8. Polinomios

En este capítulo vamos a introducir uno de los principales objetos de estudios del Álgebra: los polinomios. Los polinomios poseen una estructura algebraica muy rica que es similar a la teoría de números enteros (mejor conocida como Teoría de números*) y aparecen prácticamente en todas las ramas de la Matemática. En este curso, estudiaremos los resultados más relevantes de esta teoría.*

8.1 ¿Qué es un polinomio?

Los polinomios son expresiones que se construyen a partir de números y potencias de una variable x. Aquí los trabajaremos desde una visión algebraica.

En este apartado estudiaremos...

- La definición de polinomio de una variable como objeto algebraico.
- Las operaciones que pueden llevarse a cabo entre polinomios.
- La evaluación de polinomios en números.

8.1.1 La visión algebraica de los polinomios

Los polinomios suelen ser considerados como un tipo especial de funciones reales. Si bien esta interpretación es válida, los polinomios poseen una estructura muy *regular*, lo que permite realizar operaciones entre ellos y tratarlos como objetos algebraicos. Los polinomios constan de una única variable x, que es elevada a distintas potencias, cada una de estas potencias es multiplicada por una constante (número) y, finalmente, todos estos términos son sumados entre sí. Si lo relacionamos con la noción de combinación lineal que estudiamos en el capítulo 3, se lo puede pensar como una *combinación lineal de potencias de* x. Veremos más adelante que esta interpretación es, de hecho, bastante acertada. La importancia de los polinomios desde el punto de vista algebraico, es que admiten operaciones conocidas, como la suma, multiplicación y división, y, en cada caso, el resultado vuelve a ser un polinomio. En este sentido, el conjunto de estas funciones no es simplemente un conjunto, sino que es lo que se conoce como un *anillo* (un conjunto con una estructura algebraica muy rica).

Definición 78 Un *polinomio* $P(x)$ en una indeterminada (o variable) x con coeficientes en $\mathbb{C}$ es una expresión de la forma:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x + a_0,$$

donde los $a_0, \ldots, a_n$ son números complejos. Si todos los a_i son números reales, decimos que $P(x)$ es un polinomio con coeficientes en $\mathbb{R}$ y si todos los a_i son racionales, que $P(x)$ es un polinomio con coeficientes en $\mathbb{Q}$. El índice i más grande tal que $a_i \neq 0$ se llama el *grado* del polinomio y se nota $gr(P)$.

Las constantes $a_0, a_1, ..., a_n$ se llaman *coeficientes* del polinomio. Al coeficiente a_0 se le da el nombre de *término independiente* y al coeficiente a_n, el de *coeficiente principal*. Cuando el coeficiente principal es 1, al polinomio se le llama *mónico*. El conjunto de polinomios con coeficientes complejos se nota $\mathbb{C}[x]$, el de polinomios con coeficientes reales, $\mathbb{R}[x]$, y el de polinomios con coeficientes racionales, $\mathbb{Q}[x]$. Por supuesto, $\mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$.

Importante En general, vamos a usar $\mathbb{K}$ para representar alguno de los conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$, de forma que $\mathbb{K}[x]$ representará el conjunto de polinomios con coeficientes en $\mathbb{K}$. De esta manera, vamos a poder enunciar resultados de manera más sencilla (utilizando el $\mathbb{K}$), en lugar de tener que escribir un enunciado para cada conjunto numérico $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. ■

■ **Ejemplo 82**

- $P(x) = 1$ es un polinomio donde el único coeficiente no nulo es el término independiente (no aparece explícitamente la variable x). En general, un polinomio $P(x) = \lambda \in \mathbb{C}$, con $\lambda \neq 0$, se llama *polinomio constante*. El grado de un polinomio constante es 0.
- Observemos que, en el caso de los polinomios constantes, hemos descartado la posibilidad que la constante sea el 0. El polinomio $P(x) = 0$ es un polinomio especial que se llama *polinomio nulo* y *no tiene grado*. Entenderemos esta diferenciación con los polinomios constantes cuando veamos el producto de polinomios.
- $Q(x) = 2x - 5$ es un polinomio de grado 1. Su coeficiente principal es 2 y su término independiente es -5. A los polinomios de grado 1 se los llama *polinomios lineales*.
- $R(x) = -\frac{2}{5}x^2 - 3x + 7$ es un polinomio de grado 2. Su coeficiente principal es $-\frac{2}{5}$ y su término independiente es 7. A los polinomios de grado 2 se los llama *polinomios cuadráticos*. Tengamos en cuenta que las ecuaciones cuadráticas que estuvimos resolviendo en el apartado 3 del capítulo anterior, son precisamente polinomios cuadráticos en $\mathbb{C}[x]$.
- $N(x) = x^4 + 1$ y $M(x) = 3x^4 - 2x^3 + 5x^2 - x$ son polinomios de grado 4. El primero es mónico (su coeficiente principal 1); el segundo, no. Consideremos que el término independiente de $M(x)$ es 0.
- $S(x) = x^3 - 3ix^2 + (1 - 2i)x + 7i$ es un polinomio con coeficientes complejos. A diferencia de los ejemplos anteriores, este polinomio no está en $\mathbb{R}[x]$.

■

Observación 51 *Así como consideramos $\mathbb{R} \subset \mathbb{C}$ mediante la identificación $\mathbb{R} = \{a + bi \ : \ b = 0\}$, también podemos considerar los números complejos como contenidos en los polinomios con coeficientes complejos; es decir, $\mathbb{C} \subset \mathbb{C}[x]$. La identificación, por supuesto, es interpretar a $\mathbb{C}$ como el conjunto de polinomios constantes; es decir, $\mathbb{C} = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x] \ : \ a_n = a_{n-1} = \cdots = a_2 = a_1 = 0\}$. De la misma manera, podemos considerar $\mathbb{R} \subset \mathbb{R}[x]$ y $\mathbb{Q} \subset \mathbb{Q}[x]$.*

8.1.2 Operaciones con polinomios

Comentamos en el comienzo del capítulo que los polinomios se pueden sumar, multiplicar e, inclusive, dividir.

Primero veamos *suma y resta de polinomios*. Para sumar (o restar) dos polinomios, se agrupan los términos de igual grado y se suman (o restan) sus coeficientes. Por ejemplo, si $P(x) = 2x^4 - 5x^3 + x - 7$ y $Q(x) = 6x^4 + x^3 - 2x^2 - 6x + 9$, el polinomio $P(x) + Q(x)$ se calcula:

$$\begin{aligned} P(x) + Q(x) &= (2x^4 - 5x^3 + x - 7) + (6x^4 + x^3 - 2x^2 - 6x + 9) \\ &= (2+6)x^4 + (-5+1)x^3 - 2x^2 + (1-6)x + (-7+9) \\ &= 8x^4 - 4x^3 - 2x^2 - 5x + 2 \end{aligned}$$

Por otro lado, el polinomio $P(x) - Q(x)$ se calcula:

$$\begin{aligned} P(x) - Q(x) &= (2x^4 - 5x^3 + x - 7) - (6x^4 + x^3 - 2x^2 - 6x + 9) \\ P(x) + Q(x) &= (2-6)x^4 + (-5-1)x^3 + (0-(-2))x^2 + (1-(-6))x + (-7-9) \\ &= -4x^4 - 6x^3 + 2x^2 + 7x - 16 \end{aligned}$$

Si P y Q tienen sus coeficientes en $\mathbb{K}$, entonces $P + Q$ y $P - Q$ también.

Experimento 47 Si $gr(P) = n$ y $gr(Q) = m$, observen cuál es el grado de $P + Q$. ■

Prosigamos con *Multiplicación de polinomios*. Para multiplicar dos polinomios, basta aplicar la propiedad distributiva y las leyes de la multiplicación y de las potencias. Es decir, se multiplica cada término de uno de los polinomios por cada término del otro y se suman todas estas multiplicaciones. Por ejemplo, para $P(x) = 2x^4 - 5x^3 + x - 7$ y $Q(x) = 2x^2 - x + 1$, el producto $P(x)Q(x)$ se calcula:

$$\begin{aligned} P(x)Q(x) &= (2x^4 - 5x^3 + x - 7)(2x^2 - x + 1) \\ &= (2x^4 - 5x^3 + x - 7)2x^2 + (2x^4 - 5x^3 + x - 7)(-x) + (2x^4 - 5x^3 + x - 7) \\ &= 4x^6 - 10x^5 + 2x^3 - 14x^2 - 2x^5 + 5x^4 - x^2 + 7x + 2x^4 - 5x^3 + x - 7 \\ &= 4x^6 + (-10x^5 - 2x^5) + (5x^4 + 2x^4) + (2x^3 - 5x^3) + (-14x^2 - x^2) + (7x + x) + (-7) \\ &= 4x^6 - 12x^5 + 7x^4 - 3x^3 - 15x^2 + 8x - 7 \end{aligned}$$

Si P y Q tienen sus coeficientes en $\mathbb{K}$, entonces PQ también.

Experimento 48 Si $gr(P) = n$ y $gr(Q) = m$, observen cuál es el grado de PQ (noten que, como P y Q tienen grado, entonces ninguno es el polinomio nulo). Este experimento explica, en parte, la diferenciación que hacemos entre los polinomios constantes (de grado 0) y el polinomio nulo (que no tiene grado). ■

Igualdad de polinomios. ¿Cuándo dos polinomios son iguales? Cuando tienen el mismo grado y sus coeficientes coinciden término a término. Es decir, decimos que el polinomio $P(x) = a_n x^n + \cdots + a_1 x + a_0$ es igual al polinomio $Q(x) = b_n x^n + \cdots + b_1 x + b_0$ si $a_i = b_i$ para todo i entre 0 y n. Por ejemplo, los polinomios $x^2 + 3x - 2$ y $x^3 + x - 1$ no son iguales porque tienen distinto grado. También, los polinomios $x^3 - 4x^2 - x + 9$ y $x^3 - 4x^2 + 3x + 9$ son distintos, pues el coeficiente que acompaña a x en el primero es -1, mientras que en el segundo es 3.

Una característica a tener en cuenta es lo que se denomina *evaluación de polinomios*. Un hecho importante sobre los polinomios es que se los puede evaluar en números (racionales, reales, complejos). Esto da lugar a una función (que es, seguramente, la manera más común de considerarlos). Por supuesto, la evaluación de un polinomio $P(x) \in \mathbb{K}[x]$ en un número $b \in \mathbb{C}$ consiste simplemente en reemplazar la indeterminada x por el número b en la expresión del polinomio y llevar a cabo la cuenta indicada por el polinomio. Por lo tanto, evaluar un polinomio da como resultado un número. El polinomio $P(x)$ evaluado en un número b se nota $P(b)$. Es decir, si $P(x) = a_n x^n + \cdots + a_1 x + a_0$ entonces:

$$P(b) = a_n b^n + \cdots + a_1 b + a_0 \in \mathbb{C}.$$

Por ejemplo, si $P(x) = x^3 - 4x^2 + 3x + 9$, entonces $P(-2) = (-2)^3 - 4(-2)^2 + 3(-2) + 9 = -21$.

Un *monomio* es un tipo especial de polinomio que solo tiene un coeficiente que no es cero. Dicho de otra manera, un monomio es un polinomio de la forma $P(x) = ax^n$ con $a \neq 0$. La importancia de los monomios es que *todo polinomio es una suma de monomios*.

$$P(x) = \underbrace{a_n x^n}_{monomio} + \underbrace{a_{n-1} x^{n-1}}_{monomio} + \ldots + \underbrace{a_2 x^2}_{monomio} + \underbrace{a_1 x}_{monomio} + \underbrace{a_0}_{monomio}$$

De hecho, la expresión *polinomio* expresa que es un objeto que consta de varios monomios. Cabe aclarar que los polinomios constantes se consideran monomios de grado 0 (pues $a = ax^0$). Veremos, más adelante, que los monomios son muy útiles a la hora de llevar a cabo muchas operaciones. Esto no debería sorprendernos, ya que sumando monomios podemos “generar” todos los polinomios.

La palabra “generar” utilizada en la última oración no es casualidad. Sucede que $\mathbb{C}[x]$ también es un espacio vectorial (donde la suma es la suma de polinomios y el producto por escalar es el producto de un polinomio por otro polinomio constante). Un sistema de generadores natural para el espacio de todos los polinomios consta de los monomios de todas los grados: $\{1, x, x^2, x^3, \ldots, x^n, \ldots\}$. Noten que, pensado de esta manera, los polinomios son precisamente las combinaciones lineales de los monomios.

¿Qué hicimos en el apartado 8.1?

- Definimos a los polinomios como objetos algebraicos y las operaciones entre polinomios (suma y multiplicación). Vimos que estas operaciones cumplen propiedades idénticas a las operaciones con números reales o complejos.
- Determinamos cuándo dos polinomios son iguales y desarrollamos la idea de evaluar un polinomio en un número.
- Definimos los monomios como los polinomios de la forma ax^n.

8.2 División de polinomios

Vamos ahora a aprender cómo llevar a cabo la división entre dos polinomios y a estudiar algunos resultados fundamentales de la Teoría de divisibilidad.

En este apartado estudiaremos...

- El algoritmo de división.
- Teorema del resto.

8.2.1 ¿A qué se le llama dividir dos polinomios?

La división de polinomios se define de manera análoga a la división entre números enteros. ¿Qué hacíamos para dividir dos números enteros? Pues dividir $a \in \mathbb{Z}$ por $b \in \mathbb{Z}$ consistía en encontrar enteros $q, r \in \mathbb{Z}$ tales que $a = qb + r$ para $0 \leq r < b$. El número q se llamaba el *cociente* de la división y el número r el *resto*. También, el número a era el *dividendo* y el número b el divisor. El propósito de dividir el número a por b es ver cuántas veces “entra” en a el número b (dado por el cociente q) y, si no entra “justo”, cuánto “sobra” antes de poder completar a (el resto r). El hecho que pidamos que el resto sea mayor a cero y menor que el divisor hace que haya *únicos* enteros $q, r \in \mathbb{Z}$ que verifiquen $a = qb + r$. Por ejemplo, la división de 572 por 12 tiene por cociente $q = 47$ y por resto $r = 8$. En efecto, $572 = 12{,}47 + 8$ y el resto 8 es mayor a cero y menor que 12. Conocemos ya desde la escuela primaria una manera de llevar a cabo a mano la división de dos números enteros, ¡y la manera de hacerlo con polinomios es prácticamente igual! De hecho, veremos que en cierta forma es mucho más sencillo.

Primero, veamos a qué nos referimos específicamente con "división de dos polinomios". Consideremos el siguiente teorema:

Teorema 52 Dados polinomios $P, Q \in \mathbb{K}[x]$, con $Q \neq 0$, existen *únicos* polinomios C y R en $\mathbb{K}[x]$ tales que:

- $P = QC + R$ y
- o bien, $R = 0$ (el polinomio nulo) o bien, $gr(R) < gr(Q)$.

Notemos que el Teorema 52 es un resultado análogo a lo que vale en el caso de los números enteros: el cociente de la división de P por Q nos dice cuantas veces "entra" el polinomio Q dentro de P y, si no entra "justo", el resto nos indica "cuánto le sobra" para entrar justo. Observemos que, también, en lugar de pedir que el resto sea un número mayor o igual a cero y menor estricto que el divisor, pedimos que el resto sea un polinomio *de grado* mayor o igual que cero o menor o igual que el *grado* del divisor. Esto es porque no hay un orden natural entre los polinomios, pero sí hay un orden natural entre los grados de los polinomios. A lo largo del texto hablaremos de polinomios "más pequeños" o "más grandes", estas frases deben entenderse como una definición a partir del hecho de que dados dos polinomios, no iguales, el grado de uno es mayor que el del otro. Entonces al mayor se lo denomina "más grande" mientras que al de menor grado "más pequeño". El estudiante debe tener en cuenta, mientras lee, que debe llegar a familiarizarse con estas formas de expresión típicas. También, al igual que el caso de los enteros, el polinomio $P(x)$ es llamado el *dividendo*, el polinomio $Q(x)$, el *divisor*, el polinomio $C(x)$, el *cociente* y el polinomio $R(x)$, el *resto*. Por lo tanto, cuando nos referimos a "hacer la división entre dos polinomios" lo que vamos a querer hallar es el cociente y el resto de dicha división.

Observación 53 *Observemos que si P, Q tienen coeficientes en $\mathbb{K}$ entonces su cociente y resto también.*

8.2.2 El algoritmo de división

La forma para llevar a cabo el cálculo de la división entre dos polinomios se conoce como *Algoritmo de división*. Veamos con un ejemplo cómo se procede. Supongamos que queremos dividir el polinomio $P(x) = 3x^5 - 2x^3 + 7x^2 - 2x$ por el polinomio $Q(x) = x^3 + 3x^2 - 1$. Al igual que para números enteros, los ubicamos gráficamente así:

$$3x^5 - 2x^3 + 7x^2 - 2x \quad |\underline{x^3 + 3x^2 - 1}$$

Vamos a empezar a armar el cociente calculando los monomios que lo constituyen uno a la vez (de hecho, del más grande al más chico). Lo que debemos hacer es considerar el monomio de potencia más grande del divisor Q (en este caso es x^3), el monomio más grande del polinomio que estamos dividiendo ($3x^5$) y preguntarnos: ¿por qué otro monomio debo multiplicar a x^3 para "llegar" a $3x^5$? La respuesta es, por supuesto, $3x^2$. Este es, entonces, el primer monomio de cociente.

$$\begin{array}{ll} 3x^5 - 2x^3 + 7x^2 - 2x & |\underline{x^3 + 3x^2 - 1} \\ & \;3x^2 \end{array}$$

Y ahora hacemos lo mismo que en la división de enteros: multiplicamos el divisor por el monomio que acabamos de agregar al cociente y ponemos el resultado debajo del dividendo:

$$\begin{array}{r|l} 3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\ 3x^5 + 9x^4 - 3x^2 & 3x^2 \end{array}$$

Luego, restamos el dividendo por este nuevo polinomio que ubicamos bajo él:

$$\begin{array}{r|l} 3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\ 3x^5 + 9x^4 - 3x^2 & 3x^2 \\ \hline -9x^4 - 2x^3 + 10x^2 - 2x & \end{array}$$

Es importante tener en cuenta que la idea central en este último punto es la de realizar la resta de dos polinomios, con lo cual al principio de su aprendizaje tal vez sea útil que, como cálculo auxiliar, escriba explícitamente dicha operación,

$$(3x^5 - 2x^3 + 7x^2 - 2x) - (3x^5 + 9x^4 - 3x^2) = -9x^4 - 2x^3 + 10x^2 - 2x$$

¿Qué hemos logrado con este procedimiento? ¡Pues ahora nos quedó un polinomio de menor grado en el sector donde estaba el dividendo (en este caso, de grado 4)! Esto nos indica que este procedimiento va a ir disminuyendo los grados de los polinomios bajo el dividendo y, por lo tanto, eventualmente arribaremos a un polinomio de grado menor al divisor (y habremos terminado el cálculo, pues esta es la característica que buscamos en el resto).

Veamos cómo seguimos. En el lugar del dividendo, nos quedó el polinomio $-9x^4 - 2x^3 + 10x^2 - 2x$, cuyo monomio principal es $-9x^4$. Nos preguntamos nuevamente, ¿por qué monomio tenemos que multiplicar a x^3 para llegar a $-9x^4$? La respuesta es $-9x$. Entonces, sumamos este monomio al cociente:

$$\begin{array}{r|l} 3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\ 3x^5 + 9x^4 - 3x^2 & 3x^2 - 9x \\ \hline -9x^4 - 2x^3 + 10x^2 - 2x & \end{array}$$

Hacemos a continuación la multiplicación de este monomio (y solo este monomio) por Q y lo ubicamos debajo del último polinomio que calculamos:

$$\begin{array}{r|l} 3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\ 3x^5 + 9x^4 - 3x^2 & 3x^2 - 9x \\ \hline -9x^4 - 2x^3 + 10x^2 - 2x & \\ -9x^4 - 27x^3 + 9x & \end{array}$$

y restamos estos últimos dos polinomios:

$$\begin{array}{r|l} 3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\ 3x^5 + 9x^4 - 3x^2 & 3x^2 - 9x \\ \hline -9x^4 - 2x^3 + 10x^2 - 2x & \\ -9x^4 - 27x^3 + 9x & \\ \hline 25x^3 + 10x^2 - 11x & \end{array}$$

Como este último polinomio obtenido aún no tiene grado menor al grado del divisor, continuamos. ¿Por qué monomio tenemos que multiplicar x^3 para "deshacernos" del $25x^3$? Por 25 (recuerden que las constantes también son monomios). Siguiendo el mismo procedimiento que antes, tenemos:

$$\begin{array}{r|l}
3x^5 - 2x^3 + 7x^2 - 2x & \underline{x^3 + 3x^2 - 1} \\
3x^5 + 9x^4 - 3x^2 & 3x^2 - 9x + 25 \\
\hline
-9x^4 - 2x^3 + 10x^2 - 2x & \\
-9x^4 - 27x^3 + 9x & \\
\hline
25x^3 + 10x^2 - 11x & \\
25x^3 + 75x^2 + 25 & \\
\hline
-65x^2 - 11x + 25 &
\end{array}$$

Y ahora sí, como en el lugar del dividendo arribamos a un polinomio de grado menor a 3, terminamos con la división. El resultado obtenido es que el cociente de la división entre P y Q es $C(x) = 3x^2 - 9x + 25$ y el resto $R(x) = -65x^2 - 11x + 25$. Pueden corroborar que:

$$3x^5 - 2x^3 + 7x^2 - 2x = (3x^2 - 9x + 25)(x^3 + 3x^2 - 1) + (-65x^2 - 11x + 25)$$

¿Qué sucede si el grado del dividendo P es menor que el grado del divisor Q? ¡En este caso la división es obvia! El cociente es 0 y el resto es P (de forma que $P = 0.Q + P$). Notemos que el cociente y el resto, así definidos, cumplen las condiciones del Teorema 52. Además, la interpretación de este hecho es natural: si $gr(Q) > gr(P)$, entonces Q no puede "entrar" siquiera una vez dentro de P, por lo que el cociente es 0. Les dejamos para pensar en el siguiente experimento otra situación especial del algoritmo de división.

Experimento 49 ¿Cómo es el cociente y el resto de la división entre P y Q si ambos polinomios tienen el mismo grado? ■

Veamos otro ejemplo del algoritmo de división. Supongamos que queremos hacer la división entre $P(x) = -x^3 + 12x^2 - 47x + 60$ por $Q(x) = x - 4$. Escribimos todo junto el procedimiento.

$$\begin{array}{r|l}
-x^3 + 12x^2 - 47x + 60 & \underline{x - 4} \\
-x^3 + 4x^2 & -x^2 + 8x - 15 \\
\hline
8x^2 - 47x + 60 & \\
8x^2 - 32x & \\
\hline
-15x + 60 & \\
15x - 60 & \\
\hline
0 &
\end{array}$$

En este caso, el resto es el polinomio 0, lo que nos dice que $P(x) = Q(x)(-x^2 + 8x - 15)$. Esto es análogo al caso cuando obteníamos resto 0 en la división de número enteros. Por ejemplo, el resto de dividir 455 por 13 es 0, lo que quiere decir que 455 es múltiplo de 13 (o que 13 divide a 455). De la misma manera, se dice que un polinomio $Q(x)$ *divide* a $P(x)$, o que el polinomio $P(x)$ es *divisible* por el polinomio $Q(x)$, si el resto de la división entre $P(x)$ y $Q(x)$ es el polinomio nulo $R(x) = 0$. Veremos al final de la unidad cómo descomponer a los polinomios como producto de sus divisores más pequeños (llamados *factores*).

8.2.3 El Teorema del resto

En algunas situaciones, existe una manera de conocer el polinomio resto con antelación a efectuar la división entre dos polinomios. Y esto resulta útil dado que se puede conocer si la división será exacta (es decir, con resto 0) sin la necesidad de efectuarla. El Teorema del resto permite averiguar el valor del resto de la división entre un polinomio $P(x)$ por otro polinomio de la forma $Q(x) = x - a$, con $a \in \mathbb{C}$, sin necesidad de hacer la división.

Teorema 54 — Teorema del resto. El resto de dividir el polinomio $P(x) \in \mathbb{K}[x]$ por el polinomio $x - a$, con $a \in \mathbb{C}$, es igual a $P(a)$.

Observemos que, como estamos dividiendo por un polinomio de grado 1, entonces el resto de la división entre $P(x)$ y $x - a$ será el polinomio nulo o un polinomio constante. Lo que dice el teorema es que esta constante será precisamente el número $P(a)$. La demostración de este hecho no es complicada: si $C(x)$ y $R(x)$ son el cociente y el resto, respectivamente, de la división entre $P(x)$ y $x-a$, entonces $P(x) = (x-a)C(x)+R(x)$. Si ahora evaluamos al polinomio $P(x)$ en $x = a$, resulta: $P(a) = (a - a)C(a) + R(a) = R(a)$. Como $R(x)$ es un polinomio nulo o un polinomio constante, entonces toma el mismo valor cualquier número en lo que lo evaluemos. En particular, $R(x) = R(a)$, que es lo que queríamos demostrar.

■ **Ejemplo 83** Calculemos el resto de la división de $P(x) = x^3 - 5x^2 + 6x$ por el polinomio $Q(x) = x - 3$. Como el divisor es de la forma $x - a$, entonces podemos usar el Teorema del resto y hallar que el resto es $P(3) = 3^3 - 5(3^2) + 6{,}3 = 27 - 45 + 18 = -18 + 18 = 0$. ■

¿Qué hicimos en el apartado 8.2?

- Estudiamos cómo dividir polinomios (de manera análoga a la división de números enteros).
- Introducimos el concepto de que un polinomio P sea divisible por otro Q (que el resto de la división de P por Q sea el polinomio nulo).
- Enunciamos y demostramos el Teorema del resto, que nos dice cuál es el resto de la división de un polinomio P por un polinomio de la forma $x - a$.

■

8.3 Raíces

Estudiemos, ahora, cómo hallar los *ceros* de los polinomios; esto es, los números que, al evaluarlos en el polinomio, lo anulan.

En este apartado estudiaremos...

- La definición de raíz de un polinomio.
- La relación entre las raíces del polinomio P y los polinomios que dividen a P.
- Cómo buscar raíces de polinomios.
- El Teorema de Gauss.
- La multiplicidad de una raíz.
- El Teorema fundamental del Álgebra.

■

8.3.1 ¿Qué son las raíces de un polinomio?

Ya sabemos que las ecuaciones cuadráticas que resolvimos en el capítulo anterior son, en realidad, ecuaciones polinomiales (determinadas por un polinomio de grado 2). Probablemente ya estén al tanto de que los ceros de una ecuación cuadrática se llaman también *raíces* de la ecuación. Este concepto de raíz es común a todos los polinomios y, ahora, vamos a definirlo de manera general.

Definición 79 Sea $P(x) \in \mathbb{K}[x]$. Un número $a \in \mathbb{C}$ se dice una *raíz* de P si $P(a) = 0$.

Es decir, las raíces son los números donde el polinomio se anula. Notemos que, según el Teorema del resto, el resto de la división entre $P(x)$ y $x - a$ se obtiene como $P(a)$. En particular, si el resto de esta división es $0 \in \mathbb{C}[x]$, entonces $P(a) = 0$. Esto quiere decir que $x = a$ es raíz del polinomio $P(x)$. Por otro lado, si $x = a$ es raíz de $P(x)$, entonces $P(a) = 0$ (por definición de raíz). El Teorema del resto nos dice que el resto de dividir $P(x)$ por $x - a$ es, entonces, $P(a) = 0$, por lo que concluimos que $x - a$ divide a $P(x)$. Hemos hallado, así, que vale la siguiente propiedad:

Importante Un número $a \in \mathbb{C}$ es raíz del polinomio $P(x)$ si, y solo si, $x - a$ divide a $P(x)$. ■

Experimento 50 Supongan que el polinomio $Q(x)$ divide al polinomio $P(x)$. ¿Qué relación hay entre las raíces de $Q(x)$ y las de $P(x)$? ■

Supongamos ahora que a y b son raíces *distintas* del polinomio P. Esto, en particular, nos dice que tanto $x - a$ como $x - b$ dividen a P. ¿Es cierto que el polinomio cuadrático $(x - a)(x - b) = x^2 - (a + b)x + ab$ también divide a P? ¡Sí! Como $x - a$ divide a $P(x)$ entonces $P(x) = (x - a)Q(x)$ para cierto polinomio $Q(x)$. Ahora, como b es raíz de P, entonces $P(b) = 0$. Pero $P(b) = (b - a)Q(b)$. Como estamos suponiendo que $b \neq a$, entonces $b - a \neq 0$, por lo que, para que $(b - a)Q(b) = 0$, debe ser $Q(b) = 0$. Esto nos dice que b es raíz de $Q(b)$ y, por lo tanto, $(x - b)$ divide a Q. Entonces, podemos escribir $Q(x) = (x - b)R(x)$ para cierto polinomio R. De esta manera, hallamos que

$$P(x) = (x - a)Q(x) = (x - a)(x - b)R(x) = (x^2 - (a + b)x + ab)R(x).$$

Observemos que, si seguimos repitiendo el razonamiento para $R(x)$, podemos probar que, si tenemos varias raíces distintas $\lambda_1, \dots, \lambda_t$ de $P(x)$, entonces el producto $(x-\lambda_1)(x-\lambda_2)\dots(x-\lambda_t)$ divide a $P(x)$. Lo dejamos asentado en el siguiente lema.

Lema 55 Si varios polinomios de la forma $x - \lambda_1, \dots, x - \lambda_t$ dividen a P y todos los λ_i son distintos entre sí, entonces el producto $(x - \lambda_1) \dots (x - \lambda_t)$ también divide a P.

8.3.2 ¿Cómo encontrar raíces de un polinomio?

Encontrar raíces de polinomios es un problema central del Álgebra y el Análisis Matemático. Ahora bien, ¿cómo encontramos las raíces? La primera observación que podemos hacer es que *ya sabemos cómo encontrar las raíces de polinomios lineales y cuadráticos*. En efecto, para un polinomio lineal $a_1x + a_0$ (con $a_1 \neq 0$) solo debemos despejar x de la ecuación $a_1x + a_0 = 0$. O sea, la única raíz es $x = -\frac{a_0}{a_1}$. Por otro lado, a un polinomio cuadrático $a_2x^2 + a_1x + a_0$ (con $a_2 \neq 0$), también sabemos calcularle las raíces: utilizamos la fórmula resolvente:

$$x_1, x_2 = \frac{-a_1 + \sqrt{a_1^2 - 4a_2a_0}}{2a_2}$$

para la cual ya vimos, en el capítulo anterior, que siempre tiene dos soluciones en los números complejos. Para polinomios de grados mayores, ya no tenemos procedimientos o fórmulas directas para hallar las raíces. La estrategia general es ir hallando progresivamente las raíces de un polinomio $P(x)$ de la siguiente manera:

- Conseguir (de alguna manera) una raíz $a \in \mathbb{C}$ de $P(x)$.
- Como sabemos que $x - a$ divide a $P(x)$, hallar el cociente $C(x)$ de dicha división, de manera que $P(x) = (x - a)C(x)$. Recuerden que $C(x)$ tiene grado menor a $P(x)$.

- Si $C(x)$ tiene grado 1 o 2, calcular, usando las fórmulas conocidas, las raíces de $C(x)$ (que también son raíces de $P(x)$). Si el grado de $C(x)$ es mayor a 2, repetir el procedimiento para $C(x)$.

Notemos que esta estrategia pide conseguir una raíz *de alguna manera* para comenzar. Algunas veces, las raíces se pueden identificar rápidamente (por ejemplo, si el polinomio no tiene término independiente entonces $x = 0$ es raíz) y otras veces son datos del problema. El siguiente teorema, debido a Gauss, nos permite anticipar las posibles raíces *racionales* de un polinomio con coeficientes *enteros*.

Teorema 56 — Teorema de Gauss. Sea $P(x) = a_n x^n + \cdots + a_1 x + a_0$ con $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$. Si el número racional $\frac{p}{q}$ es raíz del polinomio ($q \neq 0$), siendo $\frac{p}{q}$ una fracción irreducible, entonces p divide a a_0 y q divide a a_n. En particular, si $P(x)$ es un polinomio mónico (el coeficiente principal $a_n = 1$), las posibles raíces racionales del polinomio son los divisores del término independiente a_0.

Es importante remarcar que este teorema *no nos dice* que un polinomio con coeficientes enteros tiene raíces racionales. Lo que dice es que, *de existir raíces racionales*, estas deben forzosamente ser de una manera determinada. Es decir, "si tiene, son de esta forma". Es por esta razón para determinar si tiene raíces racionales, debemos probar con los números racionales que tienen la forma anticipada por el teorema. Pero podría ser que ninguno sea raíz, y por lo tanto, el polinomio en cuestión no tendría raíces racionales (solo reales y complejas).

Ejemplos 84

- Consideremos el polinomio $P(x) = x^3 - 3x^2 - 2x + 6$. Como tiene coeficientes enteros, el Teorema de Gauss nos indica que, de tener una raíz racional $\frac{p}{q}$, debe suceder que p debe dividir al término independiente 6 y q debe dividir al coeficiente principal 1. En este caso, las únicas posibilidades para q son 1 y -1. Por otro lado, las posibilidades para p son los posibles divisores de 6: $1, -1, 2, -2, 3, -3, 6, -6$. Probando con todos encontramos que $P(3) = 0$. Hemos hallado, entonces, una raíz racional (de hecho, entera) de $P(x)$.
- Consideremos ahora el polinomio $Q(x) = 2x^4 - 10x^2 + 12$. Nuevamente, como tiene coeficientes enteros, podemos utilizar el Teorema de Gauss para ver si tiene alguna raíz racional $\frac{p}{q}$. En este caso, p debe dividir a 12 y q a 2. Las opciones para q son $1, -1, 2, -2$ y las opciones para p son $1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12$. Por lo tanto, todas las posibles opciones para $\frac{p}{q}$ se obtienen eligiendo un numerador p entre las doce opciones disponibles y un denominador q entre las cuatro opciones disponibles. Esto da un total de $12{,}4 = 48$ posibles opciones a considerar. Sin embargo, hay muchas combinaciones que dan como resultado el mismo número racional. Por ejemplo, $\frac{1}{-1}$ y $\frac{-1}{1}$; o $\frac{4}{2}$ y $\frac{2}{1}$. Al mirar con detenimiento se puede advertir que las opciones que hay que chequear son las siguientes:

$$\frac{p}{q} = 1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}.$$

  Al verificar todas estas posibilidades, no se encuentra ningún número que anule al polinomio. Por lo tanto, $P(x)$ no tiene raíces racionales.

Un dato interesante sobre el Teorema de Gauss es que proporciona una demostración del hecho que $\sqrt{2}$ no es un número racional. En efecto, consideremos el polinomio $P(x) = x^2 - 2$. Claramente, $\sqrt{2}$ es raíz de $P(x)$. Pero $\sqrt{2}$ no puede ser racional pues el Teorema de Gauss nos dice que, si un racional $\frac{p}{q}$ es raíz de P, entonces p divide a 2 y q divide a 1. Como las únicas posibilidades para q son 1 o -1 entonces una raíz racional $\frac{p}{q}$ es en realidad un número entero. Por lo tanto, si $\sqrt{2}$ fuera racional debería ser un número entero (que sabemos que no es).

Vamos a ver ahora qué es la *multiplicidad de una raíz*. Consideremos el polinomio $P(x) = x^2 - 2x + 1$. El Teorema de Gauss nos dice que las únicas posibles raíces racionales de $P(x)$ son 1 o -1. Es fácil ver que $x = 1$ es una raíz $P(x)$. Por lo visto en el apartado 8.3.1, sabemos que $x - 1$ divide a $P(x)$. Si ahora hacemos la división entre $P(x)$ y $x - 1$, hallamos que el cociente de la división es también $x - 1$. Es decir, se tiene que:

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

El hecho de que $P(x)$ "sea divisible" dos veces de $x - 1$ se interpreta diciendo que $x = 1$ es *raíz doble* de $P(x)$ o que es una *raíz de multiplicidad* 2. Definimos esta noción de manera general a continuación:

Definición 80 Sea $P(x) \in \mathbb{K}[x]$. Un número $a \in \mathbb{C}$ se dice una *raíz de multiplicidad* k de $P(x)$ si el polinomio $(x - a)^k$ divide a $P(x)$, pero el polinomio $(x - a)^{k+1}$, no. Dicho de otra manera, existe un polinomio $C(x)$ tal que $C(a) \neq 0$ y $P(x) = (x - a)^k C(x)$. Si $k = 1$, entonces a recibe el nombre de *raíz simple* y si $k > 1$, *raíz múltiple*.

■ **Ejemplo 85** El polinomio $P(x) = x^5 + 7x^4 + 18x^3 + 20x^2 + 8x$ tiene 5 raíces: la raíz $x = -2$ con multiplicidad 3, la raíz $x = -1$ con multiplicidad 1 y la raíz $x = 0$, también con multiplicidad 1. Pueden verificar que $P(x) = (x + 2)^3(x + 1)x$. ■

Si conocen la noción de derivada de una función, podrán advertir que la derivada de un polinomio (visto como función) es nuevamente un polinomio (de un grado menos). Una definición alternativa del concepto de multiplicidad es la siguiente: una raíz de $P(x)$ tiene multiplicidad k si también es raíz de los primeros k polinomios derivados $P'(x), P''(x), \dots, P^{(k)}(x)$ de $P(x)$, pero no de la derivada $(k+1)$-ésima de $P(x)$.

En este punto queremos poder responder la pregunta *¿Cuántas raíces tiene un polinomio?* El Teorema de Gauss nos ayuda a encontrar raíces racionales. En algunos casos las hallamos y en otros, no. Si queremos buscar todas las raíces de un polinomio, ¿cómo sabemos cuándo parar? ¿Cuántas raíces puede tener un polinomio? ¿Puede no tener ninguna? No es difícil ver que un polinomio de grado n no puede anularse en más de n números. Se los dejamos para pensar en el siguiente experimento:

Experimento 51 Sea $P(x) \in \mathbb{K}[x]$ de grado n. Vamos a ver que $P(x)$ no puede tener más de n raíces. Si $P(x)$ no tiene raíces, entonces lo que estamos tratando de ver es cierto (si no tiene ninguna raíz, no tiene más de n). Supongamos que posee al menos una raíz a. Sabemos que $x - a$ divide a $P(x)$ y que, por lo tanto, $P(x) = (x - a)C(x)$, donde $C(x)$ es el cociente de la división. ¿Qué grado tiene $C(x)$? Observemos que si, ahora, $C(x)$ no tiene raíces, entonces, nuevamente, hemos visto que $P(x)$ no tiene más de n raíces. ¿Qué harían si $C(x)$ tiene al menos una raíz? ¿Cómo seguirían el razonamiento? ¿Cómo concluyen el resultado? Recuerden el Experimento 50. ■

Sabemos, entonces, que un polinomio de grado n tiene, a lo sumo, n raíces. Pero, ¿puede haber polinomios sin raíces? El siguiente teorema, que fue probado por Gauss, contesta esta pregunta. Es llamado (ni más ni menos) el *Teorema fundamental del Álgebra*.

Teorema 57 Todo polinomio $P(x) \in \mathbb{C}[x]$ *[Teorema fundamental del Álgebra (TFA)]* de grado mayor a cero tiene, al menos, una raíz *compleja*.

En este teorema hemos remarcado que la raíz es compleja (lo que abarca, por supuesto, enteros, racionales y reales) pues, de lo contrario, el resultado no vale. Por ejemplo, ya vimos que el polinomio $x^2 + 1$ no tiene ninguna raíz real.

Pese a que el TFA habla de la existencia de, al menos, una raíz, podemos, en realidad, dar un enunciado más preciso de este resultado (que se deduce de este teorema que hemos escrito) y decir cuántas raíces tiene exactamente un polinomio de grado n.

Teorema 58 *[Enunciado equivalente del TFA]* Todo polinomio $P(x) \in \mathbb{C}[x]$ de grado $n > 0$ tiene exactamente n raíces *complejas* (no necesariamente distintas; es decir, contadas con multiplicidad).

Aunque este último enunciado parezca más "fuerte" que el del TFA, ambos teoremas se deducen uno del otro. En efecto, si vale el enunciado equivalente al TFA, entonces todo polinomio de grado n tiene exactamente n raíces. Pero esto quiere decir que, en particular, tiene al menos una. Por lo tanto, se tiene que vale el TFA. Les dejamos en un experimento para que vean que se deduce dicha equivalencia.

Experimento 52 Sea $P(x)$ un polinomio de grado $n > 0$. Veamos, usando el TFA, que $P(x)$ tiene exactamente n raíces. Precisamente por el TFA sabemos que $P(x)$ tiene al menos una raíz $a \in \mathbb{C}$. Por lo tanto, $x - a$ divide a $P(x)$ y se tiene $P(x) = (x - a)C(x)$. ¿Qué harían ahora? ¿Cómo seguirían el razonamiento?■

Observación 59 *Notemos que el Teorema fundamental del Álgebra es un* resultado de existencia *de raíces: solo nos dice qué cantidad debemos buscar, pero no nos dice cómo buscarlas.*

■ **Ejemplos 86**

- Hallemos todas las raíces del polinomio $P(x) = x^4 + 2x^3 - 7x^2 - 8x + 12$. Por el TFA debemos buscar cuatro raíces. El polinomio P tiene como coeficiente principal 1 y como término independiente 12. Según el Teorema de Gauss, las posibles raíces son los divisores de 12: $1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12$. Si evaluamos en $x = -1$ obtenemos $P(-1) = (-1)^4 + 2(-1)^3 - 7(-1)^2 - 8(-1) + 12 = 1 - 2 - 7 + 8 - 12 = -12$. Concluimos que $x = -1$ no es raíz de $P(x)$. Si ahora evaluamos en $x = 1$ se tiene $P(1) = (1)^4 + 2(1)^3 - 7(1)^2 - 8(1) + 12 = 1 + 2 - 7 - 8 + 12 = 0$. Entonces, $x = 1$ es raíz de $P(x)$. Haciendo la división de P por $(x - 1)$, obtenemos $P(x) = (x - 1)(x^3 + 3x^2 - 4x - 12)$. El Teorema de Gauss puede ser aplicado nuevamente el polinomio de grado 3. Si evaluamos el polinomio $Q(x)$ en $x = -2$ resulta $Q(-2) = (-2)^3 + 3(-2)^2 - 4(-2) - 12 = -8 + 12 + 8 - 12 = 0$. Haciendo la división de $Q(x)$ y $x + 2$ se tiene $Q(x) = (x + 2)(x^2 + x - 6)$. Aquí podemos utilizar la fórmula de la resolvente para hallar que las raíces de $x^2 + x - 6$ son 2 y -3. Concluímos que las raíces de P son $1, -2, 2$ y 3.
- Busquemos ahora la raíces del polinomio $Q(x) = -2x^3 - 10x^2 - 2x - 10$. El TFA nos dice que tiene que tener tres raíces complejas. Por el Teorema de Gauss, las posibles raíces son $10, -10, 5, -5, \frac{5}{2}, -\frac{5}{2}, 2, -2, 1, -1, \frac{1}{2}, -\frac{1}{2}$. Si evaluamos $Q(-5) = -2(-5)^3 - 10(-5)^2 - 2(-5) - 10 = 250 - 250 + 10 - 10 = 0$. Dividiendo $Q(x)$ por $x + 5$ obtenemos $Q(x) = (x + 5)(-2x^2 - 2)$. Observemos que $-2x^2 - 2$ es un polinomio que no tiene raíces reales (siempre toma valores negativos, por lo que no se anula en ningún valor de x). Para hallar sus raíces complejas podemos utilizar la fórmula de la resolvente o, también, simplemente igualar a 0 (que es más directo en este caso ya que el polinomio no tiene término lineal):

$$\begin{aligned} & -2x^2 - 2 = 0 \\ \Rightarrow \quad & -2x^2 = 2 \\ \Rightarrow \quad & x^2 = \tfrac{2}{-2} \\ \Rightarrow \quad & x^2 = -1 \end{aligned}$$

  Concluimos que las raíces de Q con $-5, i, -i$.

■

Proposición 60 Si $P(x)$ con coeficientes reales y $z \in \mathbb{C}$ es raíz de $P(x)$, entonces $\overline{z}$ también es raíz de $P(x)$.

■ **Ejemplo 87** Supongamos que queremos hallar todas las raíces de $P(x) = x^4 - 7x^3 + 18x^2 - 22x + 12$ y sabemos que $1+i$ es raíz de P. Como P tiene coeficientes reales, entonces $\overline{1+i} = 1-i$ también será raíz de P. Luego, $x-(1+i)$ y $x-(1-i)$ dividen a P y, como $1+i \neq 1-i$, entonces $(x-(1+i))(x-(1-i)) = x^2 - 2x + 2$ divide a P (por Lema 55). Si llevamos a cabo la división, hallamos que $P(x) = (x^2-2x+2)(x^2-5x+6)$. Finalmente, podemos calcular las raíces de $x^2 - 5x + 6$ utilizando la fórmula de la resolvente y hallar que todas las raíces de P son $1+i, 1-i, 2, 3$. ■

Existen polinomios de grado 2 que no tienen raíces. Analicen si es posible que esto suceda con los polinomios de grado 3 cuyos coeficientes son números reales.

¿Qué hicimos en el apartado 8.3?

- Definimos qué son las raíces de los polinomios y las clasificamos según su multiplicidad.
- Vimos que si a es raíz de P entonces $x - a$ divide a P.
- Dimos un procedimiento para encontrar todas las raíces de un polinomio.
- Enunciamos el Teorema de Gauss para buscar raíces racionales en polinomios con coeficientes enteros.
- Enunciamos el Teorema Fundamental del Álgebra que dice que un polinomio de grado $n > 0$ tiene necesariamente n raíces en los números complejos.

■

8.4 Factorización de polinomios

Una de las informaciones más útiles que podemos tener de un polinomio es conocer cuáles polinomios más pequeños lo componen.

En este apartado estudiaremos...

- Qué son los polinomios irreducibles.
- Cómo hallar la descomposición en factores irreducibles de un polinomio en los distintos conjuntos de polinomios $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

■

8.4.1 Polinomios irreducibles

La *descomposición en factores primos* es una herramienta fundamental de la teoría de números enteros. ¿En qué consiste? Recordemos que un número primo es un número entero cuyos únicos divisores positivos son el 1 y él mismo. Los primeros números primos positivos son $2, 3, 5, 7, 11, 13, 17, \ldots$ El 6, por ejemplo, no es primo, pues 2 divide a 6 (por lo que 6 tiene un divisor distinto de 1 y 6). Es un hecho soprendente que los números que no son primos se pueden escribir como producto de potencias de números primos. Tomemos, por ejemplo, el número 60, que se puede escribir como 2^2,3,5; es decir, es producto potencias de 2, 3 y 5, que son números primos. La expresión 2^2,3,5 se llama la *descomposición en números primos* del número 60, y es *única*: no existe otra descomposición del 60 que use otros números primos (u otras potencias de estos mismos primos). Con los polinomios sucede algo prácticamente idéntico: todo polinomio puede descomponerse en *factores irreducibles* (los análogos a los primos en este contexto); y la característica que tiene estos factores irreducibles es que *no pueden escribirse como producto de polinomios más pequeños* (de allí el nombre “irreducibles”).

Definición 81 Un polinomio $P(x) \in \mathbb{K}[x]$, de grado mayor a 0, se dice *irreducible en* $\mathbb{K}$ (o *irreducible en* $\mathbb{K}[x]$) si **no** se puede escribir como producto de dos polinomios de grados mayores a 0 que pertenecen a $\mathbb{K}[x]$. Un polinomio que no es irreducible se dice *reducible*.

Por ejemplo, el polinomio $Q(x) = x^2 - 5x + 6$ no es irreducible en $\mathbb{Q}[x]$, ya que $Q(x) = (x-2)(x-3)$, y tanto $x-2$ como $x-3$ tienen grado mayor a 0 y pertenecen a $\mathbb{Q}[x]$. Por otro lado, el polinomio $P(x) = x^2 + 1$ es irreducible en $\mathbb{R}[x]$, pues no se puede escribir como producto de polinomios de grado mayor a 0. En efecto, sabemos que sus raíces son i y $-i$, por lo cual, tanto $x-i$ como $x+i$, dividen a $P(x)$. Es fácil verificar que $P(x)$ es, exactamente, $(x-i)(x+i)$. Pero los polinomios $x-i$ y $x+i$ *no pertenecen a* $\mathbb{R}[x]$ (pues su término independiente es un número no real). Por lo tanto, $P(x)$ no se puede escribir como producto de polinomios más pequeños *que pertenecen a* $\mathbb{R}[x]$. Lo que notamos es que $P(x)$ se puede escribir como producto de polinomios más pequeños que pertenecen a $\mathbb{C}[x]$. Por lo tanto, el polinomio $P(x)$ *sí* es reducible en $\mathbb{C}[x]$. Observemos que, de este último ejemplo, podemos concluir lo siguiente: *que un polinomio sea o no irreducible depende de dónde lo estemos considerando*. Por supuesto, si un polinomio es irreducible en $\mathbb{C}[x]$, entonces también lo es en $\mathbb{R}[x]$ y en $\mathbb{Q}[x]$ (y si es irreducible en $\mathbb{R}[x]$, también lo es en $\mathbb{Q}[x]$). ¿Se dan cuenta por qué?

Ejemplos 88

- El polinomio $P(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, pues lo únicos polinomios de grado mayor a 1 que lo dividen son $x - \sqrt{2}$ y $x + \sqrt{2}$, que no tienen coeficientes racionales. En particular, sí es reducible en $\mathbb{R}[x]$, dado que $\sqrt{2} \in \mathbb{R}$. Como es reducible en $\mathbb{R}[x]$, también lo es en $\mathbb{C}[x]$.
- El polinomio $Q(x) = x^3 - x^2 + 4x - 4$ es reducible en $\mathbb{Q}[x]$, ya que puede escribirse como $(x^2+4)(x-1)$, y ambos polinomios en este producto grado mayor a cero y coeficientes racionales. También resulta, entonces, reducible en $\mathbb{R}[x]$ y $\mathbb{C}[x]$.
- El polinomio $R(x) = x^2 + 4$ es irreducible en $\mathbb{Q}[x]$ y $\mathbb{R}[x]$. Es reducible en $\mathbb{C}[x]$ ya que $R(x) = (x-2i)(x+2i)$.

■

Consideremos que, en la definición de polinomio irreducible, hemos dejado afuera a los polinomios constantes. *Estos no son considerados polinomios irreducibles ni reducibles*. También, de la misma definición, es fácil deducir que *todos los polinomios de grado* 1 *son irreducibles en cualquier* $\mathbb{K}[x]$.

Veamos como escribir cualquier polinomio como *descomposición en factores irreducibles*. Así como todos los números enteros pueden descomponerse en producto de potencias de primos, los polinomios pueden descomponerse en producto de potencias de polinomios irreducibles. En este sentido, los polinomios irreducibles son los "números primos" de los polinomios. Como mecionamos en el párrafo anterior, la reducibilidad o irreducibilidad de un polinomio varía dependiendo en qué conjunto numérico $\mathbb{K}$ estemos considerando la factorización. Por lo tanto, cuando busquemos la *descomposición en factores irreducibles* de un polinomio, deberemos especificar *respecto de qué conjunto numérico* $\mathbb{K}$ *la estamos buscando*. Por ejemplo, consideremos el polinomio $T(x) = -x^4 - 3x^3 + 9x^2 - 3x + 10$. Su descomposición en $\mathbb{Q}[x]$ es $-(x-2)(x+5)(x^2+1)$. Está también es su descomposición en $\mathbb{R}[x]$. Sin embargo, su descomposición en factores irreducibles en $\mathbb{C}[x]$ es $(x-2)(x+5)(x-i)(x+i)$. Por lo tanto, tiene tres factores irreducibles en $\mathbb{Q}$ y $\mathbb{R}$ pero cuatro en $\mathbb{C}$.

Definición 82 Una *descomposición en factores irreducibles en* $\mathbb{K}[x]$ de un polinomio $P(x) \in \mathbb{K}[x]$ es una escritura de $P(x)$ como producto de potencias polinomios irreducibles en $\mathbb{K}$.

Por ejemplo, una descomposición de $P(x) = 4x^3 - 8x^2 + 4x$ en $\mathbb{Q}[x]$ es $(4x)(x-1)^2$. En este caso, los factores irreducibles son $4x$ y $x-1$ (este último aparece elevado al cuadrado). Notemos que esta descomposición no es única, pues también podríamos escribir $P(x) = x(2x-2)^2$, y aquí los factores irreducibles resultarían x y $(2x-2)$. Lo que sucede en este caso es que hemos "reordenado" el coeficiente principal para que aparezca en un factor o en otro (en el primer caso, en el factor $4x$ y, en el segundo caso, en $2x-2$, donde el 4 aparece al elevar al cuadrado este factor). Este "intercambio" del coeficiente principal no influye en la naturaleza de la factorización y es, de hecho, irrelevante en qué lugar aparezca situado. Para simplificar las cosas, hacemos, entonces, la siguiente convención.

Importante Vamos a convenir que la descomposición en factores irreducibles $\mathbb{K}$ de un polinomio $P(x) \in \mathbb{K}$ es una descomposición en producto de potencias de polinomios irreducibles *mónicos*, *todo multiplicado por una constante de* $\mathbb{K}$. En el ejemplo anterior, escribimos $P(x) = 2x(x-1)^2$ y consideramos que los componentes irreducibles son x y $x-1$, y la constante que multiplica todo es 2. ■

Tengamos en cuenta que, con esta convención, la descomposición en factores irreducibles de un polinomio es única. ¿Se dan cuenta por qué? En general, trabajaremos con polinomios mónicos, por lo que no aparecerá la constante correspondiente al coeficiente principal. El objetivo de este apartado es, entonces, aprender a calcular la descomposición en factores irreducibles de un polinomio. A esta tarea se la conoce como *factorizar el polinomio*.

Observación 61 *Notemos que los polinomios lineales (de grado 1) son* siempre *irreducibles en cualquier conjunto $\mathbb{K}[x]$. Esto es inmediato de la definición de polinomio irreducible y las propiedades del grado de un producto de polinomios.*

Observemos *¿Cómo se halla la descomposición en factores irreducibles de un polinomio?* Estamos ya al tanto de que la descomposición en factores irreducibles está íntimamente ligada a la existencia de raíces del polinomio: si $\lambda \in \mathbb{K}$ es raíz de P entonces $x-\lambda$ divide a P, y viceversa. Por lo tanto, para calcular la factorización de un polinomio podemos intentar buscar todas las raíces del polinomio, de manera de ir obteniendo los factores irreducibles progresivamente. Si alguno de los factores que hallamos no tiene raíces en el $\mathbb{K}$ que estamos trabajando, entonces dicho factor será irreducible en $\mathbb{K}[x]$. Dado que la demostración rigurosa de esto sería demasiado exigente, veamos el procedimiento a partir de algunos casos particulares.

Factoricemos el polinomio $P(x) = x^3 - 5x^2 + 6x$ en cada uno de los tres conjuntos de polinomios con los que trabajamos: $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$. Como $P(x)$ no tiene término independiente, entonces $x = 0$ es una raíz de él. Aquí no necesitamos hacer la división de P por $x-0$, ya que podemos, simplemente, sacar x de factor común: $P(x) = x(x^2-5x+6)$. Ahora, buscamos las raíces de x^2-5x+6, que podemos hallar mediante la fórmula de la resolvente: $x = 2$ y $x = 3$. Por lo tanto, utilizando el Lema 55, se deduce que $P(x) = x(x-2)(x-3)$. Como todos los polinomios en este producto tienen grado 1 entonces son irreducibles en $\mathbb{C}[x]$ (y, por lo tanto, también en $\mathbb{R}[x]$ y $\mathbb{Q}[x]$). Como, además, estos polinomios tienen coeficientes en $\mathbb{Q}$, entonces $x(x-2)(x-3)$ es la factorización de $P(x)$ en $\mathbb{Q}$. Esta también es la factorización en $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

Consideremos ahora el polinomio $T(x) = -x^4 - 3x^3 + 9x^2 - 3x + 10$. El Teorema de Gauss nos dice que las posibles raíces racionales, de existir, son $1, -1, 2, -2, 5, -5, 10, -10$. Evaluando el polinomio en estos números, obtenemos que 2 y -5 son raíces de $T(x)$. Dividiendo $T(x)$ por $(x-2)(x+5) = x^2+3x-10$ hallamos que $T(x) = (x^2+3x-10)(x^2+1)$. Sabemos que x^2+1 no tiene raíces racionales, por lo que es un polinomio irreducible en $\mathbb{Q}$. Por lo tanto, la descomposición de $T(x)$ en $\mathbb{Q}[x]$ es precisamente $(x-2)(x+5)(x^2+1)$. Como x^2+1 tampoco tiene raíces reales, entonces la descomposición en $\mathbb{R}[x]$ es la misma. Por otro lado, x^2+1 se descompone como $(x-i)(x+i)$ en $\mathbb{C}[x]$, por lo que la descomposición de $T(x)$ en $\mathbb{C}[x]$ es $(x-2)(x+5)(x-i)(x+i)$.

Estudiemos, finalmente, cómo factorizar el polinomio $Q(x) = x^6 + x^5 - 3x^4 + 2x^3 + x^2 - 3x + 1$ sabiendo que

$\frac{1}{2} + \frac{\sqrt{3}}{2}$ es una de sus raíces. Notemos que, como $Q(x)$ tiene coeficientes en $\mathbb{Q}$, el hecho que $\frac{1}{2} + \frac{\sqrt{3}}{2}$ sea raíz de $Q(x)$ implica que su conjugada $\frac{1}{2} - \frac{\sqrt{3}}{2}$ también debe ser raíz de $Q(x)$ (por la Proposición 60). Por lo tanto, concluímos que el polinomio

$$\left(x - \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right)\right)\left(x + \left(\frac{1}{2} + \frac{\sqrt{3}}{2}\right)\right) = x^2 - x + 1$$

debe dividir a $Q(x)$. Llevemos a cabo la división.

$$\begin{array}{rl}
x^6 + x^5 - 3x^4 + 2x^3 + x^2 - 3x + 1 & |\underline{x^2 - x + 1} \\
x^6 - x^5 + x^4 & x^4 + 2x^3 - 2x^2 - 2x + 1 \\
\hline
2x^5 - 4x^4 + 2x^3 + x^2 - 3x + 1 & \\
2x^5 - 2x^4 + 2x^3 & \\
\hline
-2x^4 + 0x^3 + x^2 - 3x + 1 & \\
-2x^4 + 2x^3 - 2x^2 & \\
\hline
-2x^3 + 3x^2 - 3x + 1 & \\
-2x^3 + 2x^2 - 2x & \\
\hline
x^2 - x + 1 & \\
\underline{x^2 - x + 1} & \\
0 &
\end{array}$$

Luego:

$$Q(x) = (x^2 - x + 1)(x^4 + 2x^3 - 2x^2 - 2x + 1)$$

Para factorizar $x^4 + 2x^3 - 2x^2 - 2x + 1$ en $\mathbb{Q}[x]$ recurrimos al Teorema de Gauss, donde vemos que las únicas posibilidades son 1 y -1. Como ambos números anulan a $x^4 + 2x^3 - 2x^2 - 2x + 1$ podemos concluir que $(x^2 - 1)$ divide a $x^4 + 2x^3 - 2x^2 - 2x + 1$. Hacemos esta división.

$$\begin{array}{rl}
x^4 + 2x^3 - 2x^2 - 2x + 1 & |\underline{x^2 - 1} \\
x^4 - x^2 & x^2 + 2x - 1 \\
\hline
2x^3 - x^2 - 2x + 1 & \\
2x^3 - 2x & \\
\hline
-x^2 + 1 & \\
\underline{-x^2 + 1} & \\
0 &
\end{array}$$

Hasta aquí hemos hallado que

$$Q(x) = (x^2 - x + 1)(x - 1)(x + 1)(x^2 + 2x - 1)$$

Observemos que $x^2 + 2x - 1$ es irreducible en $\mathbb{Q}[x]$ pues, nuevamente por Teorema de Gauss, las únicas posibles raíces racionales son 1 y -1, y ninguna anula a $x^2 + 2x - 1$. Por lo tanto, la factorización de $Q(x)$ en $\mathbb{Q}[x]$ es precisamente $(x^2 - x + 1)(x - 1)(x + 1)(x^2 + 2x - 1)$.

Ahora, como $x^2 - x + 1$ es irreducible en $\mathbb{R}[x]$ (pues sus raíces son complejas no reales), entonces, para hallar la factorización de $Q(x)$ en $\mathbb{R}[x]$, debemos chequear la reducibilidad de $x^2 + 2x - 1$. Las raíces de este polinomio vienen dadas por:

$$\frac{-2 + \sqrt{4 + 4}}{2} = -1 + \sqrt{2} \in \mathbb{R}$$

$$\frac{-2-\sqrt{4+4}}{2} = -1-\sqrt{2} \in \mathbb{R}$$

Luego, la factorización de $Q(x)$ en $\mathbb{R}[x]$ es:

$$(x^2-x+1)(x-1)(x+1)(x+1-\sqrt{2})(x+1+\sqrt{2})$$

Finalmente, la factorización de $Q(x)$ en $\mathbb{C}[x]$ es:

$$\left(x-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)\right)\left(x+\left(\frac{1}{2}+\frac{\sqrt{3}}{2}\right)\right)(x-1)(x+1)(x+1-\sqrt{2})(x+1+\sqrt{2})$$

Esto concluye la solución del problema.

Quizá ya se han percatado que *todos los polinomios se descomponen en factores lineales en* $\mathbb{C}$. Esto solo es cierto para $\mathbb{C}$ (ya vimos, por ejemplo, que x^2+1 es irreducible en $\mathbb{R}$ y no es lineal).

¿Qué hicimos en el apartado 8.4?

- Definimos los polinomios irreducibles en $\mathbb{K}[x]$ como los polinomios que no se pueden escribir como producto de dos (o más) polinomios de grados mayores a 0.
- Estudiamos cómo hallar la descomposición en factores irreducibles en $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$ de polinomios en $\mathbb{K}[x]$.