

## tema 13

# MATEMÁTICAS

### **13. El anillo de polinomios. Divisibilidad y factorización. Aplicación del Teorema Fundamental del Álgebra. Criterios de irreducibilidad de polinomios.**

- 13.1. El anillo de polinomios.
- 13.2. Divisibilidad y factorización.
- 13.3. Aplicación del Teorema Fundamental del Álgebra.
- 13.4. Criterios de irreducibilidad de polinomios.





## **1. EL ANILLO DE LOS POLINOMIOS**

---

## **2. DIVISIBILIDAD Y FACTORIZACIÓN**

---

- 2.1. ALGORITMO DE DIVISIÓN
- 2.2. ALGORITMO DE EUCLIDES. IGUALDAD DE BÉZOUT
- 2.3. FACTORIZACIÓN
- 2.4. LEMA DE GAUSS

## **3. APLICACIÓN DEL TEOREMA FUNDAMENTAL DEL ÁLGEBRA**

---

## **4. CRITERIOS DE IRREDUCIBILIDAD DE POLINOMIOS**

---

- 4.1. POLINOMIOS IRREDUCIBLES EN  $\mathbb{R}[X]$
- 4.2. CRITERIOS DE IRREDUCIBILIDAD EN  $\mathbb{Q}[X]$



## INTRODUCCIÓN

Encontrar las raíces de un polinomio en una variable es uno de los problemas más antiguos en Matemáticas, pero hasta el siglo xv no se desarrolló la notación actual. En el siglo xvi G. Cardano encontró las fórmulas generales para las soluciones de las ecuaciones de tercer y cuarto grado, mucho más complejas que las de segundo grado. Fueron E. Galois y N. H. Abel los que demostraron que no existen tales fórmulas para grado 5 y mayores: hay polinomios de esos grados cuyas soluciones no son expresables por radicales.

Los polinomios en general, en varias variables, sirven para modelizar infinidad de problemas en Química, Física, Economía e Ingenierías y su estudio es uno de los pilares del Álgebra Abstracta.

Se hace un estudio de los anillos de polinomios en general, sobre un anillo de coeficientes arbitrario. Se estudian la división, cuando sea posible, el concepto de máximo común divisor, la identidad de Bézout, y la factorización única cuando el anillo de coeficientes es un cuerpo. Se da una prueba del teorema fundamental del Álgebra por métodos analíticos, y, por último, se estudia la irreducibilidad en  $\mathbb{R}[X]$  y  $\mathbb{Q}[X]$ .

En Secundaria y Bachillerato los alumnos aprenden a manejar las operaciones básicas con polinomios (división, máximo común divisor, factorización) y a resolver las ecuaciones más sencillas. Es importante hacerles ver desde el principio que un polinomio puede ser reducible y no tener raíces en el cuerpo en el que trabajemos. Los alumnos con más interés pueden trabajar con las fórmulas de Cardano o acceder a métodos sencillos numéricos de aproximación de raíces.

## 1. EL ANILLO DE LOS POLINOMIOS

Recordemos que un *anillo* es un conjunto en el que se han definido dos operaciones que se suelen denotar  $+$  y  $\cdot$ , suma y producto, que es *grupo conmutativo* con la suma, *semigrupo* (no necesariamente conmutativo) para el producto y que verifica la propiedad distributiva de la suma respecto del producto. Ejemplos de anillos son cualquier cuerpo  $k$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}/\mathbb{Z}n$  o  $\mathcal{M}_{m \times n}(k)$ , las matrices de  $m$  filas y  $n$  columnas con entradas en un cuerpo  $k$ .

► **Definición 1.1.**

Sea  $A$  un anillo. El *anillo de polinomios* en la indeterminada  $X$  con coeficientes en  $A$ , y que notaremos por  $A[X]$ , es el conjunto de expresiones formales:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

con cada  $a_i \in A$ . El elemento  $a_i$  se denomina el *coeficiente* de  $X^i$  en  $f(X)$ .

Dos polinomios se consideran iguales si para cada  $i$  los coeficientes de  $X^i$  son iguales. Por claridad, eliminamos los coeficientes nulos cuando escribimos un polinomio. El *polinomio cero* es el que tiene todos sus coeficientes igual a 0, y lo notaremos como 0.

► **Definición 1.2.**

El *grado* de  $f(X)$  es el mayor  $n$  tal que  $a_n$  es no nulo.

Si  $\text{grado}(f(X)) = n$  escribiremos  $f(X) = \sum_{k=0}^n a_k X^k$ . El coeficiente  $a_n$  se denomina *coeficiente líder* de  $f(X)$ . Si es igual a 1, decimos que  $f(X)$  es un polinomio *mónico*.

Asignamos  $\text{grado}(0) = -\infty$  y, por conveniencia en el manejo de fórmulas, establecemos que  $-\infty < n$  y  $-\infty + n = -\infty$  para cualquier  $n$  entero no negativo.

Se definen dos operaciones en  $A[X]$ . Sean:

$$f(X) = a_n X^n + \dots + a_1 X + a_0,$$

$$g(X) = b_n X^n + \dots + b_1 X + b_0.$$

- Suma.  $f(X) + g(X)$  es el polinomio con coeficiente en  $X^i$  igual a  $a_i + b_i$ . Algunos de los  $a_n$  o  $b_n$  puede ser cero para que la suma de polinomios de diferente grado tenga sentido.
- Producto. Primero definimos el producto de monomios como:

$$(aX^i)(bX^j) = abX^{i+j},$$

y se extiende a todos los polinomios mediante las leyes distributivas (lo que habitualmente conocemos como desarrollo y agrupación de términos comunes):

$$\begin{aligned} &(a_0 + a_1 X + a_2 X^2 + \dots) \cdot (b_0 + b_1 X + b_2 X^2 + \dots) \\ &= a_0 b_0 + (a_1 b_0 + a_0 b_1) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + \dots \end{aligned}$$

En general, el coeficiente de  $X^l$  igual a  $a_l b_0 + a_{l-1} b_1 + \dots + a_0 b_l = \sum_{i+j=l} a_i b_j$ .

La definición anterior hace que el producto sea distributivo con respecto a la suma.

► **Proposición 1.3.**

El conjunto  $(A[X], +)$  es un grupo.

*Demostración.*

La operación es interna, el elemento neutro es el polinomio cero, y dado un polinomio:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

su opuesto es:

$$-f(X) = (-a_n)X^n + (-a_{n-1})X^{n-1} + \dots + (-a_1)X + (-a_0).$$

Como  $A$  es un grupo con la suma, se tienen también las propiedades conmutativa y asociativa. □

► **Proposición 1.4.**

El producto en  $A[X]$  es asociativo.

*Demostración.*

Consideremos los polinomios  $f(X), g(X), h(X)$ , y veamos que:

$$(f(X) \cdot g(X)) \cdot h(X) = f(X) \cdot (g(X) \cdot h(X)).$$

Por la propiedad distributiva, basta ver el caso en el que  $f(X) = aX^i$ . Si escribimos  $g(X) = \sum_j b_j X^j, h(X) = \sum_k c_k X^k$ , tenemos que:

$$\begin{aligned} (aX^i \cdot g(X)) \cdot h(X) &= \left( \sum_j ab_j X^{i+j} \right) \sum_k c_k X^k = \sum_l \left( \sum_{i+j+k=l} ab_j c_k \right) X^l, \\ aX^i \cdot (g(X) \cdot h(X)) &= aX^i \sum_s \left( \sum_{j+k=s} b_j c_k \right) X^s = \sum_s \left( \sum_{j+k=s} ab_j c_k \right) X^{i+s}, \end{aligned}$$

y ambas expresiones son iguales sin más que hacer  $i + s = l$ . □

El elemento identidad con respecto al producto es el polinomio 1. Con estas operaciones,  $A[X]$  es un anillo.

► **Ejemplo 1.5.**

El producto en el anillo de polinomios es conmutativo si y sólo si el anillo de coeficientes lo es: así  $\mathbb{R}[X]$  o  $\mathbb{Z}[X]$  son conmutativos, pero  $\mathcal{M}_{m \times n}(k)[X]$  no lo es porque el producto de matrices no lo es en general. Con todo, si no se menciona lo contrario, se supone que un anillo de polinomios es conmutativo.

*Nota 1.6.*

Sea  $A = k$  un cuerpo, y consideremos el anillo de polinomios  $k[X]$ . Si  $f(X) = \sum_i a_i X^i$ , podemos definir la operación:

$$\alpha \cdot f(X) = \sum_i (\alpha a_i) X^i,$$

que dota a  $k[X]$  de estructura de  $k$ -espacio vectorial. Es uno de los ejemplos clásicos de espacio vectorial de dimensión infinita.

*Nota 1.7.*

La definición del anillo de polinomios se puede formalizar a partir de un espacio de funciones. Así, un elemento  $f \in A[X]$  es una función  $f: \mathbb{Z}^+ \rightarrow A$  tal que  $f(n) \neq 0$  en un número finito de enteros no negativos  $n$ . Las operaciones de suma y producto se definen como:

$$\begin{aligned}(f + g)(n) &= f(n) + g(n), \\ (f \cdot g)(n) &= \sum_{m=0}^n f(m)g(n-m).\end{aligned}$$

Observemos que la indeterminada  $X$  no aparece en esta definición. Para ver que nuestra descripción inicial de  $A[X]$  coincide con esta, definimos  $X$  como la función sobre  $\mathbb{Z}^+$  dada por:

$$X(m) = \begin{cases} 1 & \text{si } m = 1, \\ 0 & \text{si } m \neq 1. \end{cases}$$

Con la definición que hemos dado del producto, la función  $X^n = X \cdot X \cdots X$  verifica:

$$X^n(m) = \begin{cases} 1 & \text{si } m = n, \\ 0 & \text{si } m \neq n. \end{cases}$$

Entonces, cualquier elemento  $f \in A[X]$  se puede escribir de forma única como:

$$f = \sum_{n \geq 0} f(n)X^n,$$

donde la suma es sobre un número finito de términos. Se tiene que  $X^0$  es la función:

$$X^0(n) = \begin{cases} 1 & \text{si } n = 0, \\ 0 & \text{si } n > 0. \end{cases}$$

De esta forma tenemos la inclusión  $A \hookrightarrow A[X]$ .

Recordemos que un *homomorfismo de anillos* es una aplicación entre dos anillos  $A$  y  $B$  que lleva el 1 de  $A$  en el 1 de  $B$ , y que respeta la suma y el producto. Si es biyectiva, es un *isomorfismo* de anillos. Si  $A = B$ , los isomorfismos se denominan *automorfismos*. El cambio de variable en un polinomio por la variable menos un escalar es, trivialmente, de este tipo:

► **Lema 1.8.**

Sea  $a \in A$ . La aplicación  $\Phi: A[X] \rightarrow A[X]$  definida por  $\Phi(f(X)) = f(X - a)$  es un automorfismo de anillos.

► **Lema 1.9.**

Sea  $A$  un anillo y  $f(X), g(X) \in A[X]$ . Entonces:

1.  $\text{grado}(f(X) + g(X)) \leq \text{máx}\{\text{grado}(f(X)), \text{grado}(g(X))\}$ .
2.  $\text{grado}(f(X)g(X)) \leq \text{grado}(f(X)) + \text{grado}(g(X))$ .
3. La igualdad se tiene en el caso anterior si los coeficientes líderes de  $f(X)$  y  $g(X)$  no son divisores de cero. En particular, cuando  $A$  es un dominio de integridad.

La prueba es inmediata.

*Nota 1.10.*

En lo que sigue simplificaremos la notación en los anillos de polinomios  $\mathbb{Z}/\mathbb{Z}n[X]$ , escribiendo simplemente un coeficiente  $a$  cuando nos referimos en realidad a  $\bar{a} = a + \mathbb{Z}n$ .

Si los coeficientes no están en un dominio de integridad (esto es, si existen elementos no nulos  $a, b \in A$  tales que  $a \cdot b = 0$ ) entonces se puede dar la desigualdad estricta del segundo apartado: por ejemplo en  $\mathbb{Z}/\mathbb{Z}4[X]$ , se tiene que:

$$\text{grado}((2X)(2X)) = \text{grado}(0) = -\infty < \text{grado}(2X) + \text{grado}(2X) = 2.$$

► **Corolario 1.11.**

Si  $A$  es un dominio de integridad, entonces:

1.  $A[X]$  es un dominio de integridad.
2. Las unidades de  $A[X]$  son las unidades de  $A$ .

Recordemos que una *unidad* es un elemento con inverso para el producto. La segunda parte del corolario es consecuencia de que el producto de polinomios no constantes es no constante en un dominio de integridad.

## 2. DIVISIBILIDAD Y FACTORIZACIÓN

Veremos en esta sección el concepto de divisibilidad y de factorización de un polinomio. Los resultados son muy similares a los correspondientes para enteros. Terminamos con el lema de Gauss que relaciona la factorización de un polinomio en  $\mathbb{Z}[X]$  y en  $\mathbb{Q}[X]$ .

### 2.1. ALGORITMO DE DIVISIÓN

Sean  $f(X) = a_0 + a_1X + \dots + a_nX^n \in A[X]$  y  $g(X) = b_0 + b_1X + \dots + b_{m-1}X^{m-1} + b_mX^m$  un polinomio mónico, de grado  $m \geq 1$ . Si  $n \geq m$ , sea  $q_1(X) = a_nX^{n-m}$ . Entonces  $f_1(X) = f(X) - g(X)q_1(X)$  tiene grado menor o igual que  $n - 1$ . Si  $\text{grado}(f_1(X)) \geq m$ , podemos repetir el proceso con  $f_1(X)$ . Tras un número finito de pasos llegamos a un polinomio  $f_s(X)$  de grado estrictamente menor que  $m$ . Si llamamos:

$$q(X) = q_1(X) + \dots + q_s(X),$$

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

obtenemos una ecuación:

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

donde  $\text{grado}(r(X)) < \text{grado}(g(X))$ . Este proceso no es más que la tradicional división de polinomios. Observemos que si  $g(X)$  no es mónico, el proceso puede no ser posible:

► **Ejemplo 2.1.**

En  $\mathbb{Z}[X]$ , si  $f(X) = 3X^2$  y  $g(X) = 2X$ , no existe un monomio  $m(X)$  en  $\mathbb{Z}[X]$  tal que  $m(X) \cdot (2X) = 3X^2$  y la división no es posible.

► **Proposición 2.2** (Algoritmo de división).

Sea  $A$  un anillo,  $f(X), g(X) \in A[X]$  con  $g(X)$  mónico. Entonces existen unos únicos  $q(X), r(X) \in A[X]$  con  $\text{grado}(r(X)) < \text{grado}(g(X))$  tales que:

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

*Demostración.*

La existencia se sigue de la nota anterior. Consideremos ahora la unicidad. Supongamos que existen dos descomposiciones:

$$f(X) = g(X)q(X) + r(X) \quad \text{y} \quad f(X) = g(X)q_1(X) + r_1(X),$$

con  $\text{grado}(r(X)) < \text{grado}(g(X))$  y  $\text{grado}(r_1(X)) < \text{grado}(g(X))$ . Entonces:

$$g(X)(q_1(X) - q(X)) = r(X) - r_1(X).$$

Como  $g(X)$  es un polinomio mónico, si comparamos los grados de ambos lados de la igualdad:

$$\text{grado}(g(X)) + \text{grado}(q_1(X) - q(X)) = \text{grado}(r(X) - r_1(X)) < \text{grado}(g(X)).$$

Esto obliga a que  $\text{grado}(q_1(X) - q(X)) = -\infty$ , esto es,  $q_1(X) = q(X)$ . De aquí se deduce que  $r_1(X) = r(X)$ , y hemos establecido la unicidad.  $\square$

*Nota 2.3.*

1. Decimos que  $g(X)$  divide a  $f(X)$ ,  $g(X)|f(X)$ , si en el proceso anterior se obtiene  $r(X) = 0$ .
2. En el caso  $A = k$  un cuerpo, el algoritmo anterior se tiene siempre, pues el coeficiente líder de  $g(X)$  es una unidad.
3. Si  $g(X)$  no es mónico, se puede conseguir una pseudo-división de la forma:

$$c \cdot f(X) = g(X)q(X) + r(X)$$

con  $c \in A$ .

► **Ejemplo 2.4.**

En el ejemplo anterior, para  $f(X) = 3X^2$  y  $g(X) = 2X$  en  $\mathbb{Z}[X]$  podemos dividir  $2f(X)$  entre  $g(X)$ .

Dado un polinomio  $f(X) \in A[X]$ , tiene sentido *evaluar* la función que define el polinomio de forma natural para un  $a \in A$ , y lo notaremos como  $f(a)$ . Sin embargo es importante resaltar que los polinomios son expresiones formales y no debemos confundirlos con las funciones que definen.

► **Ejemplo 2.5.**

En  $\mathbb{Z}/\mathbb{Z}2[X]$  el polinomio  $X^2 + X$  y el polinomio  $0$  son distintos, pero definen ambos la función idénticamente  $0$ .

El teorema de división se puede aplicar si  $g(X) = X - a$  con  $a \in A$  con interesantes consecuencias:

► **Corolario 2.6** (Teorema del resto).

Sea  $A$  un anillo y  $a \in A$ . Entonces para cualquier  $f(X) \in A[X]$  existe  $q(X) \in A[X]$  tal que:

$$f(X) = (X - a)q(X) + f(a).$$

*Demostración.*

Por el teorema de división, podemos escribir:

$$f(X) = q(X)(X - a) + r(X),$$

donde  $\text{grado}(r(X)) \leq 0$ . Entonces  $r(X) = r \in A$ . Si aplicamos el morfismo de sustitución,  $X \mapsto a$ , tenemos que  $f(a) = (a - a)q(a) + r$ , luego  $r = f(a)$ .  $\square$

► **Corolario 2.7** (Teorema de la raíz).

Sea  $f(X) \in A[X]$  y  $a \in A$ . Entonces  $f(a) = 0$  si y solamente si  $X - a$  divide a  $f(X)$ .

*Demostración.*

Se tiene que  $f(a) = 0$  implica  $f(X) = (X - a)q(X)$ . Si  $f(X) = (X - a)q(X)$  entonces  $f(a) = (a - a)q(a) = 0$ . □

Un elemento  $a$  tal que  $f(a) = 0$  se denomina *raíz* de  $f(X)$ .

► **Corolario 2.8** (Teorema de D'Alembert).

Sea  $A$  un dominio de integridad y  $f(X) \neq 0 \in A[X]$  un polinomio de grado  $n$ . Entonces existen a lo más  $n$  raíces de  $f(X)$  en  $A$ .

*Demostración.*

Si  $n = 0$ , el resultado es cierto, ya que  $f(X) = a_0 \neq 0$  implica que  $f(a) = a_0 \neq 0$  para todo  $a \in A$ , esto es,  $f(X)$  no tiene raíces. Ahora supongamos que  $n > 0$ , y, por inducción, que el resultado es cierto para todos los polinomios de grado menor que  $n$ . Si no hay raíces de  $f(X)$  en  $A$ , no hay nada que probar. Supongamos entonces que existe  $a \in A$  raíz de  $f(X)$ . Por el teorema de la raíz, podemos escribir  $f(X) = (X - a)q(X)$ , donde  $\text{grado}(q(X)) = n - 1$ . Por la hipótesis de inducción, existen, a lo más,  $n - 1$  raíces de  $q(X)$  en  $A$ . Si  $b$  es una raíz de  $f(X)$ , tenemos que  $0 = f(b) = (b - a)q(b)$ , y deducimos que  $b = a$  o  $b$  es raíz de  $q(X)$ . En conclusión,  $f(X)$  tiene, a lo más,  $(n - 1) + 1$  raíces en  $A$ . □

► **Definición 2.9.**

Sea  $f(X) \in A[X]$  un polinomio no nulo y  $a \in A$  una raíz de  $f(X)$ . Entonces  $X - a$  divide a  $f(X)$  en  $A[X]$ . Al máximo entero  $s > 0$  tal que  $(X - a)^s | f(X)$  se le llama la *multiplicidad* de  $a$  como raíz de  $f(X)$ . Se dirá que  $a$  es una raíz *simple* de  $f(X)$  si  $s = 1$ . En caso contrario se dirá que es *múltiple*.

*Nota 2.10.*

Una forma sencilla de realizar la división de un polinomio por un monomio de la forma  $X - a$  es mediante la *regla de Ruffini*. Supongamos que:

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

es un polinomio, con  $a_n \neq 0$ , y lo queremos dividir por  $X - a$ . El procedimiento es como sigue:

1. Colocamos los coeficientes de  $f(X)$  de mayor a menor grado, y escribimos  $a$  en la esquina inferior izquierda:

$$\begin{array}{r|rrrrr} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ a & & & & & \\ \hline & & & & & \end{array}$$

2. Colocamos el coeficiente  $a_n$  en la parte inferior del recuadro, multiplicamos  $a$  por  $a_n$ , y el resultado lo ponemos debajo del coeficiente  $a_{n-1}$ :

$$\begin{array}{r|rrrrrr} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ a & & aa_n & & & \\ \hline & a_n & & & & \end{array}$$

3. Sumamos los coeficientes que aparecen en la columna  $n - 1$ , y lo llamamos  $a'_{n-1}$ :

$$\begin{array}{r|rrrrrr} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ a & & aa_n & & & \\ \hline & a_n & \underbrace{a_{n-1} + aa_n}_{a'_{n-1}} & & & \end{array}$$

4. Repetimos el procedimiento hasta llegar a  $a_0$ :

$$\begin{array}{r|rrrrrr} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ a & & aa_n & \dots & aa'_2 & aa'_1 \\ \hline & a_n & \underbrace{a_{n-1} + aa_n}_{a'_{n-1}} & \dots & \underbrace{a_1 + aa'_2}_{a'_1} & \underbrace{a_0 + aa'_1}_{a'_0} \end{array}$$

Entonces se tiene que:

$$f(X) = (X - a)(a_n X^{n-1} + a'_{n-1} X^{n-2} + \dots + a'_2 X + a'_1) + a'_0,$$

como se puede ver por inducción sobre el grado de  $f(X)$ . Observemos que  $a$  es raíz de  $f(X)$  si y solamente si  $a'_0 = 0$ , y además conseguimos una factorización. Por el teorema del resto,  $f(a) = a'_0$ .

## 2.2. ALGORITMO DE EUCLIDES. IGUALDAD DE BÉZOUT

De forma análoga a como se hace en los enteros, se puede considerar en los anillos de polinomios con coeficientes en un cuerpo el algoritmo de Euclides que produce un máximo común divisor de dos polinomios y la identidad de Bézout para polinomios.

► **Definición 2.11.**

Sean  $f(X), g(X) \in k[X]$ . Un *máximo común divisor* de  $f(X), g(X)$  es un elemento  $d(X) \in k[X]$  tal que:

- $d(X) | f(X)$  y  $d(X) | g(X)$ .
- Si  $e(X) | f(X)$  y  $e(X) | g(X)$  entonces  $e(X) | d(X)$ .

Lo escribiremos como  $d(X) = \text{mcd}(f(X), g(X))$ .

El algoritmo de Euclides para encontrar *un* máximo común divisor (si multiplicamos por cualquier elemento no nulo del cuerpo sigue verificando la definición) funciona igual que en los enteros.

Dados  $f(X), g(X) \in k[X]$  vamos dividiendo sucesivamente:

$$\begin{aligned} f(X) &= q(X)g(X) + r(X) & 0 \leq \text{grado}(r(X)) < \text{grado}(g(X)) \\ g(X) &= q_0(X)r(X) + r_1(X) & 0 \leq \text{grado}(r_1(X)) < \text{grado}(r(X)) \\ r(X) &= q_1(X)r_1(X) + r_2(X) & 0 \leq \text{grado}(r_2(X)) < \text{grado}(r_1(X)) \\ &\vdots \\ r_{n-1}(X) &= q_n(X)r_n(X) + r_{n+1}(X) & 0 \leq \text{grado}(r_{n+1}) < \text{grado}(r_n(X)) \\ r_n(X) &= q_{n+1}(X)r_{n+1}(X) + 0 & (r_{n+2}(X) = 0) \end{aligned}$$

Es muy sencillo ver que:

$$\begin{aligned} \text{mcd}(f(X), g(X)) &= \text{mcd}(g(X), r(X)) = \text{mcd}(r(X), r_1(X)) = \dots = \\ &= \text{mcd}(r_n(X), r_{n+1}(X)) = r_{n+1}(X). \end{aligned}$$

El último resto no nulo es un máximo común divisor.

► **Ejemplo 2.12.**

Calculemos un máximo común divisor de  $X^5 + 1$  y  $X^3 + 1$  en  $\mathbb{Z}/\mathbb{Z}2[X]$ :

$$\begin{aligned} X^5 + 1 &= X^2(X^3 + 1) + (X^2 + 1), \\ X^3 + 1 &= X(X^2 + 1) + (X + 1), \\ X^2 + 1 &= (X + 1)(X + 1) + 0. \end{aligned}$$

Luego  $\text{mcd}(X^5 + 1, X^3 + 1) = X + 1$ .

En las divisiones del algoritmo de Euclides, si despejamos los restos y los sustituimos en las divisiones anteriores obtenemos una expresión del máximo común divisor como combinación de los polinomios iniciales con coeficientes polinomios. Es la *identidad de Bézout* para polinomios.

► **Proposición 2.13** (Identidad de Bézout).

Sean  $f(X), g(X) \in k[X]$  y  $d(X)$  un máximo común divisor de  $f(X)$  y  $g(X)$ . Podemos encontrar  $a(X), b(X) \in k[X]$  tales que  $d(X) = a(X)f(X) + b(X)g(X)$ .

► **Ejemplo 2.14.**

En el ejemplo anterior, se obtiene:

$$X + 1 = X(X^5 + 1) + (X^3 + 1)(X^3 + 1).$$

### 2.3. FACTORIZACIÓN

---

► **Definición 2.15.**

En  $k[X]$ , un elemento  $p(X)$  es *irreducible* si no es una unidad y  $p(X) = f(X)g(X)$  implica que  $f(X)$  o  $g(X)$  es una unidad (un polinomio constante). Dos elementos  $f(X), g(X) \in k[X]$  se dicen *asociados* si existe una unidad  $u \in k$  tal que  $f(X) = ug(X)$ .

De la definición se deduce:

► **Proposición 2.16.**

Si  $p(X)$  es un polinomio irreducible y  $f(X)$  es un polinomio no divisible por  $p(X)$ , entonces  $\text{mcd}(f(X), p(X)) = 1$ .

► **Ejemplo 2.17.**

Algunos ejemplos de polinomios irreducibles en distintos anillos de polinomios son:

- $X + a$ ,  $a \in k$  en  $k[X]$ .
- $X^2 + 1 \in \mathbb{R}[X]$ . En  $\mathbb{C}[X]$  no lo es.
- $X^3 - 2 \in \mathbb{Q}[X]$ . En  $\mathbb{R}[X]$  no lo es.
- $X^2 + 1 \in \mathbb{Z}/\mathbb{Z}3[X]$ . En  $\mathbb{Z}/\mathbb{Z}5[X]$  no lo es.

Los polinomios irreducibles juegan el papel de los números primos en los enteros. Como consecuencia de la identidad de Bézout tenemos el siguiente resultado:

► **Lema 2.18.**

Sea  $p(X) \in k[X]$  irreducible. Si  $p(X)$  divide a  $f(X)g(X)$  entonces  $p(X)$  divide a  $f(X)$  o a  $g(X)$ .

*Demostración.*

Si  $p(X)$  no divide a  $f(X)$  se tiene que  $1 = a(X)p(X) + b(X)f(X)$  y de aquí:

$$g(X) = g(X)a(X)p(X) + g(X)b(X)f(X),$$

y como  $p(X)$  divide a los dos sumandos, divide a  $g(X)$ . □

Todo polinomio en  $k[X]$  de grado al menos 1 es irreducible o producto de irreducibles:

► **Proposición 2.19.**

Sea  $f(X) \in k[X]$ . Entonces  $f(X)$  se puede escribir como:

$$f(X) = uq_1(X) \cdots q_m(X)$$

donde  $u$  es una unidad y cada  $q_i(X)$  es irreducible. Además, esta factorización es única en el sentido de que si  $f(X) = vp_1(X) \cdots p_n(X)$  con  $v$  unidad y cada  $p_i(X)$  irreducible entonces  $m = n$  y existe una permutación  $\sigma$  de  $\{1, \dots, n\}$  tal que:

$$p_i(X) = w_i q_{\sigma(i)}(X)$$

con  $w_i$  unidad.

*Demostración.*

La existencia de la factorización es por inducción sobre el grado de  $f(X)$ . Si  $f(X)$  es irreducible, hemos acabado. En otro caso, se puede expresar como producto:

$$f(X) = f_1(X)f_2(X),$$

con:

$$\text{grado}(f(X)) > \text{grado}(f_1(X)), \text{grado}(f_2(X)).$$

Veamos la unicidad. Si:

$$uq_1(X) \cdots q_m(X) = vp_1(X) \cdots p_n(X)$$

entonces  $q_1(X)$  divide a algún  $p_i(X)$ . Como son irreducibles, existe  $w_i$  unidad tal que  $q_1(X) = w_i p_i(X)$ . Por inducción tenemos el resultado.  $\square$

*Nota 2.20.*

Como ocurre en los enteros (una vez más), si tenemos la descomposición en factores irreducibles es muy fácil hallar el máximo común divisor de dos polinomios tomando los factores comunes elevados al menor exponente.

## 2.4. LEMA DE GAUSS

---

► **Definición 2.21.**

Sea  $f(X) \in \mathbb{Z}[X]$  un polinomio no nulo. Llamamos *contenido* de  $f(X)$  a un máximo común divisor de los coeficientes de  $f(X)$ , y lo notaremos por  $c(f(X))$ . Decimos que el polinomio  $f(X)$  es *primitivo* si  $c(f(X)) = 1$ .

Observemos que el contenido de  $f(X)$  está unívocamente determinado salvo multiplicación por una unidad de  $\mathbb{Z}$ . Si  $f(X) \in \mathbb{Z}[X]$  es un polinomio no nulo entonces podemos escribir  $f(X) = c f_1(X)$ , donde  $c$  es el contenido de  $f(X)$  y  $f_1(X)$  es primitivo.

► **Lema 2.22.**

Sean  $f(X), g(X)$  polinomios no nulos de  $\mathbb{Z}[X]$ . Entonces:

$$c(f(X)g(X)) = c(f(X)) \cdot c(g(X)).$$

En particular, si  $f(X)$  y  $g(X)$  son primitivos entonces el producto  $f(X)g(X)$  es primitivo.

*Demostración.*

Observemos que, dado un primo  $p \in \mathbb{Z}$ , el anillo  $\mathbb{Z}/\mathbb{Z}p[X]$  es un dominio de integridad. Hay un homomorfismo natural:

$$\phi: \mathbb{Z}[X] \rightarrow \mathbb{Z}/\mathbb{Z}p[X]$$

que transforma un polinomio en el mismo con los coeficientes módulo  $p$ . Sean  $f(X), g(X)$  polinomios no nulos de  $\mathbb{Z}[X]$ . Como  $\phi(f(X)g(X)) = \phi(f(X))\phi(g(X))$ , se tiene que  $\phi(f(X)g(X)) = 0$  si y solamente si  $\phi(f(X)) = 0$  o  $\phi(g(X)) = 0$ . En otras palabras,  $p$  es un factor irreducible de  $c(f(X)g(X))$  si y solamente si  $p$  es factor irreducible de  $c(f(X))c(g(X))$ . En concreto,  $f(X)g(X)$  es primitivo si y solamente si  $f(X)$  y  $g(X)$  lo son.

A partir del caso particular obtenemos el caso general. Escribamos  $f(X) = cf_1(X)$ ,  $g(X) = dg_1(X)$ , con  $f_1(X)$ ,  $g_1(X)$  primitivos. Entonces:

$$f(X)g(X) = cd f_1(X)g_1(X),$$

con  $f_1(X)g_1(X)$  primitivo, y se deduce que  $c(f(X)g(X)) = cd = c(f(X)) \cdot c(g(X))$ .  $\square$

► **Lema 2.23.**

Si  $f(X) \in \mathbb{Q}[X]$  es un polinomio no nulo, entonces  $f(X) = \alpha f_1(X)$  con  $\alpha \in \mathbb{Q}$  y  $f_1(X)$  un elemento primitivo de  $\mathbb{Z}[X]$ . Esta factorización es única salvo producto por una unidad de  $\mathbb{Z}$ .

*Demostración.*

Consideremos  $d$  un denominador común de los coeficientes de  $f(X)$ , y podemos escribir  $f(X) = (1/d)g(X)$  donde  $g(X) \in \mathbb{Z}[X]$ . Sea  $\alpha = c(g(X))/d \in \mathbb{Q}$ . Entonces  $f(X) = \alpha f_1(X)$  con  $f_1(X)$  polinomio primitivo. Consideremos ahora la unicidad. Supongamos que  $f(X) = \beta f_2(X)$ , con  $f_2(X)$  polinomio primitivo de  $\mathbb{Z}[X]$ , y  $\beta = a/b$ . Entonces:

$$adf_2(X) = cbf_1(X).$$

El contenido de la parte izquierda es  $ad$  y el de la parte derecha es  $cb$ , luego existe  $u \in \mathbb{Z}$  unidad tal que  $ad = ucb$ . Entonces  $uf_2(X) = f_1(X)$  y los coeficientes satisfacen la misma relación  $\beta = a/b = u(c/d) = u\alpha$ .  $\square$

► **Lema 2.24 (Gauss).**

Sea  $f(X) \in \mathbb{Z}[X]$ . Son equivalentes:

1.  $f(X)$  tiene grado positivo y es irreducible en  $\mathbb{Z}[X]$ .
2.  $c(f(X)) = 1$  y  $f(X)$  es irreducible en  $\mathbb{Q}[X]$ .

*Demostración.*

Supongamos que  $f(X) \in \mathbb{Z}[X]$  es irreducible y de grado positivo. Entonces  $f(X)$  es primitivo ya que  $c(f(X))$  divide a  $f(X)$ , y todo elemento irreducible de  $\mathbb{Z}$  lo es también en  $\mathbb{Z}[X]$ . Para ver que es irreducible en  $\mathbb{Q}[X]$ , pongamos  $f(X) = g_1(X)g_2(X)$ , con  $g_1(X) \in \mathbb{Q}[X]$ ,  $i = 1, 2$ , y  $g_2(X)$  de grado positivo. Entonces  $g_i(X) = \alpha_i f_i(X)$ , donde  $\alpha_i \in \mathbb{Q}$  y  $f_i(X) \in \mathbb{Z}[X]$  primitivo. Se sigue que:

$$f(X) = \alpha_1 \alpha_2 f_1(X) f_2(X),$$

y el producto  $f_1(X)f_2(X)$  es primitivo por el lema de Gauss. Entonces, por el lema anterior,  $f(X)$  y  $f_1(X)f_2(X)$  se diferencian en el producto por una unidad de  $\mathbb{Z}$ . Esto obliga a que  $f_1(X)$  sea unidad en  $\mathbb{Z}[X]$ , esto es,  $f_1(X)$  es una unidad de  $\mathbb{Z}$ .

Recíprocamente, sea  $f(X) \in \mathbb{Z}[X]$  primitivo e irreducible en  $\mathbb{Q}[X]$ . Si se tiene que  $f(X) = g(X)h(X)$ , con  $g(X)$ ,  $h(X) \in \mathbb{Z}[X]$ , y  $h(X)$  de grado positivo, entonces  $g(X)$  tiene grado cero (una descomposición en  $\mathbb{Z}[X]$  lo es también en  $\mathbb{Q}[X]$ ). Como  $1 = c(f(X)) = g \cdot c(h(X))$ , se sigue que  $g$  es, además, unidad de  $\mathbb{Z}$ .  $\square$

### 3. APLICACIÓN DEL TEOREMA FUNDAMENTAL DEL ÁLGEBRA

Este teorema garantiza la existencia de soluciones en el cuerpo de los números complejos de toda ecuación polinómica compleja. Fue enunciado por D'Alembert, pero demostrado por Gauss. Damos una demostración simple, basada en resultados de Análisis. Para una demostración totalmente algebraica, hay que utilizar la teoría de Galois.

► **Lema 3.1.**

Si  $f : D \rightarrow \mathbb{R}$  es una función continua, y  $D$  es un conjunto cerrado y acotado (compacto) de  $\mathbb{R}^2$ , entonces  $f$  tiene un mínimo y un máximo en  $D$ .

► **Lema 3.2.**

Sea  $f(X) \in \mathbb{C}[X]$ . Entonces la función  $|f(x)|$  alcanza un valor mínimo en algún  $z_0 \in \mathbb{C}$ .

*Demostración.*

Es inmediato ver que  $\lim_{|x| \rightarrow +\infty} |f(x)| = +\infty$ . Por tanto, como  $|f(x)|$  se hace grande cuando  $|x|$  crece, se deduce que la cota inferior de  $|f(z)|$  para  $z \in \mathbb{C}$  es también la cota inferior en un disco suficientemente grande  $|z| \leq r$ . Como  $|f(x)|$  es una función continua con valores en  $\mathbb{R}$ , por el lema anterior tenemos que  $|f(z)|$  alcanza su valor mínimo en el disco.  $\square$

► **Lema 3.3.**

Sea  $f(X) \in \mathbb{C}[X]$  con la función  $f(x)$  no constante. Si  $f(x_0) \neq 0$  entonces  $|f(x_0)|$  no es el valor mínimo de  $|f(x)|$ .

*Demostración.*

Sea  $f(X) \in \mathbb{C}[X]$  no constante, y supongamos que  $x_0$  es un punto con  $f(x_0) \neq 0$ . Hagamos el cambio de variables  $x+x_0$  por  $x$ . Con esto se mueve  $x_0$  al origen, y podemos suponer  $f(0) \neq 0$ . Multiplicamos  $f(x)$  por  $f(0)^{-1}$ , y conseguimos  $f(0) = 1$ . Vamos a probar que 1 no es el valor mínimo de  $|f(x)|$ .

Sea  $k$  el exponente más pequeño de  $x$  que aparece en  $f(x)$ . Entonces:

$$f(x) = 1 + ax^k + \text{términos de grado } > k.$$

Ahora sea  $a$  una raíz  $k$ -ésima de  $-a^{-1}$ , que existe por la fórmula de DeMoivre. Hacemos ahora el cambio de variable  $ax$  por  $x$ . Entonces  $f(x)$  tiene la forma:

$$f(x) = 1 - x^k + x^{k+1}g(x) \text{ para algún polinomio } g(x).$$

Sea  $\epsilon < 1$  un número real y positivo. Entonces:

$$|f(\epsilon)| \leq |1 - \epsilon^k| + \epsilon^{k+1} |g(\epsilon)|.$$

Como  $\epsilon^k < 1$ , podemos escribir:

$$|f(\epsilon)| \leq 1 - \epsilon^k + \epsilon^{k+1} |g(\epsilon)| = 1 - \epsilon^k(1 - \epsilon |g(\epsilon)|).$$

Si  $\epsilon \rightarrow 0$  entonces  $\epsilon |g(\epsilon)| \rightarrow 0$ , por lo que podemos escoger  $x_0 < 1$  real y positivo tal que  $x_0 |g(x_0)| < 1$ . Entonces:

$$x_0^k (1 - x_0 |g(x_0)|) > 0$$

y  $|f(x_0)| < 1 = |f(0)|$ . □

► **Teorema 3.4. Teorema fundamental del Álgebra.**

Si  $f(X) \in \mathbb{C}[X]$  es un polinomio no constante, entonces tiene al menos una raíz compleja.

*Demostración.*

Sea  $f(X)$  un polinomio no constante. Entonces la función  $|f(x)|$  tiene un valor mínimo en algún  $x_0 \in \mathbb{C}$ . Por el lema anterior,  $|f(x_0)| = 0$ , de donde  $f(x_0) = 0$ . □

*Nota 3.5.*

Dados dos cuerpos  $k \subset K$  (como  $\mathbb{Q} \subset \mathbb{R}$  o  $\mathbb{R} \subset \mathbb{C}$ ) se dice que  $\alpha \in K$  es *algebraico sobre*  $k$  si existe un  $f(X) \in k[X]$  tal que  $f(\alpha) = 0$ . Así  $\sqrt{2} \in \mathbb{R}$  es algebraico sobre  $\mathbb{Q}$  porque es raíz de  $X^2 - 2 \in \mathbb{Q}[X]$ . Si un número no es algebraico se dice *trascendente*. Las pruebas de que  $\pi$  o  $e$  son trascendentes sobre  $\mathbb{Q}$  están basadas, como la del teorema fundamental del Álgebra que hemos presentado, en el Análisis.

Un cuerpo  $k$  se dice *algebraicamente cerrado* si todo polinomio (no constante) en  $k[X]$  tiene una raíz en  $K$ . El teorema fundamental del Álgebra puede enunciarse diciendo que  $\mathbb{C}$  es algebraicamente cerrado.

## 4. CRITERIOS DE IRREDUCIBILIDAD DE POLINOMIOS

Veamos algunos criterios para detectar la irreducibilidad de un polinomio sobre los reales y los racionales.

### 4.1. POLINOMIOS IRREDUCIBLES EN $\mathbb{R}[X]$

A partir del teorema fundamental del Álgebra, podemos determinar los polinomios irreducibles de  $\mathbb{R}[X]$  como una aplicación del teorema de división. Será clave utilizar que si  $\alpha \in \mathbb{C}$  es raíz de un polinomio en  $\mathbb{R}[X]$ , también lo es  $\bar{\alpha}$ .

► **Teorema 4.1.** Si  $f(X)$  es un polinomio irreducible con coeficientes reales, entonces:

- $f(X)$  tiene grado 1, o bien
- $f(X) = aX^2 + bX + c$  con  $b^2 - 4ac < 0$ .

Recíprocamente, estos dos tipos de polinomio son irreducibles.

*Demostración.*

Es claro que un polinomio de grado 1 es irreducible. Supongamos que:

$$f(X) = aX^2 + bX + c,$$

y que factoriza en  $\mathbb{C}[X]$  como:

$$f(X) = a \left( X + \frac{b}{2a} + \frac{1}{2a} \sqrt{b^2 - 4ac} \right) \left( X + \frac{b}{2a} - \frac{1}{2a} \sqrt{b^2 - 4ac} \right).$$

Si  $b^2 - 4ac < 0$  entonces estas raíces de  $f(X)$  no son reales, y como  $f(X)$  no puede tener más raíces, es irreducible. Así que estos tipos de polinomios reales son, en efecto, irreducibles.

Supongamos ahora que  $f(X)$  es un polinomio real irreducible de grado mayor que 1. Entonces no tiene raíces reales. Sea  $\alpha$  una raíz compleja no real de  $f(X)$ . Entonces su conjugada  $\bar{\alpha}$  también es raíz, y si escribimos  $\alpha = r_1 + ir_2$  tenemos que:

$$\begin{aligned} g(X) &= (X - \alpha)(X - \bar{\alpha}) = (X - (r_1 + ir_2))(X - (r_1 - ir_2)) \\ &= X^2 - 2r_1X + (r_1^2 + r_2^2) \end{aligned}$$

es un polinomio de coeficientes reales. Aplicamos el teorema de división con  $f(X)$  y  $g(X)$ , y obtenemos:

$$f(X) = q(X)g(X) + r(X), \text{ donde } q(X), r(X) \in \mathbb{R}[X],$$

y  $r(X)$  es de grado menor o igual que 1. Si sustituimos el valor  $\alpha$  en la igualdad, nos queda:

$$0 = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha).$$

Como  $g(\alpha) = 0$ , llegamos a  $r(\alpha) = 0$ . Si  $r(X) = cX + d$ , con  $c, d \in \mathbb{R}$ , entonces  $c\alpha + d = 0$ . Como  $\alpha$  no es real, tiene que ser  $c = 0$ , de donde  $d = 0$ , y concluimos que  $f(X) = q(X)g(X)$ . Esto significa que  $f(X)$  no es irreducible, salvo que  $q(X)$  fuera una constante. Si lo es, entonces  $f(X)$  es un polinomio de grado 2 sin raíces reales, como establecíamos en el enunciado.  $\square$

#### 4.2. CRITERIOS DE IRREDUCIBILIDAD EN $\mathbb{Q}[X]$

Dado un polinomio con coeficientes enteros, por el siguiente criterio sabemos cuáles son sus posibles raíces racionales:

► **Teorema 4.2** (Teorema de la raíz racional de Descartes).

Sea:

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$

un polinomio de grado  $n$  con coeficientes racionales. Si  $\frac{r}{s}$  es una fracción reducida que es raíz de  $p(X)$ , entonces  $r$  divide al término constante  $a_0$ , y  $s$  divide al término líder  $a_n$ .

*Demostración.*

Por hipótesis:

$$p\left(\frac{r}{s}\right) = 0 = a_n \frac{r^n}{s^n} + a_{n-1} \frac{r^{n-1}}{s^{n-1}} + \dots + a_1 \frac{r}{s} + a_0.$$

Si multiplicamos por  $s^n$  ambos lados de la igualdad, tenemos:

$$0 = a_n r^n + a_{n-1} r^{n-1} s + \dots + a_1 r s^{n-1} + a_0 s^n.$$

Entonces  $-a_n r^n = s(a_{n-1} r^{n-1} + \dots + a_1 r s^{n-2} + a_0 s^{n-1})$ , por lo que  $s$  divide a  $a_n r^n$ . Por hipótesis,  $s$  es primo con  $r$ , por lo que  $s$  tiene que dividir a  $a_n$ . Análogamente,  $-a_0 s^n = r(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + \dots + a_1 s^{n-1})$ , de donde  $r$  divide a  $a_0$ .  $\square$

Este criterio está limitado a polinomios de grado bajo, porque busca un factor de grado 1. Un polinomio de grado 4, por ejemplo, puede factorizar en dos polinomios irreducibles de grado 2, por lo que no tendría factores lineales.

► **Ejemplo 4.3.**

Para encontrar las raíces racionales de:

$$f(X) = X^4 + 5X^3 - 9X^2 - 14X + 24,$$

tenemos que probar con  $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm 24$ .

► **Teorema 4.4** (Criterio de Eisenstein).

Si  $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  es un polinomio con coeficientes en  $\mathbb{Z}$ , y existe un primo  $p$  que no divide a  $a_n$  pero sí divide a  $a_{n-1}, a_{n-2}, \dots, a_1, a_0$ , pero  $p^2$  no divide a  $a_0$ , entonces  $f(X)$  es irreducible en  $\mathbb{Z}[X]$  (y por tanto en  $\mathbb{Q}[X]$ ).

*Demostración.*

Supongamos que:

$$f(X) = g(X)h(X)$$

en  $\mathbb{Z}[X]$ , donde  $g(X) = b_r X^r + \dots + b_1 X + b_0$ ,  $h(X) = c_s X^s + \dots + c_1 X + c_0$ , y sin pérdida de generalidad podemos asumir que  $r \leq s$ . Igualamos los coeficientes de  $f(X)$  con los del producto de los polinomios  $g(X)$  y  $h(X)$ , y obtenemos  $n + 1$  ecuaciones:

$$\begin{aligned} a_n &= b_r c_s, \\ &\vdots \\ a_s &= b_r c_{s-r} + b_{r-1} c_{s-r+1} + \dots + b_0 c_s, \\ &\vdots \\ a_r &= b_r c_0 + b_{r-1} c_1 + \dots + b_0 c_r, \\ &\vdots \\ a_3 &= b_3 c_0 + b_2 c_1 + b_1 c_2 + b_0 c_3, \\ a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2, \\ a_1 &= b_1 c_0 + b_0 c_1, \\ a_0 &= b_0 c_0. \end{aligned}$$

Como  $p^2$  no divide a  $a_0$ , pero  $p$  sí lo hace, entonces  $p$  divide a  $b_0$  o a  $c_0$ , pero no a los dos a la vez. Supongamos que  $p$  divide a  $b_0$  pero no a  $c_0$ . Como  $p$  divide a  $a_1, a_2, \dots, a_r$ , pero no a  $c_0$ , se deduce que  $p$  divide a  $b_1$ , a  $b_2$ , hasta  $b_r$ . Pero entonces  $p$  divide a  $a_n$ , que es contrario a la hipótesis. Análogamente se trata el caso en que  $p$  divide a  $c_0$  pero no a  $b_0$ . En consecuencia, la factorización inicial no puede existir.  $\square$

► **Ejemplo 4.5.**

Sea  $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}[X]$ , con  $p$  primo. Con el polinomio en esta forma no podemos aplicar el criterio de Eisenstein, pero vamos a hacer un cambio de variable. Sea  $g(X) = \Phi_p(X + 1)$ . Observemos en primer lugar que  $\Phi_p(X) = \frac{X^p - 1}{X - 1}$ , de donde:

$$\begin{aligned} g(X) &= \frac{(X+1)^p - 1}{X+1-1} = \frac{1}{X} ((X+1)^p - 1) \\ &= \frac{1}{X} \left( X^p + \binom{p}{1} X^{p-1} + \binom{p}{2} X^{p-2} + \dots + \binom{p}{k} X^{p-k} + \dots + pX + 1 - 1 \right) \\ &= X^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} X^{p-k-1} \\ &= X^{p-1} + a_{p-2} X^{p-2} + \dots + a_1 X + a_0. \end{aligned}$$

Entonces  $p$  divide a cada  $a_i$ ,  $i = 0, 1, \dots, p - 2$ , y  $a_0 = p$ . Por el criterio de Eisenstein, el polinomio  $g(X)$  es irreducible, y por tanto también  $\Phi_p(X)$ .

Una técnica para detectar la irreducibilidad es trabajar módulo  $n$ . Si  $f(X)$  es un polinomio con coeficientes enteros y primitivo, podemos reducir módulo  $n$  y obtener un polinomio no nulo  $\bar{f}(X)$  en  $\mathbb{Z}_n[X]$ . Si  $n$  es un entero primo con el coeficiente líder de  $f(X)$ , entonces  $\bar{f}(X)$  es un polinomio del mismo grado que  $f(X)$ . Supongamos que  $f(X) = a(X)b(X)$ , donde  $a(X)$  y  $b(X)$  tienen coeficientes enteros y son primitivos. Entonces  $\bar{f}(X) = \bar{a}(X)\bar{b}(X)$  en  $\mathbb{Z}_n[x]$ , y  $\bar{f}(X)$  sería reducible. En otras palabras:

► **Corolario 4.6.**

Si  $\bar{f}(X) \in \mathbb{Z}_n[X]$  es irreducible para algún  $n$  que no divida al término líder de  $f(X)$ , entonces  $f(X)$  es irreducible en  $\mathbb{Q}[X]$ .

Esta técnica también tiene sus limitaciones. Por ejemplo, el polinomio  $X^4 + 1$  es irreducible en  $\mathbb{Z}[X]$ , pero es reducible módulo cualquier primo, y el polinomio  $X^4 - 10X^2 + 17$  es irreducible en  $\mathbb{Z}[X]$ , pero es reducible módulo cualquier entero.

## CONCLUSIÓN

El lenguaje algebraico se introduce en el primer curso de la ESO, con monomios y polinomios muy sencillos, ampliándose estos conceptos curso a curso hasta llegar a 1º de Bachillerato.

Sus aplicaciones dentro de las Matemáticas son muy numerosas: resolución de problemas mediante ecuaciones y sistemas, cálculos geométricos mediante fórmulas polinómicas, sucesiones y progresiones, etc.

Estos dos motivos son los fundamentales para señalar la importancia del tema para un Profesor de Enseñanza Secundaria de la especialidad de Matemáticas.



# BIBLIOGRAFÍA

## BIBLIOGRAFÍA COMENTADA

---

ADKINS, W. A. Y WEINTRAUB, S. H. (1992): *Algebra*. New York: Springer-Verlag.

El capítulo 2 contiene un tratamiento general de anillos de polinomios. Es un texto algo avanzado.

CHILDS, L. N. (2009): *A concrete introduction to higher algebra*. New York: Springer.

Trata con profundidad los polinomios, llegando incluso a los algoritmos de factorización sobre  $\mathbb{Q}[X]$  y cuerpos finitos.

DUMMIT, D.S. Y FOOTE, R. M. (2004): *Abstract algebra*. Hoboken, NJ: John Wiley & Sons Inc.

Dedica el capítulo 9 a anillos de polinomios, con todo el contenido del tema. Como en cada capítulo, propone un gran número de ejercicios.

GAMBOA MUTUBERRÍA, J. M. Y RUIZ SANCHO, J. M. (2002): *Anillos y cuerpos conmutativos*. Madrid: UNED.

El libro presenta, con gran detalle, las nociones y resultados básicos sobre anillos y cuerpos conmutativos, poniendo especial énfasis en la resolución de algunas cuestiones fundamentales acerca de polinomios en una y varias variables.



## AUTOEVALUACIÓN

1. Encontrar  $\text{mcd}(3X^3 + 4X^2 + 3, 3X^3 + 4X^2 + 3X + 4)$  en  $\mathbb{Z}/\mathbb{Z}5[X]$ .

**SOLUCIÓN:** Tenemos, usando el algoritmo de Euclides, las siguientes divisiones:

$$\begin{aligned} 3x^3 + 4X^2 + 3 &= (1)(3X^3 + 4X^2 + 3X + 4) + (2X + 4), \\ 3X^3 + 4X^2 + 3X + 4 &= (4X^2 + 4X)(2X + 4) + 0. \end{aligned}$$

Así, un  $\text{mcd}(3X^3 + 4X^2 + 3, 3X^3 + 4X^2 + 3X + 4)$  en  $\mathbb{Z}/\mathbb{Z}5[X]$  es  $2X + 4$ .

2. Factorizar  $X^7 - X$  en  $\mathbb{Z}/\mathbb{Z}7[X]$ .

**SOLUCIÓN:** Sabemos, por el pequeño teorema de Fermat que todo  $a \in \mathbb{Z}$  primo con 7 verifica  $a^7 = a$  módulo 7, por tanto

$$X^7 - X = X(X-1)(X-2)(X-3)(X-4)(X-5)(X-6).$$

3. Probar que  $X^4 - 2X^2 + 8X + 1$  es irreducible en  $\mathbb{Q}[X]$ .

**SOLUCIÓN:** Ninguno de los divisores del término independiente es raíz del polinomio. Luego no tiene factores lineales. La única posible factorización es en dos polinomios de grado 2, de tipo

$$(X^2 + aX + b)(X^2 + cX + d).$$

Igualando los coeficientes de este producto a los de nuestro polinomio obtenemos el sistema

$$\begin{aligned} bd &= 1 \\ ad + bc &= 8 \\ ac + b + d &= -2 \\ a + c &= 0, \end{aligned}$$

que podemos considerar en  $\mathbb{Z}$  por el lema de Gauss. En cualquier caso, el sistema es incompatible.

4. Probar que, para  $1 < b \in \mathbb{Z}$  el polinomio  $X^n - b$  es irreducible en  $\mathbb{Q}$  si en la descomposición de  $b$  en factores primos, ninguno aparece al cuadrado.

**SOLUCIÓN:** Es una aplicación inmediata del criterio de Eisenstein: cualquier  $p$  primo que divida a  $b$  cumple que  $p^2 \nmid b$ .

5. Demostrar que  $f(X) = 3X^4 + 6X^3 + 12X^2 + 13X + 31$  es irreducible en  $\mathbb{Q}[X]$ .

**SOLUCIÓN:** Trabajemos módulo un número primo con 3 (módulo 3 no sirve porque se anula el coeficiente líder). Con los coeficientes módulo 2 obtenemos

$$X^4 + X + 1$$

que es irreducible en  $\mathbb{Z}/\mathbb{Z}2$ . Por tanto lo es en  $\mathbb{Q}[X]$ .

