Capítulo 4

Polinomios

4.1 Introducción

Polinomios con coeficientes en A

Sea A un anillo. Llamaremos **conjunto de polinomios con coeficientes en** A, y lo denotaremos por $A[x]$, al conjunto de las expresiones de la forma

$$a(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0,$$

con los $a_i \in A$ y $m \in \mathbb{N}$.

Grado

El **grado** de un polinomio no nulo $a(x)$, notado grado$(a(x))$, es el mayor entero n tal que $a_n \neq 0$. El polinomio cuyos coeficientes son todos nulos se llama **polinomio nulo** y se denota por 0. Por convención, su grado es grado$(0) = -\infty$.

Definiciones

Sea $a(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$ un polinomio no nulo con $a_n \neq 0$ (de grado n).
Llamaremos **término líder** de $a(x)$ al término $a_n x^n$, **coeficiente líder** a a_n y **término constante** a a_0.
Un polinomio es **mónico** si su coeficiente líder es 1. Los polinomios se dicen **constantes** cuando su grado es cero, así como el polinomio nulo.

Nota 4.1.1. Los polinomios se pueden sumar y multiplicar, extendiendo las operaciones de A:

Si $a(x) = \sum_{i=0}^{n} a_i x^i$, $b(x) = \sum_{i=0}^{m} b_i x^i$, suponiendo sin pérdida de generalidad que $m \geq n$, podemos definir la suma como

$$a(x) + b(x) = \sum_{i=0}^{n} (a_i + b_i)x^i + b_{n+1}x^{n+1} + \ldots + b_m x^m.$$

Cuando $m = n$, basta quedarnos con el primer sumando de la expresión anterior.

Tomando de nuevo $a(x)$ y $b(x)$, su producto está definido como:

$$d(x) = a(x)b(x) = \sum_{l=0}^{m+n} d_l x^l, \quad \text{donde} \quad d_l = \sum_{i+j=l} a_i b_j.$$

Estando así definidas las operaciones, es claro que extienden las de A; basta tomar $m = n = 0$. Por otro lado, también es evidente que tenemos[1]

- $\text{grado}(a(x)+b(x)) \leq \max\{\text{grado}(a(x)), \text{grado}(b(x))\}$, no dándose la igualdad solamente cuando $m = n$ y $a_m + b_n = 0$.
- $\text{grado}(a(x)b(x)) \leq \text{grado}(a(x)) + \text{grado}(b(x))$ (se da la igualdad cuando A es dominio de integridad).

Es fácil comprobar que la suma y el producto de polinomios verifican las propiedades asociativa y distributiva, además de poseer la suma elemento neutro, elemento opuesto y ser conmutativa. En otras palabras:

[1]Para ser estrictos, esto es cierto siempre y cuando asumamos que $-\infty < n$ y $-\infty + n = -\infty$ para cualquier $n \geq 0$.

El anillo $A[x]$

El conjunto $A[x]$ con la suma y producto definidos anteriormente es un anillo. Además:

- Si A es un anillo conmutativo, $A[x]$ es conmutativo.
- Si A es dominio de integridad, $A[x]$ es dominio de integridad.

Unidades de $A[x]$

Si A es un dominio de integridad, un polinomio de $A[x]$ es una **unidad** si y sólo si es una constante y es una unidad en A. Es decir, el grupo multiplicativo $A[x]^*$ de las unidades de $A[x]$ es el grupo A^* de las unidades de A.

4.2 El anillo $k[x]$. Divisibilidad

En adelante consideraremos principalmente el anillo de polinomios $k[x]$, donde k es un cuerpo (por ejemplo, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$). Este anillo de polinomios es un dominio de integridad, conmutativo y unitario. Sus unidades son las de k, es decir, $k^* = k \setminus \{0\}$. El grado de los polinomios puede ser usado como una medida que, a modo del valor absoluto en los enteros, nos permite realizar la división euclídea. Veremos que ésta no es la única similitud con $\mathbb{Z}$.

Teorema de división

Sean $f(x), g(x) \in k[x]$ dos polinomios, con $g(x) \neq 0$. Entonces, existen dos únicos polinomios $q(x), r(x) \in k[x]$ tales que

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

y grado$(r(x)) <$ grado$(g(x))$.

PRUEBA: La demostración es constructiva, indicando cómo se calculan cociente y resto de la división euclídea.

Si grado$(f(x)) <$ grado$(g(x))$ tomamos $q(x) = 0$, $r(x) = f(x)$, y ya hemos terminado nuestra construcción.

Supongamos ahora que grado$(f(x)) \geq$ grado$(g(x))$ y sean ax^m, bx^n los términos líder de $f(x), g(x)$ respectivamente. Escribamos

$$f_1(x) = f(x) - (a/b)x^{m-n}g(x);$$

así pues $f_1(x)$ es un polinomio de grado estrictamente inferior al de $f(x)$ y escogiendo $q_1(x) = (a/b)x^{m-n}$, tenemos que $f(x) = q_1(x)g(x) + f_1(x)$.

Aplicando el mismo razonamiento a $f_1(x)$ y así sucesivamente, logramos crear un conjunto finito de igualdades del tipo

$$\begin{array}{rcl} f(x) & = & q_1(x)g(x) + f_1(x) \\ f_1(x) & = & q_2(x)g(x) + f_2(x) \\ \vdots & & \vdots \\ f_{t-1}(x) & = & q_t(x)g(x) + f_t(x), \end{array}$$

donde

$$\text{grado}(f_1(x)) > \text{grado}(f_2(x)) > \ldots > \text{grado}(f_t(x))$$

y como vamos descendiendo al menos una unidad el grado en cada $f_i(x)$, o bien $f_t(x) = 0$ o bien es de grado inferior al de $g(x)$, y de ahí la finitud del proceso. Poniendo

$$q(x) = \sum_{i=1}^{t} q_i(x), \ r(x) = f_t(x)$$

se tiene $f(x) = q(x)g(x) + r(x)$.

Hemos probado la existencia. Probemos ahora la unicidad. Consideremos pues dos expresiones para $f(x)$ que verifiquen las propiedades que establece el teorema de división:

$$f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x);$$

entonces

$$r(x) - r'(x) = (q'(x) - q(x))g(x),$$

con lo que $r(x) - r'(x)$ debe ser nulo, ya que todo múltiplo no nulo de $g(x)$ tiene que ser de grado mayor o igual que él. □

Algoritmo de división

Para calcular el cociente y el resto de la división entre $f(x)$ y $g(x)$, de grados respectivos m y n.
Si $m \geq n$ tome

$$f_1(x) = f(x) - (a/b)x^{m-n}g(x)\,,\, q_1(x) = (a/b)x^{m-n}.$$

Repita con $f_1(x)$ y $g(x)$ hasta que grado$(f_t(x)) <$ grado$(g(x))$.
El cociente y el resto son

$$q(x) = q_1(x) + \ldots + q_{t-1}(x),\, r(x) = f_t(x).$$

Si $m < n$, el cociente es 0 y el resto el propio $f(x)$.

Ejemplo 4.2.1. Sean

$$f(x) = x^5 - \frac{1}{2}x^3 + 2x^2 - 3x + 3, \quad g(x) = 2x^3 - \frac{2}{3}x^2 + 3x - 1$$

dos polinomios de $\mathbb{Q}[x]$. Si queremos calcular el cociente y el resto de la división de $f(x)$ entre $g(x)$, tomamos en primer lugar

$$f_1(x) = f(x) - \frac{1}{2}x^2 g(x) = \frac{1}{3}x^4 - 2x^3 + \frac{5}{2}x^2 - 3x + 3.$$

Como grado$(f_1(x)) = 4$, seguimos. Sea ahora

$$f_2(x) = f_1(x) - \frac{1}{6}xg(x) = -\frac{17x^3}{9} + 2x^2 - \frac{17x}{6} + 3.$$

Tenemos que seguir, pues todavía no hemos bajado de grado 3, pero este será el último paso. Así,

$$f_3(x) = f_2(x) + \frac{17}{18}g(x) = \frac{37x^2}{27} + \frac{37}{18}.$$

Ahora ya hemos terminado. El cociente y el resto de la división son

$$q(x) = \frac{1}{2}x^2 + \frac{1}{6}x - \frac{17}{18}, \quad r(x) = \frac{37}{27}x^2 + \frac{37}{18}.$$

Corolario 4.2.2. *Sea $I \subset k[x]$ un ideal. Entonces I es un ideal principial. Eso es, existe $m(x) \in k[x]$ tal que*

$$I = (m(x)) = \{f(x)m(x) \mid f(x) \in k[x]\}.$$

PRUEBA: Queda como ejercicio, al ser similar a la equivalente para enteros. □

Algunos otros resultados, circunscritos en este caso al anillo $k[x]$ son los suiguientes.

Corolario 4.2.3. (Teorema del resto) *Sea un polinomio $f(x) \in k[x]$, y sea un elemento del cuerpo $a \in k$. Entonces $f(a)$ es el resto de dividir $f(x)$ por $x - a$.*

PRUEBA: Por el teorema de división,

$$f(x) = (x-a)q(x) + r(x), \text{ con grado}(r(x)) < \text{grado}(x-a) = 1.$$

Por tanto, $r(x)$ debe ser constante, digamos r, luego $f(a) = (a-a)q(a) + r = r$. □

Raíz de un polinomio

Sea $f(x) \in A[x]$ un polinomio, se dice que $a \in A$ es una **raíz de** $f(x)$ si $f(a) = 0$.

Corolario 4.2.4. (Teorema de la raíz) *Sea un polinomio $f(x) \in k[x]$ de grado positivo. Entonces $f(x)$ tiene una* **raíz** *$a \in k$ si y sólo si es divisible por $x - a$.*

PRUEBA: En efecto, podemos escribir $f(x) = q(x)(x-a) + r$ con $r \in k$. Así $f(a) = 0$ si y sólo si $r = 0$, lo que equivale a que $(x-a)|f(x)$. □

Multiplicidad de una raíz

Sean $f(x) \in A[x]$ un polinomio y $a \in A$ una raíz. Se llama multiplicidad de a al mayor entero positivo m tal que $(x-a)^m$ divide a $f(x)$.

Corolario 4.2.5. (D'Alembert) *Un polinomio no nulo $f(x) \in k[x]$ de grado n tiene a lo sumo n raíces distintas en k.*

PRUEBA: Lo probaremos por inducción en n, el grado de $f(x)$.

Si grado$(f(x)) = 0$, entonces $f(x)$ es un polinomio constante no nulo, luego no tiene raíces en k. Nuestra hipótesis de inducción es que si $h(x)$ es polinomio no nulo de grado $n-1$ con r raíces distintas, entonces $r \leq n-1$.

Supongamos ahora que $f(x)$ es un polinomio de grado $n > 0$ y que tiene r raíces distintas $a_1, \ldots, a_r$ en k. Veamos que $r \leq n$.

Tenemos que $f(a_r) = 0$, luego por el teorema de la raíz $f(x) = (x - a_r)g(x)$, con grado$(g(x)) = n - 1$. Para cada i con $1 \leq i \leq r-1$,

$$f(a_i) = 0 = (a_i - a_r)g(a_i).$$

Como $a_i \neq a_r$, por fuerza $g(a_i) = 0$. En consecuencia $a_1, \ldots, a_{r-1}$ son raíces de $g(x)$ y grado$(g(x)) = n - 1$. Por inducción, $r - 1 \leq n - 1$, así que $r \leq n$. □

4.3 Máximo común divisor

Máximo común divisor

Sean dos polinomios $f(x), g(x) \in k[x]$. Un polinomio $p(x) \in k[x]$ es un **máximo común divisor** de $f(x)$ y $g(x)$ si verifica:

1. $p(x)|f(x)$ y $p(x)|g(x)$
2. Si $q(x)$ es otro polinomio que divide a $f(x)$ y a $g(x)$ entonces $q(x)|p(x)$.

Nota 4.3.1. El máximo común divisor de dos polinomios no es único. Si $p(x) =$ mcd$(f(x), g(x))$, entonces, para cualquier $a \in k \setminus \{0\}$, $ap(x) =$ mcd$(f(x), g(x))$. Por eso cuando hablamos de un máximo común divisor, podremos acordar que estamos tomando un polinomio mónico y, en esas condiciones, sí que es único.

Como en los enteros, podemos calcular un máximo común divisor de dos polinomios usando el teorema de división. Consideremos dos polinomios $f(x), g(x) \in k[x]$; sabemos que existen $q(x), r(x) \in k[x]$ con grado$(r(x)) <$ grado$(g(x))$ tales que

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

Proposición 4.3.2. *Con las notaciones anteriores, se tiene que*

$$mcd(f(x), g(x)) = mcd(g(x), r(x))$$

PRUEBA: Supongamos que

$$a(x) = \text{mcd}(g(x), r(x)),\ b(x) = \text{mcd}(f(x), g(x)).$$

Como $f(x) = q(x)g(x) + r(x)$, $a(x)$ no puede sino dividir a $f(x)$ y así $a(x)$ es un divisor común de $f(x)$ y $g(x)$, luego por ser $b(x)$ el máximo entre ellos, $a(x)|b(x)$.

Análogamente, como

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

se tiene que $b(x)|r(x)$ y así $b(x)$ es un divisor común de $g(x)$ y $r(x)$, luego $b(x)|a(x)$. □

Algoritmo de Euclides

Sean $f(x), g(x) \in k[x]$ dos polinomios no nulos, con grado$(f(x)) \geq$ grado$(g(x))$. Entonces, si haciendo divisiones sucesivas obtenemos

$$\begin{array}{rcl} f(x) & = & q(x)g(x) + r(x) \\ g(x) & = & q_0(x)r(x) + r_1(x) \\ r(x) & = & q_1(x)r_1(x) + r_2(x) \\ & \vdots & \\ r_{n-2}(x) & = & q_{n-1}(x)r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) & = & q_n(x)r_n(x), \end{array}$$

este proceso es finito y, con las notaciones anteriores, $\text{mcd}(f(x), g(x)) = r_n(x)$.

PRUEBA: Consideremos la sucesión $\{\text{grado}(r_i(x))\}$, que es una sucesión estrictamente decreciente de enteros no negativos, pues el resto de la división polinómica es de menor grado que el divisor. Como el primer elemento es grado$(f(x))$, la sucesión puede tener a lo más grado$(f(x)) + 1$ elementos. Por tanto, existe un $n \geq 1$ tal que $r_{n+1}(x) = 0$. Esto prueba la finitud del proceso.

Ahora queda preguntarse si realmente obtenemos el máximo común divisor de $f(x)$ y $g(x)$. Para la respuesta basta con aplicar el resultado anterior para obtener que

$$\text{mcd}(f(x), g(x)) = \text{mcd}(g(x), r(x)) = \ldots = \text{mcd}(r_{n-1}(x), r_n(x)) = r_n(x).$$

□

Así pues, con este teorema se demuestra que el siguiente algoritmo es correcto:

Algoritmo de Euclides

Para hallar el máximo común divisor de dos polinomios no nulos $f(x), g(x) \in k[x]$.
Efectúe la división $f(x) = q(x)g(x)+r(x)$ y tome $f_0(x) = f(x)$, $g_0(x) = g(x)$ y $r_0(x) = r(x)$. Mientras $r_i(x) \neq 0$, repita con $f_{i+1}(x) = g_i(x)$ y $g_{i+1}(x) = r_i(x)$.
Si $r_{n+1}(x) = 0$, $\text{mcd}(f(x), g(x)) = r_n(x)$, notando $r_{-1}(x) = g(x)$.

Ejemplo 4.3.3. Queremos hallar el máximo común divisor de $f(x) = x^5 - \frac{1}{2}x^3 + 2x^2 - 3x + 3$ y $g(x) = 2x^3 - \frac{2}{3}x^2 + 3x - 1$ en $\mathbb{Q}[x]$. Siguiendo el algoritmo, dividimos el primero entre el segundo, y tomamos

$$f_0(x) = f(x)\ ,\ g_0(x) = g(x)\ ,\ r_0(x) = \frac{37x^2}{27} + \frac{37}{18}.$$

Como $r_0(x) \neq 0$, dividimos $g(x)$ entre $r_0(x)$, tomando

$$f_1(x) = g(x)\ ,\ g_1(x) = r_0(x)\ ,\ r_1(x) = 0.$$

La división anterior era exacta de cociente $\frac{18}{37}(3x-1)$, con lo que $\text{mcd}(f(x), g(x)) = r_0(x)$, o tomando el polinomio mónico asociado,

$$\text{mcd}(f(x), g(x)) = x^2 + \frac{3}{2}.$$

Identidad de Bézout

Sean $f(x), g(x) \in k[x]$ dos polinomios no nulos. Si denotamos $\text{mcd}(f(x), g(x)) = d(x)$ entonces existen elementos $a(x), b(x) \in k[x]$ tales que

$$d(x) = a(x)f(x) + b(x)g(x).$$

PRUEBA: La demostración es consecuencia de aplicar el algoritmo de Euclides al revés.
En efecto, si con la notación del teorema, llamamos $r_n(x) = d(x)$, tendremos que

$$\begin{aligned} r_n(x) = & \ r_{n-2}(x) - q_{n-1}(x)r_{n-1} = \\ = & \ r_{n-2}(x) - q_{n-1}(x)(r_{n-3}(x) - q_{n-2}(x)r_{n-2}(x)) = \\ & \ \vdots \\ = & \ \tilde{a}(x)r(x) + \tilde{b}(x)g(x) = \\ = & \ \tilde{a}(x)f(x) + (\tilde{b}(x) - \tilde{a}(x)q(x))g(x). \end{aligned}$$

Tomando $a(x) = \tilde{a}(x)$ y $b(x) = (\tilde{b}(x) - \tilde{a}(x)q(x))$, tenemos lo que queríamos.

Es posible dar una prueba distinta (no efectiva), siguiendo la expuesta en el tema anterior para los enteros, ya que solo se usa que todos los ideales del anillo son principales, y este es un hecho que también se verifica en $k[x]$. □

Ejemplo 4.3.4. Sabemos que el máximo común divisor de nuestros polinomios predilectos, $f(x) = x^5 - \frac{1}{2}x^3 + 2x^2 - 3x + 3$ y $g(x) = 2x^3 - \frac{2}{3}x^2 + 3x - 1$ en $\mathbb{Q}[x]$ es $d(x) = x^2 + \frac{3}{2}$. ¿Cuáles son los polinomios $a(x)$ y $b(x)$ de la identidad de Bézout para ellos? Siguiendo el algoritmo de Euclides realizado anteriormente para ellos,

$$d(x) = \frac{27}{37}f(x) - \frac{27}{37}\left(\frac{1}{2}x^2 + \frac{1}{6}x - \frac{17}{18}\right)g(x),$$

luego $a(x) = \frac{27}{37}$ y $b(x) = -\frac{27}{37}q(x)$.

4.4 Factorización. Factores múltiples

Polinomio irreducible

Un polinomio $p(x) \in k[x]$ es **irreducible** si no es una constante, y si el que podamos escribir $p(x) = f(x)g(x)$ implica que uno de los dos factores sea una unidad (una constante).

Proposición 4.4.1. *Sea $p(x) \in k[x]$ un polinomio irreducible. Si $f(x)$ es un polinomio que no es divisible por $p(x)$, entonces mcd$(f(x), p(x)) = 1$.*

PRUEBA: Sea $d(x) = \text{mcd}(p(x), f(x))$. Como $d(x)|p(x)$, existirá cierto polinomio $p_0(x)$ de modo que podamos escribir $p(x) = d(x)p_0(x)$. Ahora bien, por la definición de irreducibilidad, o bien $d(x)$ o bien $p_0(x)$ es constante. Si el

polinomio constante es $d(x)$, tendríamos el resultado.
Veamos pues qué pasa cuando el que fuera constante fuera $p_0(x)$. En ese caso $p(x)|d(x)$, por lo que $p(x)$ dividiría a $f(x)$, que no es posible. Por consiguiente $d(x)$ no puede ser nada más que una constante. □

Veremos a continuación algunos resultados que dejaremos sin demostrar, pues sus pruebas se pueden escribir de una manera completamente análoga a las de sus semejantes del ámbito de los enteros.

Proposición 4.4.2. (Teorema de Euclides) *Sea $p(x) \in k[x]$ un polinomio irreducible. Dados dos polinomios $f(x), g(x) \in k[x]$, si $p(x)|f(x)g(x)$, entonces $p(x)$ divide a alguno de los dos.*

Descomposición en factores irreducibles

Cualquier polinomio no constante de $k[x]$ es irreducible o factoriza en producto de polinomios irreducibles. Este producto es único en tanto que si tenemos dos factorizaciones de $f(x)$ en producto de polinomios irreducibles en $k[x]$ de la forma

$$f(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x)$$

necesariamente $s = t$ y existe una correspondencia uno a uno entre los factores $p_1(x), \ldots, p_s(x)$ y $q_1(x), \ldots, q_t(x)$ donde si $p_i(x)$ se corresponde con $q_j(x)$, existe un $\alpha \in k \setminus \{0\}$ tal que $p_i(x) = \alpha q_j(x)$.

Proposición 4.4.3. *Sea $I = (f(x)) \subset k[x]$ un ideal. Entonces son equivalentes las siguientes condiciones:*

1. *I es maximal.*
2. *I es primo.*
3. *$f(x)$ es irreducible.*

Vamos a presentar una herramienta específica y útil de los polinomios, que no tiene paralelismo en los enteros: la derivada (formal), que coincide con el concepto usual de análisis.

Usaremos la notación habitual:

- $f'(x)$ es el polinomio que se obtiene al derivar $f(x)$;

- $D : k[x] \to k[x]$ es la función que a cada polinomio le asocia su derivada. Esto es, $D(f(x)) = f'(x)$.

Derivada de un polinomio

La **derivada** de un polinomio $f(x)$ viene definida por las siguientes reglas:

1. Si $f(x) = ax^n$ con $a \in k$, entonces $D(ax^n) = nax^{n-1}$. (Si $n = 0$, $D(a) = 0$.)

2. Si $f(x) = g(x) + h(x)$, entonces $D(f(x)) = D(g(x)) + D(h(x))$. Esto es, la derivada es un homomorfismo de grupos aditivos.

Proposición 4.4.4. *Para cualesquiera polinomios $f(x), g(x) \in k[x]$ y para todo natural $s > 1$ se verifica que:*

1. $D(f(x)g(x)) = f(x)D(g(x)) + g(x)D(f(x))$.
2. $D(f(x)^s) = sf(x)^{s-1}D(f(x))$.

PRUEBA: La prueba es puramente efectiva. □

Factores múltiples de un polinomio

Sea $f(x) \in k[x]$ un polinomio, donde $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Entonces $f(x)$ tiene factores múltiples si y sólo si $f(x)$ y $f'(x)$ no son primos entre sí.

PRUEBA: Supongamos en primer lugar que $f(x)$ tiene algún factor múltiple, y sea por tanto $f(x) = p(x)^s q(x)$, con $s > 1$. Entonces

$$f'(x) = p(x)^{s-1}[sp'(x)q(x) + p(x)q'(x)],$$

luego $p(x)$ es un factor común de $f(x)$ y $f'(x)$.

Supongamos ahora que $d(x) = \text{mcd}(f(x), f'(x))$ es de grado mayor que cero, y sea $p(x)$ un factor irreducible de $d(x)$. Veamos que $p(x)$ es un factor múltiple de $f(x)$. Notemos que $p'(x) \neq 0$, al ser $p(x)$ irreducible.
En efecto, como $p(x)|f(x)$, tenemos $f(x) = p(x)g(x)$. Derivando esa expresión,

$$f'(x) = p'(x)g(x) + p(x)g'(x).$$

Como $p(x)|f'(x)$, $p(x)$ también divide al producto $p'(x)g(x)$, y, por ser $p(x)$ irreducible, divide a uno de los factores. Ahora bien, $p(x)$ no puede dividir a $p'(x)$ pues tiene grado estrictamente mayor y ambos son no nulos, luego $p(x)|g(x)$, y $g(x) = p(x)h(x)$, así que sustituímos y conseguimos la expresión $f(x) = p(x)^2h(x)$. □

Nota 4.4.5. La especificación de que el cuerpo de coeficientes es $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ no es irrelevante. En efecto, en la demostración se usa que un polinomio de grado mayor que 1 no puede dividir a su derivada. Esto en cuerpos como $\mathbb{F}_p$ no es cierto ya que, por ejemplo, $f(x) = x^3 + 1$ es un polinomio irreducible de $\mathbb{F}_3[x]$ que verifica que $f'(x) = 0$ y, por tanto $f(x)|f'(x)$.

4.5 Factorización en $\mathbb{C}[x]$ y en $\mathbb{R}[x]$

A continuación enunciaremos un resultado del que hablaremos con más detalle en la última sección. Para lo que estamos tratando aquí, su importancia es que nos dice cómo son los polinomios irreducibles sobre $\mathbb{C}$. Ahora bien, su relevancia es mucho mayor, pero no adelantemos acontecimientos y centrémonos de momento en la factorización de polinomios.

Teorema fundamental del álgebra

Todo polinomio $f(x) \in \mathbb{C}[x]$ de grado positivo tiene una raíz compleja.

Corolario 4.5.1. *Todo polinomio $f(x) \in \mathbb{C}[x]$ de grado positivo, digamos n, tiene n raíces en $\mathbb{C}$, esto es, se puede escribir como*

$$f(x) = \alpha \prod_{i=1}^{n} (x - \alpha_i),$$

donde $\alpha, \alpha_i \in \mathbb{C}$.

En virtud del corolario, el problema de dilucidar si un polinomio de $\mathbb{C}[x]$ es irreducible o no es tremendamente sencillo; tanto como mirar su grado, pues los únicos polinomios irreducibles en $\mathbb{C}[x]$ son los de grado 1. En $\mathbb{R}[x]$ no ocurre así, ya que, por ejemplo, los polinomios x^2+1 o $x^3-15x-4$ no se pueden factorizar en producto de polinomios de primer grado, aunque tampoco es que la cuestión de la factorización devenga complicada. Veamos cómo son los irreducibles en este otro anillo.

Proposición 4.5.2. *Todo polinomio de $\mathbb{R}[x]$ de grado impar tiene una raíz en $\mathbb{R}$. Todo polinomio se descompone en producto de polinomios de grados 1 o 2 (los cuales son irreducibles si y sólo si sus raíces son complejas no reales).*

PRUEBA: Sea $f(x) \in \mathbb{R}[x]$ un polinomio de grado positivo, digamos n. A $f(x)$ lo podemos mirar con otros ojos, como elemento de $\mathbb{C}[x]$, así que aplicamos el teorema fundamental del álgebra para saber que $f(x)$ tiene n raíces en $\mathbb{C}$. Sea

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbb{R}, i = 0, 1, \ldots, n,$$

y sea $\alpha = a + bi$ una raíz de $f(x)$. De

$$0 = f(\alpha) = a_n(a+bi)^n + a_{n-1}(a+bi)^{n-1} + \ldots + a_1(a+bi) + a_0$$

se deduce, tomando conjugados, que

$$0 = \overline{f(\alpha)} = f(\overline{\alpha}) = a_n(a-bi)^n + a_{n-1}(a-bi)^{n-1} + \ldots + a_1(a-bi) + a_0.$$

En consecuencia, si α es una raíz de $f(x)$, también debe serlo $\overline{\alpha}$, luego las raíces no reales de $f(x)$ aparecen por pares de conjugadas. Si n es impar, tiene que haber una raíz que coincida con su conjugada, es decir, que sea real. Con esto probamos el primer aserto.

En cuanto a la segunda afirmación, obramos como sigue. Si $\alpha = a + bi$ es una raíz compleja no real de $f(x)$, el polinomio

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2ax + (a^2+b^2)$$

divide a $f(x)$ y tiene coeficientes reales, con lo que podemos descomponer a $f(x)$ en producto de factores de grado 2 a lo sumo. La cuestión de si éstos se pueden descomponer a su vez en otros de grado 1 o son irreducibles es tan simple como el hecho de que sus raíces sean reales o no. □

4.6 Factorización en $\mathbb{Q}[x]$

Sea $f(x) \in k[x]$ un polinomio de grado 2 o 3. En ese caso, $f(x)$ es reducible si y sólo si tiene una raíz en k. En efecto, el hecho de que $f(x)$ sea reducible es equivalente a decir que tiene un divisor que es de grado 1. Si éste es $ax - b$, entonces b/a es una raíz de $f(x)$.

Naturalmente, lo anterior no funciona para grados mayores. Un polinomio de grado 4 se puede descomponer, por ejemplo, en dos factores irreducibles de grado 2, como $x^4 + 3x^2 + 2$ en $\mathbb{Q}$, luego no tiene por qué tener raíces en k. Con mayor razón ocurrirá esto en grados más altos. No obstante es bueno ver si un polinomio dado tiene o no raíces en k. Si las tiene, y es de grado mayor que 1, es automáticamente reducible.

El problema de saber cuándo un polinomio de $\mathbb{Q}[x]$ es irreducible es algo intrincado si se pretende resolver de manera realmente efectiva. Sin embargo, el problema de la localización de raíces (que, como hemos notado en el párrafo anterior, es más simple), sí se puede atacar fácilmente, y es lo primero que haremos en esta sección.

Para empezar, notemos que si $f(x) \in \mathbb{Q}[x]$, es igual buscar sus raíces que las de $af(x)$, donde $a \in \mathbb{Z}$. En particular, podemos suponer que $f(x)$ está en realidad en $\mathbb{Z}[x]$ (esto es, todos sus coeficientes son enteros). En estas condiciones tenemos el siguiente resultado, también conocido como **Regla de Ruffini**:

Proposición 4.6.1 (Regla de Ruffini)**.** *Sea el polinomio*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbb{Z}, i = 0, 1, \ldots, n,$$

de grado $n > 0$. Supongamos que $f(x)$ tiene una raíz racional $\alpha = a/b$ con a y b primos entre sí. Entonces $a|a_0$ y $b|a_n$.

PRUEBA: En efecto, como a/b es raíz de $f(x)$,

$$0 = f(a/b) = a_n(a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_1(a/b) + a_0,$$

luego, previa multiplicación por b^n, tenemos que

$$0 = a_n a^n + a_{n-1}a^{n-1}b + \ldots + a_1 ab^{n-1} + a_0 b^n.$$

Como a divide a todos los términos salvo al último y es primo con b, debe dividir a a_0. E igualmente, como b divide a todos los términos salvo al primero y es primo con a, debe dividir a a_0. □

Hemos visto que intentar localizar las raíces de los polinomios en $\mathbb{Z}[x]$ tiene algo más de futuro, o por lo menos es más abarcable, que en $\mathbb{Q}[x]$, así que seguiremos reduciéndonos al caso de los polinomios con coeficientes enteros, donde la factorización única de los coeficientes nos puede ser de ayuda.

Contenido de un polinomio

Dado un polinomio $f(x) \in \mathbb{Z}[x]$ no nulo, se llama **contenido de** $f(x)$ al máximo común divisor de sus coeficientes. Se denota por $c(f)$. Se dirá que $f(x)$ es **primitivo** si su contenido es 1.

El siguiente resultado es conocido como lema de Gauss, como también se denomina del mismo modo a otros resultados en otros campos matemáticos. Al fin y al cabo, Gauss fue un matemático muy prolijo y no es de extrañar que varios lemas suyos hayan pasado a la historia con el mismo nombre. De hecho, se confunde incluso con un corolario suyo, pero el que presentamos es, en este contexto, el verdadero históricamente hablando, y aparece, con otras palabras, en el Artículo 42 de su gran obra *Disquisitiones Arithmeticae*.

Lema de Gauss

El producto de dos polinomios primitivos es primitivo.

PRUEBA: Sean

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0,\ a_i \in \mathbb{Z}, i = 0, 1, \ldots, m,$$

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0,\ b_j \in \mathbb{Z}, j = 0, 1, \ldots, n$$

dos polinomios primitivos. Para probar que $f(x)g(x)$ es primitivo basta ver que, fijado $p \in \mathbb{Z}$ irreducible, existe un coeficiente de $f(x)g(x)$ que no es divisible por él.

Fijemos pues p irreducible. Sea s (resp t) el entero $0 \leq s \leq m$ (resp. $0 \leq t \leq n$) tal que $p|a_i$ para todo $i > s$ (resp. $p|b_j$ para todo $j > t$), si se da el caso, y p no divide a a_s (resp. a b_t). El coeficiente de x^{s+t} en $f(x)g(x)$ es

$$a_0 b_{s+t} + \ldots + a_{s-1}b_{t+1} + a_s b_t + a_{s+1}b_{t-1} + \ldots + a_{s+t}b_0,$$

en el que se ve que p divide a todos los sumandos salvo a $a_s b_t$. Así, p no divide a la suma, lo que prueba el resultado. □

Corolario 4.6.2. *Si $f(x), g(x) \in \mathbb{Z}[x]$ son polinomios no nulos, entonces*

$$c(fg) = c(f)c(g).$$

PRUEBA: Podemos escribir

$$f(x) = c(f)f_0(x), \quad g(x) = c(g)g_0(x)$$

donde $f_0(x)$ y $g_0(x)$ son primitivos. Así

$$f(x)g(x) = c(f)c(g)f_0(x)g_0(x)$$

y, como $f_0(x)g_0(x)$ es primitivo por el lema de Gauss, debe ocurrir que $c(f)c(g) = c(fg)$. □

El siguiente resultado es engañosamente sencillo, pero de una importancia extrema cuando se trata de factorizar polinomios, como comprobaremos más adelante.

Corolario 4.6.3. *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado positivo, digamos n, que se descompone en $\mathbb{Q}[x]$ en producto de dos polinomios de grados estrictamente menores que n. Entonces, se descompone en $\mathbb{Z}[x]$ en producto de dos polinomios de esos mismos grados.*

PRUEBA: Sea $f(x) = f_1(x)g_1(x)$, donde $f_1(x), g_1(x) \in \mathbb{Q}[x]$ con

$$\text{grado}(f_1(x)) < n, \quad \text{grado}(g_1(x)) < n.$$

Multiplicando la anterior igualdad por un cierto elemento $a \in \mathbb{Z}$ para quitarnos los denominadores de en medio del producto, se tendrá que

$$af(x) = g(x)h(x)\ ,\ g(x), h(x) \in \mathbb{Z}[x].$$

De ahí se deduce que $ac(f) = c(gh) = c(g)c(h)$, luego $a|c(g)c(h)$. Por tanto, si tomamos $g(x) = c(g)g'(x)$, $h(x) = c(h)h'(x)$, entonces

$$f(x) = \frac{c(g)c(h)}{a} g'(x)h'(x),$$

y ésa es la descomposición buscada. □

Corolario 4.6.4. *Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado positivo, digamos n, y primitivo. Entonces $f(x)$ es reducible en $\mathbb{Z}[x]$ si y sólo si lo es en $\mathbb{Q}[x]$.*

PRUEBA: Muy simple; basta con releer el enunciado del corolario anterior. □

Incluimos también un criterio muy general y útil de irreducibilidad de polinomios, aunque no concluyente al no poderse aplicar a todos los casos.

Proposición 4.6.5 (Criterio de Eisenstein-Schönemann)**.** *Sea un polinomio de grado* $n > 0$

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbb{Z}, i = 0, 1, \ldots, n.$$

Supongamos que existe un elemento irreducible $p \in \mathbb{Z}$ *que divide a todos los coeficientes, salvo a* a_n*, y cuyo cuadrado* p^2 *no divide a* a_0*. Entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$*.*

PRUEBA: Se hará por reducción al absurdo. Supongamos que $f(x)$ fuese reducible en $\mathbb{Q}[x]$. En consecuencia se descompondría en $\mathbb{Q}[x]$ en producto de dos polinomios de grado estrictamente inferior. Por el corolario anterior se puede escribir

$$f(x) = (b_s x^s + b_{s-1}x^{s-1} + \ldots + b_1 x + b_0)(c_t x^t + c_{t-1}x^{t-1} + \ldots + c_1 x + c_0),$$

donde $b_i, c_j \in \mathbb{Z}$ para cualesquiera i, j y $s, t < n$.

Por la segunda hipótesis, p debe dividir a uno de entre b_0 y c_0, pero no a ambos. Supongamos pues sin pérdida de generalidad que $p|b_0$ y no divide a c_0. Como p no divide a a_n, no puede dividir a todos los b_i. Sea m el mínimo índice tal que p no divide a b_m, que sabemos que es menor que n. El coeficiente del término en x^m es

$$b_m c_0 + b_{m-1}c_1 + \ldots + b_0 c_m = a_m,$$

que no es divisible por p pues todos los sumandos lo son salvo el primero. Ahora bien, que a_m con $m < n$ no sea divisible por p es una contradicción, luego hemos terminado con la prueba. □

Nota 4.6.6.

- Todo polinomio $f(x) \in \mathbb{Q}[x]$ se puede escribir como $df(x) = h(x)$, con $d \in \mathbb{Z}, h(x) \in \mathbb{Z}[x]$. Por tanto, para obtener la descomposición en $\mathbb{Q}$ de $f(x)$ puedo calcular la de $h(x)$. Es decir, podemos considerar sólo polinomios con coeficientes enteros.

- Sea $f(x) \in \mathbb{Z}[x]$. Sabemos que $f(x) = c(f)h(x)$, donde $h(x) \in \mathbb{Z}[x]$ y es primitivo. Para obtener la descomposición en $\mathbb{Q}$ de $f(x)$ puedo calcular la de $h(x)$. Es decir, podemos considerar sólo polinomios con coeficientes enteros y primitivos.

Ejemplo 4.6.7. Consideremos el polinomio $f(x) = x^5 + x^3 - 2x^2 - 2 \in \mathbb{Z}[x]$, primitivo. Si $f(x)$ es reducible se podrá poner como producto de dos polinomios no constantes $f(x) = g(x)h(x)$, con $g(x), h(x) \in \mathbb{Z}[x]$. Como el polinomio de partida es de grado 5, las posibilidades son:

1. grado$(g(x)) = 1$ y grado$(h(x)) = 4$

2. grado$(g(x)) = 2$ y grado$(h(x)) = 3$

Ahora se trata de probar "manualmente" si es posible alguna de las posibilidades. Una respuesta negativa indicaría que el polinomio de partida es irreducible.

El primer caso es el teorema de Ruffini. Si $g(x) = ax + b$ es de grado 1, entonces $-b/a$ es una raíz de $f(x)$. Por tanto, se dará la posibilidad (1) si y sólo si $f(x)$ tiene raíces racionales (notemos que este argumento es válido independiente del grado del polinomio de partida).

En nuestro ejemplo sabemos por Ruffini que las posibles raíces de $f(x)$ son $\pm 1, \pm 2$. Sustituyendo en $f(x)$ comprobamos que ninguna es raíz, luego la posibilidad 1 no se da.

Veamos pues si es posible la segunda. Si lo fuera, existirían enteros a, b, c, d, e, f y r tales que:

$$x^5 + x^3 - 2x^2 - 2 = (ax^2 + bx + c)(dx^3 + ex^2 + fx + r) =$$

$$= adx^5 + (ae + bd)x^4 + (af + be + cd)x^3 + (ar + bf + ce)x^2 + (br + cf)x + cr.$$

Este polinomio será igual a $f(x)$ si tienen los mismos coeficientes. Por tanto, la segunda posibilidad se da si y sólo si existen unos enteros a, b, c, d, e, f y r verificando que

$$S : \begin{cases} 1 &= ad \\ 0 &= ae + bd \\ 1 &= af + be + cd \\ -2 &= ar + bf + ce \\ 0 &= br + cf \\ -2 &= cr \end{cases}$$

Es decir, tenemos que tratar de resolver en $\mathbb{Z}$ el sistema de ecuaciones (no lineales) S. La mejor forma es estudiar casos. La primera ecuación nos dice que $a = d = 1$ o $a = d = -1$. Supongamos que $a = d = 1$. Si con esta elección encontramos una solución, ya tendríamos los polinomios $g(x)$ y $h(x)$ y no habría necesidad de seguir buscando. En caso contrario tendríamos que resolver el sistema con $a = d = -1$.

Si $a = d = 1$, el sistema anterior es:

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be + c \\ -2 &= r + bf + ce \\ 0 &= br + cf \\ -2 &= cr \end{cases}$$

De la última ecuación nos surgen los siguientes casos: (1) $c = -1, r = 2$, (2) $c = 1, r = -2$, (3) $c = -2, r = 1$ y (4) $c = 2, r = -1$.
Caso (1). El sistema a resolver es

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be - 1 \\ -2 &= 2 + bf - e \\ 0 &= 2b - f \end{cases}$$

Sustituyendo $e = -b, f = 2b$ en la segunda ecuación se obtiene $b^2 - 2b + 2 = 0$ que no tiene solución entera. Por tanto este caso es imposible.
Caso (2). El sistema a resolver es

$$S : \begin{cases} 0 &= e + b \\ 1 &= f + be + 1 \\ -2 &= -2 + bf + e \\ 0 &= -2b + f \end{cases},$$

que tiene como solución $b = e = f = 0$.

Concluyendo, llegamos a que $f(x)$ es reducible y su descomposición es factores irreducibles es $f(x) = (x^2 + 1)(x^3 - 2)$. Los polinomios $x^2 + 1$ y $x^3 - 2$ son irreducibles pues no tienen raíces racionales.

Como el lector atento habrá podido observar al final no ha sido necesario lidiar con el caso en que $a = d = -1$. Esto es porque si el polinomio de partida es mónico, podemos suponer que los factores en que se descompone son también mónicos. De haber supuesto esto, habríamos obtenido los polinomios $-x^2 - 1$ y $-x^3 + 2$.

4.7 Factorización en $\mathbb{F}_p[x]$

El mismo procedimiento "artesanal" que hemos usado en la sección anterior para factorizar en $\mathbb{Q}[x]$ se puede usar para obtener la descomposición en factores irreducibles de polinomios con coeficientes en $\mathbb{F}_p$, con p primo.

Ejemplo 4.7.1. Consideremos el polinomio $f(x) = x^4 + x^3 + x + 2 \in \mathbb{F}_3[x]$. Si $f(x)$ es reducible se puede expresar como producto de dos polinomios no constantes $f(x) = g(x)h(x)$, con $g(x), h(x) \in \mathbb{F}_3[x]$. Como el polinomio de partida es de grado 4, las posibilidades son:

1. grado$(g(x)) = 1$ y grado$(h(x)) = 3$
2. grado$(g(x)) = 2$ y grado$(h(x)) = 2$

El primer caso se resuelve, como en $\mathbb{Q}$, comprobando si $f(x)$ posee alguna raíz en $\mathbb{F}_3$. Como $\mathbb{F}_3 = \{0, 1, 2\}$ es finito, basta comprobar si algún elemento es raíz. En nuestro caso $f(0) = 2$, $f(1) = 2$ y $f(2) = 1$, luego la primera posibilidad no se da.

Para estudiar el segundo supuesto escribamos

$$f(x) = (x^2 + ax + b)(x^2 + cx + d)$$

(nótese que ya estamos asumiendo que los factores serán mónicos como $f(x)$). Operando e igualando coeficientes obtenemos el sistema

$$S : \begin{cases} 1 &= a + c \\ 0 &= b + ac + d \\ 1 &= ad + bc \\ 2 &= bd \end{cases}$$

De la cuarta ecuación, teniendo en cuenta los elementos de $\mathbb{F}_3$, obtenemos que o bien $b = 1$ y $d = 2$, o bien $b = 2$ y $d = 1$. Ahora bien, dado que ambos polinomios son de grado 2, podríamos reordenarlos si se diera lo segundo para suponer sin pérdida de generalidad que $b = 1$ y $d = 2$. El sistema se queda del siguiente modo:

$$S : \begin{cases} 1 &= a + c \\ 0 &= ac \\ 1 &= 2a + c \end{cases}$$

Su única solución es $a = 0, c = 1$. Por consiguiente, $f(x) = (x^2+1)(x^2+x+2)$ es la descomposición en factores irreducibles buscada. (Los polinomios $x^2 + 1$ y $x^2 + x + 2$ son irreducibles al no tener raíces en $\mathbb{F}_3$.)

Para ilustrar la importancia del problema de factorizar sobre $\mathbb{F}_p[x]$ de la que hablábamos antes veamos cómo podemos relacionar la irreducibilidad en $\mathbb{Q}$ y en $\mathbb{F}_p$, con p primo. Sea

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

primitivo, sea p un primo que no divida a a_n, y llamemos $\overline{f}(x)$ al polinomio

$$\overline{f}(x) = \overline{a}_n x^n + \ldots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{F}_p[x],$$

siendo $\overline{a}_i = a_i + \mathbb{Z}p$, $0 \leq i \leq n$.

Proposición 4.7.2. *Si $\overline{f}(x)$ es irreducible en $\mathbb{F}_p[x]$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.*

PRUEBA: Solo hay que tener en cuenta que para cualesquiera polinomios $f(x), g(x)$, $\overline{f(x)g(x)} = \overline{f}(x)\overline{g}(x)$ y escribir el contrarrecíproco del enunciado. □

Veamos, con un ejemplo, cómo podemos usar el resultado anterior.

Ejemplo 4.7.3. Sea $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Z}[x]$. Tomemos $p = 2$. Entonces $\overline{f}(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2$. Ya que $\overline{f}(0) = 1$ y $\overline{f}(1) = 1$, $\overline{f}(x)$ no tiene raíces en $\mathbb{F}_2$.

Como en caso de ser reducible, ningún factor de la descomposición de $\overline{f}(x)$ sería de grado 1, pongamos por caso que

$$\overline{f}(x) = (x^2 + ax + b)(x^2 + cx + d).$$

Como otras veces, operando e igualando coeficientes obtenemos el sistema

$$S : \begin{cases} 1 &= a + c \\ 1 &= b + ac + d \\ 1 &= ad + bc \\ 1 &= bd \end{cases}$$

La última ecuación nos dice que $b = d = 1$, y sustituyendo en el resto nos quedamos con

$$S : \begin{cases} 1 &= a + c \\ 1 &= ac \end{cases},$$

que no tiene solución. Por tanto, $\overline{f}(x)$ es irreducible en $\mathbb{F}_2$ y así, por la proposición, $f(x)$ es irreducible sobre $\mathbb{Q}$.

Nota 4.7.4. Si bien en apariencia este procedimiento simplifica los cálculos a la hora de estudiar si un polinomio es o no irreducible sobre $\mathbb{Q}$, tiene un grave inconveniente. El recíproco de la proposición anterior es falso. Por ejemplo, el polinomio $x^2 + 2$ es irreducible sobre $\mathbb{Q}$, pero $\overline{f}(x) = x^2 \in \mathbb{F}_2[x]$ es reducible, o el polinomio $x^2 - x + 1$, irreducible en $\mathbb{Q}$ y con $\overline{f}(x)$ reducible en $\mathbb{F}_3$.

4.8 El teorema fundamental del álgebra*

El contenido de esta sección está tomado del artículo *The Fundamental Theorem of Algebra and Linear Algebra*, de Harm Derksen, publicado en el American Mathematical Monthly **110** (2003), número 7, páginas 620-623. El objetivo que perseguimos es dar una prueba del teorema fundamental del álgebra con argumentos puramente algebraicos y a la vez asequible al lector que no tenga un conocimiento profundo de esta materia, pues solamente usa algunas nociones de álgebra lineal.

Teorema fundamental del álgebra

Todo polinomio no constante de $\mathbb{C}[x]$ tiene una raíz en $\mathbb{C}$.

Si de algo no se puede quejar alguien que se acerque por primera vez al teorema que nos ocupa, es por falta de demostraciones. Existe una cantidad considerable de pruebas distintas, y usando técnicas variopintas. Desde la primera, elaborada por Gauss en su tesis doctoral de 1799 (aunque con algún fallo en el rigor matemático), hasta esta que aquí expondremos, existen pruebas topológicas, usando propiedades de la curva compleja que describe un polinomio, pruebas analíticas, que utilizan el teorema de Liouville de que toda función entera es acotada, pruebas algebraicas, basándose en la teoría de Galois entre otras herramientas, o incluso mixturas de los tres tipos anteriores.

Vayamos, sin más dilación, al desarrollo de la prueba. Para ello, definamos la propiedad $\mathscr{P}_{k,r}(d)$, donde k es un cuerpo, $\mathbb{R}$ o $\mathbb{C}$, y $r = 1, 2$. Su enunciado es el siguiente:

$\mathscr{P}_{k,r}(d)$: *Dados r endomorfismos A_i que conmuten entre todos de un k-espacio vectorial V de dimensión n, no divisible por d, existe un autovector no nulo que es común a todos ellos.*

Para probar el teorema, bastaría con demostrar que se cumple la propiedad $\mathscr{P}_{\mathbb{C},1}(2^r)$ para todo $r \in \mathbb{N}$. Así, para cualquier polinomio (que podemos suponer mónico sin problema) no constante $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{C}[x]$, se tiene que

$$f(x) = \det(xI_n - A), \text{ con } A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Como A representa a un endomorfismo de $\mathbb{C}$ y existe algún r tal que 2^r no divide a n, A tendría un autovector no nulo. Su autovalor asociado sería raíz de $f(x)$, y habríamos acabado. □

Así pues, para probar $\mathscr{P}_{\mathbb{C},1}(2^r)$ seguiremos el camino marcado a través de diversos lemas, cada uno apoyándose en los anteriores. Como en la demostración de arriba, denotaremos por A_i tanto a un endomorfismo como a su matriz asociada.

Lema 4.8.1. *Si se tiene $\mathscr{P}_{k,1}(d)$, también se cumple $\mathscr{P}_{k,2}(d)$.*

PRUEBA: Sean A_1 y A_2 dos endomorfismos que conmutan de un k-espacio vectorial V de dimensión n no divisible por d. Vamos a probar por inducción en n que tienen un autovector en común. Si $n = 1$, cada A_i no es más que la multiplicación por una constante, y todos los vectores de V son propios, siendo trivial el aserto. Supongamos pues que también es cierto si $\dim V < n$, y veámoslo para $\dim V = n$.

Como $\mathscr{P}_{k,1}(d)$ se cumple, A_1 tiene un autovalor $\lambda \in k$. Sean W y Z, respectivamente, el núcleo y la imagen del endomorfismo $A_2 - \lambda I$. Como A_1 y A_2 conmutan, W y Z permanecen fijos por A_1.
Supongamos que $W \neq V$. Entonces, como $\dim W + \dim Z = \dim V$, d no dividirá a al menos alguna de las dos dimensiones, y además ambas son menores que n. Por tanto, por la hipótesis de inducción, A_1 y A_2 compartirán un autovector no nulo directamente en W o en Z.
Si $W = V$, cualquier vector propio de A_1 $\mathbf{v}$ cumple que $A_2\mathbf{v} = \lambda\mathbf{v}$, luego también tenemos la propiedad. □

Lema 4.8.2. *Si $k = \mathbb{R}$, $\mathscr{P}_{k,r}(2)$ son ciertas para $r = 1, 2$.*

PRUEBA: Por el lema anterior bastaría probar que $\mathscr{P}_{\mathbb{R},1}(2)$ es cierta, esto es, que todo endomorfismo de un espacio vectorial sobre $\mathbb{R}$ de dimensión impar tiene un autovector no nulo, pero eso es equivalente a que su polinomio característico $f(x) = \det(xI - A)$ tenga alguna raíz en $\mathbb{R}$. Ahora bien, $f(x)$ es un polinomio de grado impar con coeficientes reales, y ya hemos visto que siempre tiene al menos una raíz real. □

Lema 4.8.3. *Todo endomorfismo de un $\mathbb{C}$-espacio vectorial de dimensión impar tiene un autovector no nulo, esto es, $\mathscr{P}_{\mathbb{C},1}(2)$ se cumple.*

PRUEBA: Sea $A : \mathbb{C}^n \to \mathbb{C}^n$ un endomorfismo con n impar, y sea $V = \mathrm{Herm}_n(\mathbb{C})$, el $\mathbb{R}$-espacio vectorial de las matrices hermíticas (aquellas que $A^* = \overline{A}^t = A$) de orden $n \times n$. Consideremos los siguientes endomorfismos $\mathbb{R}$-lineales de V definidos como:

$$L_1(B) = \frac{AB + BA^*}{2}\ ,\ L_2(B) = \frac{AB - BA^*}{2i}.$$

Ver que L_1 y L_2 están bien definidos y conmutan es un cálculo bien sencillo y no lo escribiremos en estas líneas.

Sabemos que $\dim_{\mathbb{R}} V = n^2$, que es impar. Entonces, por el lema anterior, L_1 y L_2 comparten un autovector no nulo al cumplirse $\mathscr{P}_{\mathbb{R},2}(2)$. Sea $\mathbf{B}$ ese autovector en V, cuyos valores propios asociados sean λ y μ respectivamente. En ese caso,

$$(L_1 + iL_2)(\mathbf{B}) = A\mathbf{B} = (\lambda + \mu i)\mathbf{B},$$

luego cualquier columna no nula de $\mathbf{B}$ constituirá uno de los autovectores buscados para A. $\square$

Ya hemos acabado el ensamblaje de lemas previos al resultado que nos bastaba para probar el teorema fundamental del álgebra. No hemos usado más que algunas propiedades básicas de espacios vectoriales y matrices. Ahora demostremos la proposición siguiente.

Proposición 4.8.4. *Para todo $r \in \mathbb{N}$ se cumple $\mathscr{P}_{\mathbb{C},1}(2^r)$.*

PRUEBA: Se hará por inducción en r. Si $r = 1$ es el enunciado del lema anterior, así que supongamos como hipótesis de inducción que tenemos $\mathscr{P}_{\mathbb{C},1}(2^l)$, con $l < r$.
Tomemos pues un endomorfismo $\mathbb{C}$-lineal $A : \mathbb{C}^n \to \mathbb{C}^n$, con n divisible por 2^{r-1} pero no por 2^r. Esto lo podemos asumir, puesto que si n no fuera divisible por 2^{r-1} estaríamos en el caso de probar $\mathscr{P}_{\mathbb{C},1}(2^{r-1})$. Sea $V = \mathrm{Ant}_n(\mathbb{C})$ el $\mathbb{C}$-espacio vectorial de las matrices antisimétricas con coeficientes complejos. Definamos dos endomorfismos de V, L_1 y L_2 como

$$L_1(B) = AB - BA^t \, , \, L_2(B) = ABA^t.$$

De nuevo, no probaremos que están bien definidos ni que conmutan entre ellos, y queda para el lector.

Notemos que 2^{r-1} no divide a $\dim V$, que es igual a $n(n-1)/2$. Por tanto, por la hipótesis de inducción, existe un vector propio $\mathbf{B}$ común a L_1 y L_2. Sean sus autovalores asociados λ y μ, respectivamente. Así,

$$\mu\mathbf{B} = A\mathbf{B}A^t = A(A\mathbf{B} - \lambda\mathbf{B}),$$

es decir,

$$(A^2 - \lambda A - \mu I)\mathbf{B} = \mathbf{0}.$$

Sea $\mathbf{v}$ un vector columna de $\mathbf{B}$, y sean α y β las dos raíces complejas del polinomio $x^2 - \lambda x - \mu$, que sí que sabemos que tiene raíces en $\mathbb{C}$, porque es de grado 2. Si llamamos $\mathbf{w} = (A - \beta I)\mathbf{v}$ y es no nulo, tenemos que $(A - \alpha I)\mathbf{w} = \mathbf{0}$, y hemos terminado, siendo $\mathbf{w}$ el autovector que buscábamos. Si $\mathbf{w} = \mathbf{0}$ eso querría decir que $(A - \beta I)\mathbf{v} = \mathbf{0}$, siendo $\mathbf{v}$ el vector propio buscado. $\square$