = x^2 - 2\,x + 2 = (x-1)^2 + 1.$$

Raíces de un polinomio y su multiplicidad

Supongamos que $c \in \mathbb{C}$ es raíz de $p \in \mathcal{P}(\mathbb{C})$, entonces existe (un único) $q \in \mathcal{P}(\mathbb{C})$ tal que $p(x) = q(x)\,(x-c)$. Entonces, puede ocurrir que,

1. c no es raíz de q, es decir, $q(c) \neq 0$. En este caso se dice que c es *raíz simple* de p,
2. c es raíz de q. Entonces existe (único) $s \in \mathcal{P}(\mathbb{C})$ tal que $q(x) = s(x)\,(x-c)$ y, por tanto, $p(x) = s(x)\,(x-c)^2$. Ahora, puede nuevamente ocurrir que
   - 2.1 c no es raíz de s, en cuyo caso decimos que c es *raíz de multiplicidad 2* de p,
   - 2.2 c es raíz de s, entonces existe (único) $u \in \mathcal{P}(\mathbb{K})$ tal que $s(x) = u(x)(x-c)$ y, por tanto, $p(x) = u(x)(x-c)^3$. Si
     - 2.2.1 c no es raíz de u, se dice que c es *raíz de multiplicidad 3* de p,
     - 2.2.2 c es raíz de u, existe (único) $t \in \mathcal{P}(\mathbb{K})$ tal que $u(x) = t(x)(x-c)$ y, por tanto, $p(x) = t(x)(x-c)^4$, c es entonces raíz de multiplicidad mayor o igual que 4 de p.

$$\vdots$$

Esto motiva la siguiente definición.

Definición 20. Multiplicidad de una raíz. Sea $c \in \mathbb{C}$ raíz de $p \in \mathcal{P}(\mathbb{C})$ y sea k el mayor número natural tal que $p(x) = q(x)(x-c)^k$ con $q \in \mathcal{P}(\mathbb{C})$ tal que $q(c) \neq 0$.

Si $k = 1$, se dice que c es *raíz simple* de p y si $k > 1$, se dice que c es *raíz de multiplicidad k* de p.

Ejemplo 21. Sea $p(x) = 8\,x^3 + 16\,x^2 + 10\,x + 2$. Averigüemos si $-\frac{1}{2}$ es raíz de p y su multiplicidad. Evaluemos $p\left(-\frac{1}{2}\right) = 8\left(-\frac{1}{2}\right)^3 + 16\left(-\frac{1}{2}\right)^2 + 10\left(-\frac{1}{2}\right) + 2 = -1 + 4 - 5 + 2 = 0$

$$
\begin{array}{rrrrl}
8x^3 & +16\,x^2 & +10x & +2 & : x+0,5 = \quad 8x^2+12x+4 \\
-(8x^3 & +4x^2) & & & \\
\hline
 & 12x^2 & +10x & +2 & \\
 & -(12x^2 & +6x) & & \\
\hline
 & & 4x & +2 & \\
 & & -(4x & +2) & \\
\hline
 & & & 0 &
\end{array}
$$

Por tanto, se confirma que $-\frac{1}{2}$ es raíz de p y $p(x) = (8\,x^2 + 12\,x + 4)\ \left(x + \frac{1}{2}\right)$.

Sea $q(x) = 8\,x^2 + 12\,x + 4$. Si $q\left(-\frac{1}{2}\right)$ es distinto de cero, $-\frac{1}{2}$ es raíz simple de p. Calculemos $q\left(-\frac{1}{2}\right) = 8\ \left(-\frac{1}{2}\right)^2 + 12\ \left(-\frac{1}{2}\right) + 4 = 2 - 6 + 4 = 0$. La multiplicidad de $-\frac{1}{2}$ es 2 o más, empleemos de nuevo la división para averiguar cuánto es.

$$
\begin{array}{rrrl}
8\,x^2 & +12x & +4 & : x+0,5 = 8x+8 \\
-(8x^2 & +4x) & & \\
\hline
 & 8x & +4 & \\
 & -(8x & +4) & \\
\hline
 & & 0 &
\end{array}
$$

Con esto tenemos que $-\frac{1}{2}$ es raíz de q y $q(x) = (8\,x{+}8)\ \left(x + \frac{1}{2}\right)$, y por tanto, $p(x) = \underbrace{(8\,x+8)}_{=s(x)}\ \left(x + \frac{1}{2}\right)^2$.

Dado que $s\left(-\frac{1}{2}\right) = 8\left(-\dfrac{1}{2}\right) + 8 \neq 0$, se cumple que $-\frac{1}{2}$ es raíz de multiplicidad 2 de p.

Observe que $p(x) = 8\,(x+1)\left(x + \frac{1}{2}\right)^2$, de donde podemos concluir que -1 y $-\frac{1}{2}$ son raíces de p, siendo -1 raíz simple y $-\frac{1}{2}$, raíz de multiplicidad 2 de p.

Ahora que escribimos a p en como $p(x) = 8\,(x+1)\ \left(x + \frac{1}{2}\right)^2$, ¿existe $x \in \mathbb{R} - \left\{-1, -\frac{1}{2}\right\}$ que sea raíz de p?

Ejemplo 22. Sea $p(x) = x^4 - x^3 - 5\,x^2 - x - 6$. Averigüemos si i es raíz de p y, si lo es, su multiplicidad.

Para averiguar si i es o no raíz de p lo más simple es evaluar $p(i) = i^4 - i^3 - 5\,i^2 - i - 6 = 1 + i + 5 - i - 6 = 0$

Ahora odemos aplicar el algoritmo de la división para calcular cuociente y resto de $\dfrac{p}{x-i}$.

$$
\begin{array}{rrrrrl}
x^4 & -x^3 & -5\,x^2 & -x & -6: & x-i = \quad x^3+(i-1)x^2-(6+i)x-6i \\
-(x^4 & -ix^3) & & & & \\
\hline
 & (i-1)x^3 & -5\,x^2 & -x & -6 & \\
 & -((i-1)x^3 & +(1+i)x^2) & & & \\
\hline
 & & -6-i)\,x^2 & -x & -6 & \\
 & & -(-(6+i)x^2 & +(6i-1)x) & & \\
\hline
 & & & -6ix & -6 & \\
 & & & -(-6ix & -6) & \\
\hline
 & & & & 0 &
\end{array}
$$

Confirmamos que i es raíz de p y

$$p(x) = \big(x^3 + (i-1)\,x^2 - (i+6)\,x - 6\,i\big)\,(x-i).$$

Debemos seguir dividiendo para determinar la multiplicidad de i como raíz de p. Pero antes evaluamos el cuociente en i: $i^3 + (i-1)\,i^2 - (i+6)\,i - 6\,i = -i - i + 1 + 1 - 6i - 6i = 2 - 14i \neq 0$ Por tanto, i es raíz simple de p.

En el siguiente lema se muestra una relación importante entre las raíces de un polinomio p con coeficientes complejos y las raíces del polinomio conjugado, es decir, aquel cuyos coeficientes son los conjugados de los coeficientes de p.

Lema 23. Consideremos $p \in \mathcal{P}(\mathbb{C})$. Si $z_0 \in \mathbb{C}$ es raíz de p, entonces $\overline{z_0}$ es raíz de $\overline{p}$, siendo $\overline{p}$ el polinomio cuyos coeficientes son los conjugados de los coeficientes de p.

Demostración. Sea $p(x) = a_0 + a_1\,x + \ldots + a_n\,x^n$, con $a_0,\, a_1,\, a_2,\, \cdots,\, a_n \in \mathbb{C}$. Entonces

$$\overline{p}(x) = \overline{a_0} + \overline{a_1}\;x + \cdots + \overline{a_n}\;x,$$

de donde

$$\overline{p}(\overline{z_0}) = \overline{a_0} + \overline{a_1}\;(\overline{z_0}) + \overline{a_2}\;(\overline{z_0})^2 + \cdots + \overline{a_n}\;(\overline{z_0})^n\,.$$

Dado que el conjugado de un producto es el producto de los conjugados, para cada $k \in \mathbb{N}$ se cumple que $(\overline{z_0})^k = \overline{z_0^k}$, y por tanto,

$$\overline{p}(\overline{z_0}) = \overline{a_0} + \overline{a_1}\;\overline{z_0} + \overline{a_2}\;\overline{z_0^2} + \cdots + \overline{a_n}\;\overline{z_0^n} = \overline{a_0} + \overline{a_1\,z_0} + \overline{a_2\,z_0^2} + \cdots + \overline{a_n\,z_0^n}.$$

Por último, como el conjugado de una suma es la suma de los conjugados, se concluye que

$$\bar{p}(\overline{z_0}) = \overline{a_0 + a_1\,z_0 + a_2\,z_0^2 + \cdots + a_n\,z_0^n} = \overline{p(z_0)} = \overline{0} = 0.$$

$\square$

Observe que si los coeficientes de p son complejos reales, entonces $\overline{p} = p$. De donde obtenemos la siguiente e importante consecuencia para polinomios con coeficientes reales.

Corolario 24. Sea $p : \mathbb{C} \to \mathbb{C}$ un polinomio cuyos coeficientes son números complejos reales. Entonces si $z_0 \in \mathbb{C}$ es raíz de p, se cumple que $\overline{z_0}$ también lo es.

Además, si z_0 es raíz de multiplicidad k de p, $\overline{z_0}$ también es raíz de multiplicidad k de p.

Ejemplo 25. En el ejemplo anterior vimos que i es raíz simple de $p(x) = x^4 - x^3 - 5\,x^2 - x - 6$. Como todos los coeficientes de este polinomio son números reales, entonces $-\,i$ también es raíz de p. Además, dado que i es raíz simple de p, $-\,i$ es raíz simple de p.

Teorema fundamental del Álgebra y sus consecuencias

El teorema fundamental del Álgebra es un resultado importante que tiene múltiples consecuencias, que mencionaremos más adelante.

Teorema 26. (Teorema fundamental del Álgebra) Sea $p \in \mathcal{P}(\mathbb{C})$[1] de grado mayor o igual que 1. Entonces, existe $c \in \mathbb{C}$ tal que $p(c) = 0$.

La demostración de este teorema no la presentaremos en estos apuntes, pero podemos analizar sus consecuencias. Ahora solo las mencionamos, pero más adelante las veremos más en detalle.

- si $p \in \mathcal{P}(\mathbb{C})$ es un polinomio de grado n, entonces existen exactamente n números complejos $c_1,\, c_2,\, \cdots,\, c_n$ (no necesariamente distintos entre sí) que son raíces de p.
- para todo $p \in \mathcal{P}(\mathbb{C})$ se cumple que si p tiene grado n, entonces existen $\alpha,\, c_1,\, c_2,\, \cdots,\, c_n \in \mathbb{C}$ tales que $p(x)$ puede escribirse como

$$p(x) = \alpha\,(x - c_1)\,(x - c_2)\,\cdots\,(x - c_n).$$

- si $p, q \in \mathcal{P}(\mathbb{C})$ son de grado menor o igual que n y existen $n + 1$ números complejos $c_1, c_2, \ldots, c_{n+1}$, distintos entre sí, de modo que

$$p(c_1) = q(c_1), \quad p(c_2) = q(c_2), \quad \cdots \quad , \quad p(c_{n+1}) = q(c_{n+1}),$$

  entonces p y q son iguales.

[1] cualquier polinomio con coeficientes reales es un elemento de $\mathcal{P}(\mathbb{C})$.

La segunda de las propiedades anteriores nos permitirá, más adelante, descomponer una función racional propia en suma de fracciones parciales.

La tercera de las propiedades anteriores tiene múltiples aplicaciones, una de ellas la conocerán en el curso de Cálculo Numérico, cuando se estudien los polinomios de interpolación.

A pesar que el teorema fundamental del Álgebra permite concluir que un polinomio de grado n tiene exactamente n raíces complejas (no necesariamente distintas entre sí), no establece cómo calcular las raíces de un polinomio.

Si p es un polinomio de grado 1 ó 2, ya se sabe cómo calcular las raíces de p.

Si p es un polinomio de grado mayor que 2 no hemos enseñado un procedimiento general con el cual se pueda proceder, como en el caso de polinomios de grado 1 o 2, para calcular las raíces de p. Sin embargo, sí existen fórmulas que permiten, dados los coeficientes de un polinomio de grado 3 o 4, determinar sus raíces. Para polinomios de grado mayor o igual que 5 no existe una fórmula general para el cálculo de sus raíces a partir de los valores de sus coeficientes.

Esto no significa que no se puedan calcular las raíces de ningún polinomio de grado mayor o igual que 5, por ejemplo, el polinomio $(x-1)^{100}$ es de grado 100 y se sabe que tiene una sola raíz, 1, de multiplicidad 100.

En el curso de Cálculo Numérico se va a aprender métodos (algoritmos) para la aproximación de las raíces de polinomios de cualquier grado.

Ejemplo 27.

- Si $p \in \mathcal{P}(\mathbb{K})$ es de grado 1, entonces $p(x) = a_1\, x + a_0$ con $a_1,\, a_0 \in \mathbb{K}$ y $a_1 \neq 0$. El número $c = -\dfrac{a_0}{a_1}$ es tal que $p(c) = 0$. Éste es el único elemento de $\mathbb{K}$ que es raíz de p.

  Por ejemplo, el polinomio $p(x) = 2\,x + 1$ es de grado 1 y $c = -\frac{1}{2}$ es tal que $p(c) = 0$.

- Si p es de grado 2, entonces $p(x) = a_2\, x^2 + a_1\, x + a_0$ con $a_2,\, a_1,\, a_0 \in \mathbb{C}$ y $a_2 \neq 0$.

  Ya sabemos cómo determinar las dos (no necesariamente distintas entre sí) raíces de p.

  Por ejemplo, si $p(x) = (x+1)^2$, entonces $c = -1$. Si $p(x) = x^2 + 2\,x + 2$, entonces c puede ser $-1+i$, o bien, c puede ser $-1-i$.

  En general, sabemos que si $p(x) = a_2\, x^2 + a_1\, x + a_0$ con $a_2,\, a_1,\, a_0 \in \mathbb{C}$ y $a_2 \neq 0$, los números complejos

  $$\frac{-\,a_1 \pm \sqrt{a_1^2 - 4\,a_2\,a_0}}{2\,a_2}$$

  son raíces de p.

- Si p es un polinomio de grado 3, no estudiaremos en este curso una fórmula general para determinar las raíces de p. Sin embargo, para algunos polinomios de grado 3 se puede determinar fácilmente sus raíces. Por ejemplo, si $p(x) = (x-1)\,(x^2 + 2\,x + 2)$ se sabe que $p(x) = 0$ si y solo si $x - 1 = 0$, o bien, $x^2 + 2\,x + 2 = 0$ y, por tanto, podemos asegurar que 1, $-1+i$ y $-1-i$ son las raíces de p.

Veamos por qué el teorema fundamental del Álgebra nos permite concluir que un polinomio de grado $n \in \mathbb{N}$, tiene exactamente n raíces complejas.

Supongamos que p es un polinomio de grado n, es decir,

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

con $a_n,\, a_{n-1},\, \ldots,\, a_1,\, a_0 \in \mathbb{K}$ y $a_n \neq 0$. Si $n > 1$, el teorema fundamental del Álgebra asegura que existe $c_0 \in \mathbb{C}$ tal que $p(c_0) = 0$ y, por tanto, existe un único q_1, polinomio de grado $n-1$, de modo que

$$p(x) = (x - c_0)\, q_1(x).$$

Dado que q_1 tiene grado $n-1$, si $n-1$ es mayor o igual que 1, es decir, si $n \geq 2$, existe $c_1 \in \mathbb{C}$ tal que $q_1(c_1) = 0$ con lo que

$$q_1(x) = (x - c_1)\, q_2(x) \quad \Leftrightarrow \quad p(x) = (x - c_0)\,(x - c_1)\, q_2(x)$$

y el grado de q_2 es $n-2$.

Si $n = 2$, entonces q_2 es de grado cero, es decir, igual a una constante $\alpha \in \mathbb{C}$ y

$$p(x) = (x - c_0)\,(x - c_1)\, \alpha,$$

siendo c_0 y c_1 las dos raíces de p (pueden ser iguales).

Si $n \geq 3$, el grado de q_2 es mayor o igual que 1 y podemos aplicar nuevamente el teorema fundamental del Álgebra, pero ahora a q_2, con lo que obtendríamos que existe $c_2 \in \mathbb{C}$ tal que $q_2(c_2) = 0$ lo que implica que existe q_3 de grado $n-3$ tal que

$$q_2(x) = (x - c_2)\, q_3(x)$$

y con ello,

$$p(x) = (x - c_0)\,(x - c_1)\,(x - c_2)\, q_3(x).$$

Si $n = 3$, q_3 es de grado cero, es decir, igual a una constante $\beta \in \mathbb{K}$ y

$$p(x) = (x - c_0)\,(x - c_1)\,(x - c_2)\, \beta,$$

siendo c_0, c_1 y c_2 las tres raíces de p (pueden ser iguales).

Aplicando sucesivamente esta idea se obtiene que si p es un polinomio de grado n, existen $c_0,\, c_1,\, \cdots,\, c_{n-1} \in \mathbb{C}$, $\alpha \in \mathbb{C}$, $\alpha \neq 0$, tales que

$$p(x) = (x - c_0)\,(x - c_1)\, \cdots\, (x - c_{n-1})\, \alpha \tag{5}$$

donde $c_0,\, c_1,\, \cdots,\, c_{n-1}$ son las raíces de p, no necesariamente distintas entre sí.

Lamentablemente el teorema fundamental del Álgebra, y ningún teorema, puede darnos una manera de determinar $c_0,\, c_1,\, \cdots,\, c_{n-1}$ que funcione para cualquier polinomio, veamos algunos ejemplos en los que esto sí es posible.

Ejemplo 28. Sabiendo que i es una raíz de $p(x) = x^4 - 2\,x^3 + 2\,x^2 - 2\,x + 1$, determinemos las restantes.

Como p es de grado 4, existen c_1, c_2, c_3, $c_4 \in \mathbb{C}$ tales que $p(c_1) = p(c_2) = p(c_3) = p(c_4) = 0$ (los valores de c_1, c_2, c_3 y c_4 no tienen que ser distintos entre sí).

Si i es raíz de p, entonces $\dfrac{p(x)}{x-i}$ tiene que tener resto θ. Aplicando división obtenemos

$$p(x) = (x-i)\,\underbrace{\left(x^3 + (-2+i)\,x^2 + (1-2\,i)\,x + i\right)}_{=q_1(x)}.$$

Como p tiene coeficientes reales, $-i$ también tiene que ser raíz de p. Dado que

$$p(-i) = (-2\,i)\,q_1(-i),$$

tiene que cumplirse $q_1(-i) = 0$. Aplicando nuevamente división obtenemos

$$q_1(x) = (x+i)\,(x^2 - 2\,x + 1).$$

Por tanto,

$$p(x) = (x-i)\,(x+i)\,(x^2 - 2\,x + 1) = (x+i)\,(x-i)\,(x-1)^2,$$

y así, las cuatro raíces de p son i, $-i$, 1 y 1. Observe que i y $-i$ son raíces simples y 1 es raíz de multiplicidad 2.

Observación 29.

1. Sean $p, q \in \mathcal{P}_n(\mathbb{K})$ con $n \in \mathbb{N}$. Si existen x_0, x_1, $\cdots$, $x_n \in \mathbb{C}$, distintos entre sí, tales que

$$p(x_0) = q(x_0), \quad p(x_1) = q(x_1), \quad p(x_2) = q(x_2), \quad \cdots, \quad p(x_n) = q(x_n), \tag{6}$$

   entonces para todo $x \in \mathbb{K}$ se cumple que $p(x) = q(x)$.

   En efecto, pues si p y q tienen grado menor o igual que n, el polinomio $d = p - q$ también tiene grado menor o igual que n. Esto significa que $\mathrm{gr}(d) \in \mathbb{N} \cup \{0\}$ o bien $d \equiv 0$. En el primer caso, una de las consecuencias del teorema fundamental del Álgebra es que d tiene, a lo sumo, $\mathrm{gr}(d)$ raíces.

   Si (6) se cumple, entonces x_0, x_1, $\cdots$, x_n son $n+1$ raíces distintas de d y, como el grado de d es menor o igual que n, esto sólo es posible si $d = \theta$, es decir, $p = q$.

2. Teniendo en cuenta el teorema sobre las raíces complejas de un polinomio con coeficientes reales, una consecuencia del teorema fundamental del Álgebra es, además, que todo polinomio $p \in \mathcal{P}(\mathbb{R})$, cuyo grado sea un número impar tiene, al menos, una raíz real.

Ejemplo 30. Sabiendo que -2 es raíz de multiplicidad 2 de $p(x) = x^5 - 2x^4 - 11x^3 + 12x^2 + 36x$, determinemos las restantes raíces de p y escribamos a p como un producto de la forma (5).

El polinomio p puede escribirse como $p(x) = x\,(x^4 - 2x^3 - 11x^2 + 12x + 36)$. Esto significa que 0 es una de las raíces de p y es una raíz simple (¿por qué?). Llamemos $q(x) = x^4 - 2x^3 - 11x^2 + 12x + 36$.

Como $p(-2) = (-2)\,q(-2)$, entonces -2 tiene que ser raíz de multiplicidad 2 de q. Aplicando división a q y al cuociente de la división de q por $x+2$ (porque -2 es raíz de multiplicidad 2 de p si y solo si es raíz de multiplicidad 2 de q), obtenemos que

$$q(x) = (x+2)\,(x^3 - 4x^2 - 3x + 18) = (x+2)^2\,(x^2 - 6x + 9).$$

Por tanto, $p(x) = x\,(x-2)^2\,(x^2 - 6x + 9) = x\,(x+2)^2\,(x-3)^2$. De esta manera, las cinco raíces de p son 0 (simple), -2 (de multiplicidad 2) y 3 (de multiplicidad 2.)

Observa que, en general, un polinomio de grado $n \in \mathbb{N}$ no tiene que tener n raíces distintas, sino que el número de raíces distintas es mayor o igual que 1 y la suma de sus multiplicidades es n.

Los valores de $c_0, c_1, \cdots, c_{n-1}$ en (5) no tienen que ser distintos entre sí, como ocurrió en el ejemplo anterior. En (5) podría ocurrir que c_0 apareciera l_0 veces (c_0 sería raíz de multiplicidad l_0 de p), c_1, l_1 veces y así sucesivamente hasta un c_r que aparecería l_r veces con $l_0 + l_1 + \cdots + l_r = n$. Entonces

$$p(x) = \alpha(x - c_0)^{l_0}\,(x - c_1)^{l_1}\,\cdots\,(x - c_r)^{l_r}. \tag{7}$$

Polinomios irreducibles

En el conjunto de los polinomios con coeficientes en $\mathbb{K}$ existe un concepto similar al de número primo en $\mathbb{N}$ y es el de polinomio irreducible.

Definición 31. Un polinomio $p \in \mathcal{P}(\mathbb{K})$ tal que $\mathrm{gr}(p) > 0$. El polinomio p es *irreducible en* $\mathcal{P}(\mathbb{K})$ si y solo si no es posible descomponer a p como producto de dos polinomios de grado mayor que cero y coeficientes en $\mathbb{K}$.

Si un polinomio p no es irreducible, es decir, si es posible escribir a p como producto de dos polinomios de grado mayor que cero y coeficientes en $\mathbb{K}$, se dice entonces que p es *reducible en* $\mathcal{P}(\mathbb{K})$.

Observe que polinomios de grado cero no se consideran irreducibles. Esto es porque ellos cumplen, en $\mathcal{P}(\mathbb{K})$ un rol similar al que cumple el número 1 en el conjunto de los números naturales, es decir, si c es un polinomio de grado cero, todo polinomio p es divisible por c pues si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, entonces

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

Ejemplo 32. El polinomio $p(x) = x^2 - 1$, como elemento de $\mathcal{P}(\mathbb{R})$, puede escribirse como $p(x) = (x+1)(x-1)$. Él es, por tanto, reducible en $\mathcal{P}(\mathbb{R})$.

También es reducible en $\mathcal{P}(\mathbb{C})$.

El polinomio $q(x) = x^2 + 1$ es reducible, si lo consideramos elemento de $\mathcal{P}(\mathbb{C})$, $p(x) = (x-i)(x+i)$, pero irreducible como elemento de $\mathcal{P}(\mathbb{R})$ pues no puede escribirse como producto de polinomios de grado 1 con coeficientes reales.

Podemos demostrar entonces las siguientes propiedades.

Lema 33. Sea $p \in \mathcal{P}(\mathbb{K})$. Entonces es cierto que

1. si $\mathrm{gr}(p) = 1$, entonces p es irreducible.
2. Si $\mathbb{K} = \mathbb{C}$ y $\mathrm{gr}(p) \geq 2$, entonces p es reducible.
3. Si $\mathbb{K} = \mathbb{R}$, $\mathrm{gr}(p) = 2$ y las raíces de p pertenecen a $\mathbb{C} - \mathbb{R}$, entonces p es irreducible.
4. Si $\mathbb{K} = \mathbb{R}$, $\mathrm{gr}(p) = 2$ y las raíces de p son números reales, entonces p es reducible.
5. Si $K = \mathbb{R}$ y $\mathrm{gr}(p) \geq 3$, entonces p es reducible.

Demostración.

1. Esto es cierto porque el producto de dos polinomios de grado mayor o igual que 1 es un polinomio de grado mayor o igual que dos.
2. Si p es un polinomio de grado $n \geq 2$, existen $n+1$ números complejos $c_1, c_2, \ldots, c_n, \alpha \in \mathbb{C}$ de modo que $p(x) = \alpha(x-c_1)(x-c_2)\cdots(x-c_n)$ y p es, por tanto, reducible.
3. Supongamos que $p \in \mathcal{P}(\mathbb{R})$ tiene grado 2, sus dos raíces son complejas (con parte imaginaria distinta de cero) y p es reducible en $\mathcal{P}(\mathbb{R})$. Entonces existen polinomios $q_1, q_2 \in \mathcal{P}(\mathbb{R})$, de grado 1 y tales que $p = q_1 q_2$. Pero esto significa que la raíz real de q_1 (y de q_2) también es raíz de p y, con ello, p tendría, al menos, 3 raíces, lo que no es posible si p es un polinomio de grado 2.
4. En este caso, si $c_1, c_2 \in \mathbb{R}$ son las raíces de p, entonces existe $\alpha \in \mathbb{R}$ de modo que $p(x) = \alpha(x-c_1)(x-c_2)$ y p es, por tanto, reducible.

5. Si $p \in \mathcal{P}(\mathbb{R})$ tiene grado $n > 2$, entonces, por el teorema fundamental del Álgebra, p tiene n raíces complejas, no necesariamente distintas entre sí y

$$p(x) = \alpha\,(x - c_0)^{l_0}\,\cdots\,(x - c_r)^{l_r}.$$

Supongamos que, de esas raíces, m son complejos reales y las restantes tienen parte imaginaria distinta de cero. Denotemos por $a_0,\, a_1,\, \cdots,\, a_{m-1}$ a las raíces que son complejos reales y por $\alpha_1 \pm i\,\beta_1,\, \cdots,\, \alpha_s \pm i\,\beta_s$ a las que son complejas con parte imaginaria distinta de cero. Entonces,

$$p(x) = \alpha(x-a_0)^{l_0}\cdots(x-a_{m-1})^{l_{m-1}}(x-(\alpha_1+i\,\beta_1))^{l_m}(x-(\alpha_1-i\,\beta_1))^{l_m}\cdots(x-(\alpha_s+i\,\beta_s))^{l_r}(x-(\alpha_s-i\,\beta_s))^{l_r}$$

y $l_0 + l_1 + \ldots + l_{m-1} + 2(l_m + \ldots + l_r) = n$. Observando que

$$\big(x - (\alpha_j + i\,\beta_j)\big)\,\big(x - (\alpha_j - i\,\beta_j)\big) = x^2 - 2\,\alpha_j\,x + \alpha_j^2 + \beta_j^2$$

es un polinomio de grado 2 con coeficientes reales que no tiene raíces reales, p puede escribirse como

$$p(x) = \alpha\,(x - a_1)^{l_1}\,\cdots\,(x - a_r)^{l_m}\,\big(x^2 - 2\,\alpha_1\,x + \alpha_1^2 + \beta_1^2\big)^{l_{m+1}}\,\cdots\,\big(x^2 - 2\,\alpha_s\,x + \alpha_s^2 + \beta_s^2\big)^{l_r}.$$

Para que p fuera irreducible tendría que: 1) no tener raíces reales: $m = 0$; 2) tener solo un par de raíces complejas distintas conjugadas entre sí: $r = m + 1$; y 3) que la multiplicidad de esas raíces sea 1: $l_{m+1} = 1$. Pero en ese caso $n = \mathrm{gr}(p) = \mathrm{gr}\big(x^2 - 2\,\alpha_1\,x + \alpha_1^2 + \beta_1^2\big) = 2$, lo cual contradice la hipótesis de $n > 2$.

$\square$

Del mismo modo en que todo número natural puede escribirse de manera única como producto de potencias de números primos, todo polinomio $p \in \mathcal{P}(\mathbb{K})$ de grado mayor o igual que 1 puede escribirse, de manera única, salvo constante multiplicativa, como un producto de la forma

$$p_1 p_2 \ldots p_m.$$

En el lema anterior ya se vió una forma de factorizar un polinomio en un producto polinomios irreducibles $p_1, p_2, \ldots, p_m$, para cualquier p de grado mayor o igual que 1.