Polinomios

Pablo De Nápoli

versión 0.8.6

Resumen

Este es un apunte de las teóricas de álgebra I, del primer cuatrimestre de 2007, turno noche, con algunas modificaciones introducidas en 2014.

1. Introducción

Históricamente el álgebra surgió del estudio de las ecuaciones algebraicas. Por ejemplo, consideramos la ecuación

$$X^2 = 5X - 6$$

donde X es un número desconocido que queremos determinar ("una indeterminada"). Una estrategia para resolverla, consiste en pasar de término todos los términos a un mismo miembro de la igualdad, para obtener una ecuación igualada a cero:

$$X^2 - 5X + 6 = 0$$

Esta es una ecuación cuadrática de las que se estudian en la escuela secundaria. Una expresión tal como la que aparece en el primer miembro de esta ecuación:

$$P(X) := X^2 - 5X + 6$$

que se obtiene sumando potencias no negativas de X multiplicadas por números, se denomina un **polinomio** en la indeterminada X. Resolver la

ecuación consiste entonces en determinar los **ceros** o **raíces** del polinomio, es decir aquellos valores de X para los cuales el polinomio se anula.

Entonces la estrategia consiste en tratar de **factorizar** el polinomio, esto es expresarlo como producto de polinomios de grado más pequeño. En este caso, esto puede usarse utilizando la técnica de "completar el cuadrado":

$$P(X) = \left(X - \frac{5}{2}\right)^2 - \frac{25}{4} + 6 = 0$$

Utilizando entonces la factorización de una "diferencia de cuadrados"

$$a^2 - b^2 = (a - b)(a + b)$$

obtenemos:

$$P(X) = \left(X - \frac{5}{2}\right)^2 - \frac{1}{4} = 0$$

$$P(X) = \left(X - \frac{5}{2} - \frac{1}{2}\right)\left(X - \frac{5}{2} + \frac{1}{2}\right)$$

o

$$P(X) = (X - 2)(X - 3)$$

Como para que el producto de dos números sea cero alguno de los dos debe ser cero, deducimos que el polinomio se anulará exactamente cuando $X = 2$ o cuando $X = 3$. Estas son pues, los ceros o raíces del polinomio P.

Así pues, vemos que existe una importante conección entre el problema de encontrar los ceros o raíces de un polinomio, y el problema de factorizarlo. Exploraremos esta conección más en detalle en lo sucesivo.

1.1. Las estructuras algebraicas de anillo y de cuerpo

Nuestro primer objetivo será dar una definición formal del concepto de polinomio.

Consideraremos en lo sucesivo polinomios de distintos tipos, como por ejemplo con coeficientes enteros como

$$3X^3 - 5X^2 + 10X - 2$$

con coeficientes racionales como

$$\frac{3}{2}X^2 - \frac{5}{2}X + 10$$

con coeficientes reales taales como

$$\frac{X^2}{2} - \frac{\sqrt{2}}{2}X + \pi$$

o con coeficientes complejos tales como

$$(2+i)X^2 - (3-i)X + 1$$

Para poder tratar todos estos casos de una manera unificada, necesitaremos introducir la estructura algebraica de anillo. Informalmente, un anillo es un conjunto A en el que están definidas de alguna manera las operaciones de suma, resta, producto y multiplicación. Veamos una definición formal:

Definición 1.1 *Un anillo es un conjunto A donde están definidas dos operaciones* [1]

$$+ : A \times A \to A$$

$$\cdot : A \times A \to A$$

de modo que se verifiquen las siguientes propieades (axiomas de la estructura de anillo):

1. *Propiedad Asociativa de la suma:*

$$(a+b)+c = a+(b+c) \ \forall \ a,b,c \in A$$

2. *Propiedad Conmutativa de la suma*

$$a+b = b+a \ \forall \ a,b \in A$$

[1] Una operación tal como la suma $+$, en un conjunto A, no es otra cosa que una función $+ : A \times A \to A$. Por convención, escribiremos

$$a+b$$

en lugar de $+(a,b)$. Similarmente, escribiremos

$$a \cdot b$$

en lugar de $\cdot(a,b)$.

3. *Existencia de neutro para la suma Existe un elemento* $0 \in A$*, tal que:*

$$a + 0 = 0 + a = a \; \forall \; a \in A$$

4. *Existencia de inversos aditivos Para todo* $a \in A$*, existe un elemento* $-a \in A$*, tal que:*

$$a + (-a) = (-a) + a = 0$$

Notamos que en cualquier anillo se puede definir la operación de resta $a - b$ *especificando que:*

$$a - b = a + (-b)$$

5. *Propiedad asociativa del producto*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \; \forall \; a, b, c \in A$$

6. *Existencia de elemento neutro para el producto Existe un elemento* $1 \in A$ *tal que*

$$a \cdot 1 = 1 \cdot a = a$$

7. *Propiedad Distributiva*

$$a \cdot (b + c) = a \cdot b + a \cdot c \; \forall \; a, b, c \in A$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \; \forall \; a, b, c \in A$$

Si además se verifica que:

$$a \cdot b = b \cdot a \; \forall a, b \in A$$

diremos que A *es un* **anillo conmutativo**. *Todos los ejemplos de anillos con los que trabajaremos en lo sucesivo serán conmutativos, razón por la cuál omitiremos mencionarlo explícitamente*[2].

Son ejemplos de anillos (conmutativos): $\mathbb{Z}$ (los enteros), $\mathbb{Q}$ (los números racionales), $\mathbb{R}$ los números reales, $\mathbb{C}$ (los números complejos) y $\mathbb{Z}_n$ (las clases de enteros módulo n).

En algunos casos, necesitaremos una propiedad que no está incluida en la definición de anillo:

[2]Existen ejemplos de anillos que no son comutativos, como las matrices de $n \times n$ con coeficientes reales, pero no trabajaremos con ellos en este curso.

Definición 1.2 *Un anillo conmutativo A se dice un* **dominio íntegro** *si*

$$ab = 0 \text{ si y sólo si } a = 0 \text{ o } b = 0$$

Por ejemplo $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios íntegros (en cambio $\mathbb{Z}_n$ sólo lo es cuando n es primo).

Más adelante, consideraremos otra clase especial de anillos: los cuerpos. Estos son los anillos conmutativos en los que es posible la división.

Definición 1.3 *Un anillo conmutativo A es un* **cuerpo** *si cada elemento $a \in A$ con $a \neq 0$, tiene un inverso multiplicativo a^{-1} tal que:*

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

En tal caso, podemos definir la división $a : b$ con $b \neq 0$ en A, especificando que:

$$a : b = a \cdot b^{-1}$$

Por ejemplo: $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son ejemplos de cuerpos. En cambio, $\mathbb{Z}$ no es un cuerpo. $\mathbb{Z}_n$ es un cuerpo si y sólo si n es primo.

Observamos que todo cuerpo es un dominio íntegro, pero la afirmación recíproca no es cierta ($\mathbb{Z}$ es un ejemplo de un dominio íntegro que no es un cuerpo).

2. La definición formal de polinomio

Definición 2.1 *Sea A un anillo conmutativo. Un polinomio en una indeterminada X con coeficientes en el anillo A es una expresión formal de la forma:*

$$P = \sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_2 X^2 + a_1 X + a_0$$

donde los a_i son elementos de A (se llaman **coeficientes***) del polinomio P*

Si $a_n \neq 0$ diremos que P es un polinomio de **grado** *n, y diremos que a_n es el coeficiente principal de P. Notamos $gr(P)$ al grado de P.*

Si $a_n = 1$ diremos que P es un polinomio **mónico**.

Notamos $A[X]$ al conjunto de todos los posibles polinomios en la indeterminada X con coeficientes en el anillo A.

Ejemplos: Algunos ejemplos de polinomios que dimos anteriormente:

$$3X^3 - 5X^2 + 10X - 2 \in \mathbb{Z}[X]$$

$$\frac{3}{2}X^2 - \frac{5}{2}X + 10 \in \mathbb{Q}[X]$$

$$\frac{X^2}{2} - \frac{\sqrt{2}}{2}X + \pi \in \mathbb{R}[X]$$

$$(2+i)X^2 - (3-i)X + 1 \in \mathbb{C}[X]$$

Naturalmente,

$$\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$$

2.1. Igualdad de polinomios

Convenimos en decir que dos polinomos:

$$P = \sum_{i=0}^{n} a_i \, X^i$$

$$Q = \sum_{i=0}^{m} b_i \, X^j$$

son iguales si $a_i = b_i$ para $0 \leq i \leq \text{mín}(n, m)$ y si $a_i = 0$ para $i = m+1, m+2, \ldots, n$ en el caso que $n > m$, o si $b_i = 0$ para $i = n+1, n+2, \ldots, m$ cuando $n < m$.

Dicho de otro modo, consideramos iguales a dos polinomios si tienen igual grado y los mismos coeficientes, pero consideraremos iguales a polinomios que difieren en términos con coeficientes nulos, como:

$$P = 0X^3 + 3X^2 + 2X + 1$$

y

$$Q = 3X^2 + 2X + 1$$

Un polinomio particularmente importante es el **polinomio nulo**, que corresponde a tomar todos los coeficiente a_i como cero (Conforme a nuestro convenio sobre la igualdad de polinomios, existe un único polinomio nulo en $A[X]$). Notemos que la noción de grado no está definida para el polinomio nulo.

Otros polinomios importantes, son los polinomios constantes, de la forma a_0X^0 donde $a_0 \in A$ (o sea $a_i = 0$ si $i > 0$). Son precisamente los polinomios de grado cero, si $a_0 \neq 0$. Si identificamos el elemento $a_0 \in A$ con el polinomio constante $a_0X^0 \in A[X]$, podemos pensar que:

$$A \subset A[X]$$

Para comprender mejor el significado de la definición formal de polinomio, es conveniente mencionar que para representar un polinomio en una computadora se utiliza con frecuencia un vector conteniendo sus coeficientes.

2.2. Evaluación de polinomios

Un hecho fundamental sobre los polinomios es que se pueden **especializar** o **evaluar**. Más específicamente si $P \in A[X]$, y $b \in A$, definimos

$$P(b) = \sum_{i=0}^{n} a_i \cdot b^i$$

como el elemento de A que se obtiene si reemplazamos la indeterminada X por el elemento b y efectuamos el cálculo expresado por el polinomio utilizando las operaciones del anillo b. Claramente, $P(b) \in A$.

Ejemplo: Si $P = 3X^2 + 2X + 1 \in \mathbb{Z}[X]$ y $b = 2$, entonces $P(2) = 3 \cdot 2^2 + 2 \cdot 2^2 + 1 = 21$.

Por medio de la evaluación, cada polinomio $P \in A[X]$ origina una función (función polinómica definida por P) de A en A. La notaremos f_P.

$$f_P : A \to A \quad f_P(a) = P(a)$$

En general, es necesario distinguir entre el polinomio como expresión formal, y la función polinómica que origina. Por ejemplo si $A = \mathbb{Z}_p$ con p primo, el polinomio $P = X^p - X$ da origen la la función nula (por el teorema de Fermat), o sea:

$$f_P(a) = 0 \ \forall a \in \mathbb{Z}_p$$

al igual que el polinomio nulo, a pesar de que P no es el polinomio nulo.

Si embargo cuando A es un cuerpo infinito (por ejemplo $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$), probaremos más adelante que si dos polinomios originan la misma función polinómica deben ser iguales.

3. Suma y resta de polinomios

Para definir la suma (o la resta) de polinomios se procede a sumar (respectivamente, restar) los términos correspondientes a la misma potencia de X.

Ejemplo: Si $P = 3X^2 + X + 1$ y $Q = 3X - 2$ entonces

$$P - Q = (3 + 0)X^2 + (1 + 3)X + (1 - 2) = 3X^2 + 4X - 1$$

y

$$P - Q = (3 - 0)X^2 + (1 - 3)X + (1 + 2) = 3X^2 - 2X + 3$$

Esto origina la siguiente definición formal:

Definición 3.1 *Si P y Q son dos polinomios:*

$$P = \sum_{i=0}^{m} a_i X^i$$

$$Q = \sum_{i=0}^{n} b_i X^i$$

Definimos la suma de polinomios $P + Q$ por:

$$(P + Q) = \sum_{i=0}^{\text{máx}(n,n)} (a_i + b_i) X^i$$

donde en concordancia con la definición de igualdad de polinomios, convenimos en que

$$a_i = 0 \text{ si } i > m \text{ cuando } m < n$$

y

$$b_i = 0 \text{ si } i > n \text{ cuando } n < m$$

Análogamente, podemos definir la resta de polinomios $P - Q$ por:

$$(P - Q) = \sum_{i=0}^{\text{máx}(n,m)} (a_i - b_i)X^i$$

con idéntico convenio.

Notamos que las definiciones de estas operaciones están hechas de tal manera que se verifique que:

$$(P + Q)(b) = P(b) + Q(b)$$

$$(P - Q)(b) = P(b) - Q(b)$$

Así mismo, otra consecuencia inmediata de esta definición es que el grado de la suma o resta de dos polinomios es menor o igual que el máximo de los grados de P y Q.

$$\text{gr}(P \pm Q) \leq \text{máx}(\text{gr}(P), \text{gr}(Q))$$

Esta desigualdad puede sin embargo ser estricta, como muestra el ejemplo siguiente:

Ejemplo: Sean (en $\mathbb{Z}[X]$) $P = X^2 + 3X - 1$ y $Q = -X^2 + 2$. Entonces $P + Q = 3X + 1$ que tiene grado 1, mientras que P y Q tienen ambos grado 2.

Notamos que el polinomio nulo 0, actúa como el elemento neutro de la suma de polinomios:

$$P + 0 = 0 + P = P \ \forall \ P \in A[X]$$

4. Producto de polinomios

Para efectuar un producto de polinomios tal como

$$(X - 2)(X - 3)$$

debemos "efectuar la distributiva"

$$X^2 - 2X - 3X + 2 \cdot 3$$

para después sumar los términos en los que aparece la misma potencia de X:

$$X^2 - (2+3)X + 2 \cdot 3 = X^2 - 5X + 6$$

Esto conduce a la siguiente definción formal:

Definición 4.1 *Si*

$$P = \sum_{i=0}^{n} a_i X^i$$

$$Q = \sum_{j=0}^{n} b_j X^j$$

definimos el polinomio producto $P \cdot Q$ por

$$P \cdot Q = \sum_{k=0}^{n+m} \left(\sum_{i,j:i+j=k} a_i b_j \right) X^k$$

Nuevamente esta definición está hecha, para que sea consistente con la evaluación de polinomios, es decir para que se verifique que:

$$(P \cdot Q)(b) = P(b) \cdot Q(b) \; \forall \; b \in A$$

Dado que hemos definido las operaciones de suma, resta y producto de polinomios, el conjunto de polinomios $A[X]$ con coeficientes en el anillo A, resulta así mismo tener estructa de anillo.

Una consecuencia inmediata de la definición del producto $P \cdot Q$, es que el coeficiente principal de $P \cdot Q$ es el producto del coeficiente principal de P por el de Q.

En particular, si el anillo A es un dominio íntegro (ver definición 1.2, cosa que se cumple en los ejemplos usuales $K = \mathbb{Q}$, $K = \mathbb{R}$ o $K = \mathbb{C}$), se deduce que

$$P \cdot Q = 0 \text{ si y sólo si } P = 0 \text{ o } Q = 0$$

(es decir que $A[X]$ resulta a su vez un dominio íntegro) y que:

$$\text{gr}(PQ) = \text{gr}(P) + \text{gr}(Q)$$

5. Raíces de un polinomio

Por razones técnicas, que pronto serán claras, haremos la hipótesis de que el anillo de coeficientes A es un cuerpo, y lo notaremos en adelante, por la letra$K$ (podemos pensar $K = \mathbb{Q}$, $K = \mathbb{R}$ o $K = \mathbb{C}$, los cuerpos que conocemos).

Definición 5.1 *Si $P \in K[X]$ es un polinomio y $b \in K$, diremos que b es un* **cero** *o una* **raíz** *de P si $P(b) = 0$.*

Observación: Un polinomio de grado 1, $aX + b$ siempre tiene una única raíz $\frac{-b}{a}$.

Ejemplo: Si la ecuación de segundo grado:

$$P(X) = aX^2 + bX + c \text{ con } a \neq 0 \ (a, b, c \in K)$$

desde la escuela secundaria, conocemos una fórmula para determinar sus raíces. Dicha fórmula puede demostrarse utilizando el procedimiento de "completar el cuadrado" (generalizando lo que hicimos en la introducción) y es válida en cualquier cuerpo [3]:

Primero sacamos a como factor común:

$$P = a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right)$$

$$P = a\left[\left(X^2 + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + \frac{c}{a}\right]$$

o sea:

$$P = a\left[\left(X^2 + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a}\right]$$

El número $\Delta = b^2 - 4ac$ se denomina el **discriminante** de el polinómio cuadrático P. Si Δ tiene una raíz cuadrada en K, es decir si existe un elemento $\sqrt{\Delta} \in K$ que resuelva la ecuación

$$X^2 = \Delta$$

[3] Siempre que $1 + 1 \neq 0$ en K, lo que ocurre si $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, pero no por ejemplo si $K = \mathbb{Z}_2$

(lo que ocurre en los números reales si $\Delta \geq 0$, y siempre en los números complejos) entonces, podemos escribir P como una diferencia de cuadrados:

$$P = a\left[\left(X^2 + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{\Delta}}{2a}\right)^2\right]$$

y factorizarlo como:

$$P = a\left(X^2 + \frac{b}{2a} - \frac{\sqrt{\Delta}}{2a}\right)\left(X^2 + \frac{b}{2a} + \frac{\sqrt{\Delta}}{2a}\right)$$

O sea:

$$P = a(X - \alpha_1)(X - \alpha_2)$$

siendo

$$\alpha_1 = \frac{-b + \sqrt{\Delta}}{2a}$$

y

$$\alpha_2 = \frac{-b - \sqrt{\Delta}}{2a}$$

Deducimos que P se anula exactamente cuando $X = \alpha_1$ o cuando $X = \alpha_2$, es decir que α_1 y α_2 son exactamente las raíces de P.

Resumiendo nuestra discusión: vemos que un polinomio de segundo grado tiene exactamente dos raíces, siempre que sea posible "extraer la raíz cuadrada" de su discriminante $\Delta = b^2 - 4ac$ en K; en particular, esto sucederá siempre cuando $K = \mathbb{C}$, y si $\Delta \geq 0$ cuando $K = \mathbb{R}$.

La denominación "raíz" ha quedado por razones históricas, porque los matemáticos pensaban inicialmente que los ceros de un polinomio podrían determinarse mediante fórmulas involucrando la extracción de raíces análogas a la que hemos demostrado para ecuaciones cuadráticas. De hecho, esto es posible si el grado de es tres o cuatro, pero las fórmulas correspondientes (que pueden encontrarse por ejemplo en [2], capítulo IV, sección 19), son bastante complicadas). Sin embargo, posteriormente se vio que ello no es en general posible (gracias a los trabajos de Abel y Galois), para ecuaciones de grado mayor o igual que cinco.

Observación 5.1 *Cuando $P \in \mathbb{R}[X]$ es un polinomio de grado impar, es fácil demostrar utilizando el teorema de Bolzano (visto en los cursos de análisis) que P debe tener alguna raíz real.*

Prueba: En efecto, si P es de grado impar y su coeficiente principal a_n es positivo tendremos:

$$\lim_{x\to+\infty} P(x) = +\infty$$

$$\lim_{x\to-\infty} P(x) = -\infty$$

(Si $a_n < 0$, la situación es inversa). En consecuencia, P debe cambiar de signo (esto es: existen $a, b \in \mathbb{R}$ tales que $P(a) < 0$ y $P(b) > 0$); y entonces, como $P(x)$ es una función continua de la variable real x, por el teorema de Bolzano debe existir algún $\alpha \in [a, b]$ tal que $P(\alpha) = 0$. □

Ejemplo: Consideramos el polinomio $X^n - 1$ ($n \in \mathbb{N}$) como polinomio en $\mathbb{C}[X]$. Sus raíces son entonces, precisamente las raíces n-ésismas de la unidad, dadas por

$$\omega_k = e^{\frac{2\pi ik}{n}} \ (0 \leq k < n)$$

Ejemplo: Considerando el cuerpo $K = \mathbb{Z}_p$ con p primo, podemos aplicar la teoría de polinomios al estudio ecuaciones de congruencias de la forma:

$$P(X) \equiv 0 \pmod{p}$$

siendo $P \in \mathbb{Z}[X]$ un polinomio con coeficientes enteros.

Por ejemplo, consideramos la ecuación de congruencia:

$$X^2 \equiv 1 \pmod{5}$$

Podemos escribirla como:

$$X^2 - 1 \equiv 0 \pmod{5}$$

y factorizando el polinomio:

$$(X-1)(X+1) \equiv 0 \pmod{5}$$

pero, precisamente como $\mathbb{Z}_5$ es un cuerpo, esto sucederá si y sólo si

$$X - 1 \equiv 0 (\text{mod } 5) \quad \text{o} \quad X + 1 \equiv 0 (\text{mod } 5)$$

o sea si y sólo si:

$$X \equiv 1 \pmod 5 \quad \text{o} \quad X \equiv -1 \equiv 4 \pmod 5$$

O sea: las clases $\overline{1}$ y $\overline{4}$ son las raíces del polinomio $X^2 - \overline{1}$ en $\mathbb{Z}_5$.

Este razonamiento no funciona si el módulo no es primo (precisamente porque entonces $\mathbb{Z}_n$ no es un cuerpo). Por ejemplo, la ecuación:

$$X^2 \equiv 1 \pmod{\text{8}}$$

tiene cuatro soluciones módulo 8, a saber $X \equiv 1, 3, 5$ o 7, a pesar de ser una ecuación de segundo grado.

6. Divisibilidad de polinomios

El hecho de que en el conjunto de polinomios $A[X]$ hayamos definido las operaciones de suma, resta y producto (que como hemos dicho, le da estructura de anillo), abre la posibilidad de estudiar en él cuestiones de divisibilidad o factorización, en completa analogía con la aritmética de los números enteros. Recordemos que, como hemos señalado en la introducción, la factorización de polinomios, guarda estrecha relación con el problema de encontrar las raíces o ceros de un polinomio.

Definición 6.1 *Sean P, Q en $K[X]$. Diremos que P divide a Q, y lo escribiremos $P|Q$, si existe un polinomio S en $K[X]$ tal que $Q = P \cdot S$.*

Ejemplo: El polinomio $X-1$ divide a X^3-1 en $\mathbb{Q}[X]$ ya que este último polinomio admite la factorización:

$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

Observación: Dado que, por hipótesis, K es un cuerpo, las constantes no nulas de K (pensadas como polinomios constantes), dividen a todos los polinomios. Juegan el mismo rol en la aritmética de polinomios que los números 1 y -1 jugaban en la aritmética de $\mathbb{Z}$ (se dice que son las **unidades** del anillo $K[X]$).

También podemos introducir la noción de **polinomio irreducible**, que es la noción análoga para polinomios, a la noción de número primo en la aritmética de $\mathbb{Z}$.

Definición 6.2 *Sea $P \in K[X]$ un polinomio no constante. Diremos que el polinomio P es irreducible en $K[X]$ si no es posible factorizarlo en la forma $P = Q \cdot S$ donde Q y S son polinomios en $K[X]$ no contantes.*

Ejemplo 1: Un polinomio de primer grado siempre es irreducible.

Ejemplo 2: En cambio, un polinomio de segundo grado será irreducible según tenga o no raíces en K.

Por ejemplo, consideremos el polinomio $P = X^2 + 1$. Si lo pensamos en $\mathbb{R}[X]$, dicho polinomio es irreducible, pue si admitiera una factorización como producto de dos factores de grado uno:

$$X^2 + 1 = k(X - a)(X - b)$$

con $k, a, c \in \mathbb{R}$, P admitiría dos raíces reales a, b, pero sabemos que no tiene ninguna.

En cambio en $\mathbb{C}[X]$, P se factoriza en la forma:

$$X^2 + 1 = (X - i)(X + i)$$

y entonces no es irreducible.

Más adelante, veremos que en general, un polinomio que admite raíces en K no puede ser irreducible en $K[X]$.

Dado que, como hemos dicho, el concepto de polinomio irreducible es análogo para los polinomios, al concepto de número primo, en la aritmética de $\mathbb{Z}$, cabe preguntarse si los polinomios admitirán factorización única como producto de polinomios irreducibles. Veremos que la respuesta es afirmativa, pero para poder enunciar y demostrar este teorema, henos de profundizar la analogía entre los polinomios y la aritmética de $\mathbb{Z}$.

7. El algoritmo de división para polinomios

Si repazamos como hicimos en $\mathbb{Z}$ para demostrar los resultados fundamentales, que condujeron al teorema de factorización única, veremos que en la base de la aritmética de $\mathbb{Z}$ estaba el algoritmo de división. Por ello, tiene sentido preguntarse si existirá un concepto análogo para polinomios.

Dados dos polinomios P y D con $D \neq 0$, aunque D no divida a P, podríamos preguntarnos si es posible escribirlo en la forma

$$P = QD + R$$

donde el resto es "pequeño" en relación con D. Pero dado que entre los polinomios no hay orden, utilizaremos el grado para compararlos. Este es el contenido del siguiente teorema.

Teorema 7.1 *Sea K un cuerpo. Entonces, dados polinomios $P, D \in K[X]$ con $D \neq 0$, existen únicos polinomios Q (cociente) y R (resto) de la división de polinomios de P por D, tales que*

$$P = QD + R$$

y $R = 0$ (el polinomio nulo) o sino $gr(R) < gr(D)$.

El algoritmo para dividir polinomios es conocido desde la escuela secundaria. La demostración siguiente, es una formalización de dicho algoritmo:
Prueba: Demostremos primero la existencia: Para ello, hacemos inducción en el grado del dividendo, P.

Si $P = 0$ o si $\text{gr}(P) = 0$ (polinomios contantes), claramente podemos tomar $Q = 0$, y $R = P$.

Hagamos ahora el paso inductivo: Supongamos pues que $grP = n$ y que ya hemos demostrado el teorema cuando el grado del dividendo es menor que n.

Sean pues:

$$P = \sum_{i=0}^{n} a_i X^i \text{ con } a_n \neq 0 \ (\text{gr}(P) = n)$$

$$D = \sum_{j=0}^{m} b_j X^j \text{ con } b_m \neq 0 \ (\text{gr}(D) = m)$$

Nuevamente si $n < m$, podemos tomar $Q = 0$ y $R = P$.

Supongamos pues que $n \geq m$.Entonces podemos determinar un primer cociente aproximado Q_0, dividiendo el monomio principal de P, $a_n X^n$, por el monomio principal $b_m X^m$ de Q, obteniendo:

$$Q_0 = \frac{a_n}{b_m} \, X^{n-m}$$

(Aquí hacemos uso de la hipótesis de que en K podemos dividir, es decir que K es un cuerpo).

Entonces, definiendo $R_0 = P - Q_0 D$, obtenemos un primer resto aproximado. Si fuera $R_0 = 0$ o $\text{gr}(R_0) < \text{gr}(D)$, hemos terminado: tomando $Q = Q_0$ y $R = R_0$ obtenemos lo que queremos.

Si no, hemos de repetir el proceso. Para ello notamos que $\text{gr}(R_0) < \text{gr}(P)$, ya que en la forma que hemos elegido Q_0 los términos correspondientes a la potencia X^n se cancelan. Entonces, en virtud de la hipótesis de inducción, existirán Q_1 y R_1, cociente y resto respectivamente en la división de R_0 por D, de modo que:

$$R_0 = Q_1 D + R_1$$

donde $R_1 = 0$ o $\text{gr}(R_1) < \text{gr}(D)$. Entonces,

$$P = Q_0 D + R_0 = Q_0 D + Q_1 D + R_1 = (Q_0 + Q_1)D + R_1$$

Entonces tomando $R = R_1$ y $Q = Q_0 + Q_1$ obtenemos lo que queremos. Esto demuestra la parte de existencia.

Queda por demostrar la unicidad: Para ello supongamos que tenemos dos cocientes Q y $\tilde{Q}$, y dos restos R y $\tilde{R}$ de modo que:

$$P = QD + R \text{ y } R = 0 \text{ o } \text{gr}(R) < \text{gr}(D)$$

$$P = \tilde{Q}D + \tilde{R} \text{ y } \tilde{R} = 0 \text{ o } \text{gr}(\tilde{R}) < \text{gr}(D)$$

Entonces obtenemos que:

$$QD + R = \tilde{Q}D + \tilde{R}$$

o sea:

$$(Q - \tilde{Q})D = \tilde{R} - R$$

Si $R = \tilde{R}$ tendríamos que $(Q - \tilde{Q})D = 0$ y por lo tanto como $D \neq 0$, $Q - \tilde{Q} = 0$; o sea, $Q = \tilde{Q}$.

Hemos pues de probar que no puede suceder que $R \neq \tilde{R}$. Pero si esto ocurriera sería $R - \tilde{R} \neq 0$, $Q - \tilde{Q} \neq 0$ y comparando los grados obtenemos una contradicción pues:

$$\text{gr}[(Q - \tilde{Q})D] = \text{gr}(Q - \tilde{Q} + \text{gr}(D) \geq \text{gr}(D)$$

y por otra parte:

$$\text{gr}(\tilde{R} - R) \leq \text{máx}(\text{gr}(R), \text{gr}(\tilde{R}) < \text{gr}(D)$$

Esta contradicción provino de suponer que $R \neq \tilde{R}$. Así pues, debe ser $R = \tilde{R}$, y consecuentemente, $Q = \tilde{Q}$. Esto prueba la unicidad del cociente y el resto. □

8. El teorema del resto

Un caso importante de la división de polinomios, es la división de polinomios por polinomios de la forma $X - a$:

Teorema 8.1 (Teorema del Resto) *El resto de la división de un polinomio $P \in K[X]$ por $X - a$ ($a \in K$), coincide con el valor $P(a)$ del polinomio P especializado cuando $X = a$.*

Prueba: Diviendo P por $X - a$ lo escribimos como:

$$P(X) = Q(X) \cdot (X - a) + R$$

donde el resto R debe ser un polinomio constante. Luego, especializando esta expresión en $X = a$, obtenemos que: $P(a) = R$ □

Corolario 8.1 *Sea $P \in K[X]$ un polinomio. Entonces P es divisible por $X - a$ ($a \in K$) si y sólo si a es raíz de P.*

Ejemplo: Consideremos la ecuación cúbica:

$$P(X) = X^3 - 6X^2 + 11X - 6 = 0$$

Se ve a ojo que $X = 1$, es raíz. Entonces el polinomio P será divisible (en $\mathbb{Q}[X]$) por $X - 1$. Efectuando la división de polinomios, obtenemos la factorización:

$$P(X) = (X - 1)(X^2 - 5X + 6) = (X - 1)Q(X)$$

Entonces, para que X sea raíz de P debe ser $X - 1 = 0$ o

$$Q(X) = X^2 - 5X + 6 = 0$$

Esta es la ecuación cuadrática que resolvimos en la introducción, y sus raíces son $X = 2$ y $X = 3$, con lo que Q se factoriza en la forma:

$$Q(X) = (X - 2)(X - 3)$$

Por lo tanto, las raíces de P son $X = 1$, $X = 2$ y $X = 3$, y su factorización es:

$$P(X) = (X-1)(X-2)(X-3)$$

Vemos que en general el corolario 8.1, es útil a la hora de resolver ecuaciones, porque significa que una vez que encontramos alguna raíz a del polinomio P, el problema se reduce al de resolver una ecuación de un grado menor, efectuando la división de P por $X - a$.

Otro Ejemplo: Consideremos el polinomio $P = X^n - 1$ en $\mathbb{Q}[X]$. Claramente 1 es raíz de P. En consecuencia, P es divisible por $X - 1$. Efectuando la división de polinomios se ve que P se factoriza de la siguiente manera:

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \ldots + X^2 + X + 1)$$

Similarmente consideremos el polinomio $Q = X^n + 1$. Ahora vemos que -1 es raíz de Q si y sólo si n es impar. En este caso, el polinomio Q se factoriza de la siguiente manera:

$$X^n + 1 = (X+1)(X^{n-1} - X^{n-2} + X^{n-3} - X^{n-4} \pm \ldots + X^2 - X + 1)$$

Corolario 8.2 *Si un polinomio P es irreducible en $K[X]$, no puede tener raíces en K.*

Corolario 8.3 *Si $P \in K[X]$ es un polinomio de grado 2 o 3, entonces P es irreducible en $K[X]$ si y sólo si P no tiene raíces en K.*

Prueba: Por el corolario anterior, basta probar la afirmación recíproca: a saber, que si P es irreducible, no puede tener raíces. Pero si tuviéramos que $P = RS$ con R, S no constantes, entonces alguno de los factores R o S sería de primer grado (pues $\mathrm{gr}(P) = \mathrm{gr}(R) + \mathrm{gr}(S)$), y entonces P tendría una raíz. □

Ejemplo: Consideremos el polinomio $P(X) = X^3 - 2 \in \mathbb{Q}[X]$. Como $\sqrt[3]{2}$ es irracional, P no tiene raíces en $\mathbb{Q}$. Luego es irreducible en $\mathbb{Q}[X]$.

Razonando inductivamente (por inducción en r) podemos demostrar lo siguiente:

Corolario 8.4 *Si $P \in K[X]$ es un polinomio, y $\alpha_1, \alpha_2, \ldots, \alpha_r$ son raíces distintas de P, entonces P admite la factorización siguiente:*

$$P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_r)Q(X)$$

Comparando los grados de ambos miembros en esta ecuación, obtenemos la siguiente consecuencia importante:

Corolario 8.5 *Si K es un cuerpo y $P \in K[X]$ es un polinomio de grado n, P no puede tener más de n raíces en K.*

de aquí deducimos en particular

Corolario 8.6 *Si K es un cuerpo infinito, y $P, Q \in K[X]$ son dos polinomios que originan la misma función polinómica ($f_P = f_Q$ o sea $P(a) = Q(a)$ para todo $a \in K$), entonces son iguales.*

Pues en efecto, $P - Q$ debe anularse para todo los elementos de K, y como K es infinito, por el corolario anterior; esto sólo puede suceder si $P - Q$ es el polinomio nulo. Es decir si $P = Q$.

Otro colorario es:

Corolario 8.7 *Si K es un cuerpo, y $P \in K[X]$ es un polinomio de grado n*

$$P = \sum_{i=0}^{n} a_i X^i \text{ con } a_n \neq 0$$

que tiene exactamente n raíces distintas $\alpha_1, \alpha_2, \ldots, \alpha_n$ en K, tenemos que:

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n)$$

siendo a_n el coenficiente principal de P.

Prueba: Comparando los grados en el corolario 8.4, vemos que en este caso, Q debe ser de grado cero, es decir un polinomio constante. Igualnado entonces los coeficientes principales, vemos que $Q = a_n$. □

Ejemplo: Volvamos a mirar el ejemplo del polinomio $P = X^n - 1 \in \mathbb{C}[X]$, cuyas raíces son las n raíces n-ésimas de la unidad:

$$\omega_k = e^{\frac{2\pi ik}{n}} \ (0 \leq k < n)$$

Entonces P admite la factorización:

$$X^n - 1 = \prod_{k=0}^{n-1}(X - \omega_k) \tag{1}$$

Otro Ejemplo: Sea p un número primo, y consideremos el polinomio $Q = X^{p-1} - 1$, sobre el cuerpo $K = \mathbb{Z}_p$. Por el teorema de Fermat, cualquier elemento no nulo de $\mathbb{Z}_p$ es una raíz de este polinomio. Deducimos que su factorizaciòn en $\mathbb{Z}_p$ es[4]

$$X^{p-1} - 1 = (X-1)(X-2)(X-3)\dots(X-(p-1)) \quad \text{en } \mathbb{Z}_p[X]$$

Comparando los términos independientes se otra demostración de una de las implicaciones del teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}$$

9. Raíces Racionales

En general, para polinomios de grado alto, no existe un método general para determinar sus raíces (aunque para polinomios de coeficientes reales, existen métodos numéricos para determinarlas aproximadamente con tanta precisión como se desee, lo cual es suficiente para cualquier aplicación práctica[5]).

Sin embargo, existe un método general para determinar todas las posibles raíces racionales de un polinomio con coeficientes racionales. Sea $P \in \mathbb{Q}[X]$:

$$P(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_2 X^2 + a_1 X + a_0 \text{ con } a_I \in \mathbb{Q}$$

Multiplicando a P por el mínimo común múltiplo de los denominadores de los a_i, podemos suponer que todos sus coeficientes son enteros, es decir que $P \in \mathbb{Z}[X]$. Entonces, se tiene el siguienteteorema:

[4]Para simplificar la notación, escribirmos aquí por ejemplo 3 y no $\overline{3}$, pero recordamos que los elementos de $\mathbb{Z}_p$ no son enteros, sino clases de enteros congruéntes módulo p

[5]Esto lo verán en el curso de Elementos de Cálculo Numérico (para matemática) o de métodos numéricos (para computación).

Teorema 9.1 (Criterio de Gauss) *Si $P \in \mathbb{Z}[X]$ y $a = \frac{p}{q} \in \mathbb{Q}$ es una raíz racional de P, escrita como fracción irreducible (o sea con p y q coprimos), se tiene necesariamente que $p|a_0$ y que $q|a_n$.*

En particular, si P es mónico (o sea $a_n = 1$) las posibles racies racionales de P deben ser enteras.

Prueba: Como $P(a) = 0$, tendremos:

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \ldots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n = 0$$

Luego:

$$p(a_n p^{n-1} + a_{n-1} p^{n-2} q + a_{n-2} p^{n-3} q^2 + \ldots + a_2 p q^{n-1} + a_1 q^{n-1}) = -a_0 q^n$$

En particular:

$$p|a_0 q^n$$

Pero como p es coprimo con q, p es coprimo con q^n (como consecuencia del teorema fundamental de la aritmética). Por lo tanto, p debe dividir a a_0.

Similarmente:

$$q(a_{n-1} p^{n-1} + a_{n-2} p^{n-2} q + \ldots + a_2 p^2 q^{n-3} + a_1 p q^{n-2} + a_0 q^{n-1}) = -a_n p^n$$

Por lo tanto

$$q|a_n p^n$$

Pero como q es coprimo con p, q es coprimo con p^n; y en consecuencia, $q|a_n$. □

Ejemplo: El criterio de Gauss proporciona una nueva prueba de que si $d \in \mathbb{N}$ no es una potencia n-ésima de un entero, $\sqrt[n]{d}$ es irracional. En efecto, por el criterio de Gauss las posibles raíces racionales del polinomio $X^n - d$ deben ser enteras. Luego si $\sqrt[n]{d}$ no es entero, tampoco puede ser racional.

Ejercicio: Probar que bajo las mismas hipótesis del teorema 9.1, se cumple que[6].

$$q - p|P(1)$$

$$q + p|P(-1)$$

Esta observación es con frecuencia útil, ya que reduce el número de ensayos a efectuar al aplicar el criterio de Gauss.

[6] Ver [2], capítulo X, sección 41, ecuación [41-31]

10. Multiplicidad de las raíces

Para poder precisar los resultados anteriores, necesitamos introducir la noción de multiplicidad de una raíz. Para motivar en este concepto recordemos que en el caso de las ecuaciones cuadráticas:

$$P = aX^2 + bX + c = 0$$

las dos raíces α_1, α_2 que proporciona la fórmula para resolver ecuaciones de segundo grado coinciden cuando el discriminante $\Delta = b^2 - 4ac$ de la ecuación se anula, y tenemos en este caso:

$$\alpha_1 = \alpha_2 = \frac{-b}{2a}$$

y el polinomio P se factoriza en la forma:

$$P(X) = a(X - \alpha_1)^2$$

Decimos en este caso que el polinomio P tiene a α_1 como raíz doble.

Generalizando este ejemplo, introducimos la siguiente definición:

Definición 10.1 *Sea $P \in K[X]$ un polinomio, y sea $a \in K$ una raíz de P. Decimos que a es una raíz de P de multiplicidad m ($m \in \mathbb{N}$) si P admite la factorización:*

$$P(X) = (X - a)^m Q(X)$$

donde el polinomio Q no se anula en $X = a$, o sea $Q(a) \neq 0$. Si $m = 1$ se dice que a es una raíz simple, si $m = 2$ que es doble, etcétera.

Proposición 10.1 *Si P es un polinomio que tiene en K las raíces: $a_1, a_2, \ldots, a_r$ con multiplicidades $m_1, m_2, \ldots m_r$, entonces P admite la factorización*

$$P(X) = (X - a_1)^{m_1}(X - a_2)^{m_2} \cdots (X - a_r)^{m_r} Q(X)$$

donde $Q(a_i) \neq 0$ para $0 \leq i \leq r$.

Prueba: Hacemos inducción en r (Ejercicio: desarrollar la demostración). □

Veremos a continuación otra caracterización de la multiplicidad de las raíces. Para ello, necesitaremos introducir el concepto de derivada de un polinomio. Si $K = \mathbb{R}$, este concepto coincidirá con el concepto de derivada visto en los cursos de análisis. Sin embargo, en un cuerpo cualquiera K es posible introducir este concepto de una manera totalmente algebraica, sin referencia alguna a coceptos analíticos (como el concepto de límite) de la siguiente manera[7]:

Definición 10.2 *Sea $P \in K[X]$ un polinomio.*

$$P = \sum_{k=0}^{n} a_k X^k$$

entonces, definimos el polinomio derivado P' por:

$$P' = \sum_{k=1}^{n} k a_k X^{k-1}$$

Aunque no lo demostraremos, es relativamente sencillo comprobar que esta noción de derivada puramente formal, conserva las propiedades usuales de la derivada, como la regla para derivar una suma o un producto:

$$(P + Q)' = P' + Q'$$

$$(P \cdot Q)' = P' \cdot Q + P \cdot Q'$$

Inductivamente, podemos definir también la derivada n-ésima $P^{(n)}$ del polinomio P de la siguiente manera:

$$\left\{ \begin{array}{rcl} P^{(0)} & = & P \\ P^{(n+1)} & = & (P^n)' \end{array} \right.$$

Haremos también en el resto de esta sección, otra hipótesis de caracter técnico, a saber que no sea posible obtener cero, sumando 1 finitas veces en K:

$$\overbrace{1 + 1 + \cdots + 1}^{n \text{ veces}} \neq 0 \text{ en } K \tag{2}$$

[7]Cuando $K = \mathbb{C}$, es posible también dar una interpretación analítica del concepto de derivada de un polinomio, pero esto se ve en el curso de análisis complejo.

Esta hipótesis[8] claramente se cumple en los ejemplos usuales $K = \mathbb{Q}$, $K = \mathbb{R}$ o $K = \mathbb{C}$ (pero no se cumple por ejemplo si $K = \mathbb{Z}_p$ con p primo).

Necesitaremos también la siguiente versión de la fórmula de Taylor para polinomios[9]:

Teorema 10.1 *Si $P \in K[X]$ es un polinomio con $gr(P) \leq n$ y $a \in K$, tenemos que:*

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Prueba: Para demostrar la fórmula de Taylor, primero la demostramos para monomios de la forma $P = X^m$. En este caso las derivadas de P valen:

$$P'(X) = mX^{m-1}$$

$$P^{(2)}(X) = m(m-1)X^{m-2}$$

$$P^{(3)}(X) = m(m-1)(m-2)X^{m-3}$$

y siguiendo de esta manera, podemos demostrar inductivamente que:

$$P^{(k)}(X) = m(m-1)(m-2)\dots(m-k+1)X^{m-k} \text{ si } k \leq m$$

mientras que

$$P^{(k)}(X) = 0 \text{ si } k > m$$

Entonces, recordando la expresión de los números combinatorios:

$$\binom{m}{k} = \frac{m(m-1)(m-2)\cdots(m-k+1)}{k!} \quad (0 \leq k \leq m)$$

[8]Un cuerpo donde se cumple esta condición se llama un cuerpo de característica cero.

[9]La hipótesis (2) es necesaria para la validez de este teorema, ya que gracias a ella podemos pensar que los números naturales $\mathbb{N}$ están contenidos en K (identificando el número $n \in \mathbb{N}$ con $\overbrace{1+1+\cdots+1}^{n \text{ veces}}$) y entonces tiene sentido dividir por $k!$ a los elementos de K. Por ejemplo, si fuera $K = \mathbb{Z}_p$, donde dicha hipótesis no se verifica, $k!$ sería $\overline{0}$ en $\mathbb{Z}_p$ para $k \geq p$, y estaríamos dividiendo por cero.

y el teorema del binomio de Newton[10], vemos que:

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{m} \binom{m}{k} X^k (X-a)^k = (X+(X-a))^m = X^m$$

Para demostar el teorema en general, observamos que cualquier polinomio es una combinación lineal de potencias de X y que la expresión que aparece en el segundo miembro de la fórmula de Taylor es lineal en el polinomio P:

Si

$$P = \sum_{i=0}^{m} a_i X_i$$

y notamos $P_i(X) = X^i$ entonces

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=0}^{n} \frac{1}{k!} \left(\sum_{i=0}^{m} a_i P_i^{(k)}(a) \right) (X-a)^k$$

$$= \sum_{i=0}^{m} a_i \left(\sum_{k=0}^{n} \frac{P_i^{(k)}(a)}{k!}(X-a)^k \right)$$

que por el caso anteriormente demostrado del teorema es:

$$= \sum_{i=0}^{m} a_i P_i(X) = P$$

□

Ahora podemos demostrar:

Teorema 10.2 *Sea $P \in K[X]$ un polinomio, y $a \in K$. Entonces, a es una raíz de P de multiplicidad m si y sólo si $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Dicho de otro modo, la multiplicidad de a como raíz de P viene dada por el orden de la primer derivada de P que no se anula cuando la especializamos en $X = a$.*

Ejermplo: Volvamos a consideremos el polinomio cuadrático $P(X) = aX^2 + bX + c$. Entonces $P'(X) = 2aX + b$, que se anula en $X = \frac{-b}{2a}$. Entonces

[10] Aquí estamos utilizando el teorema del binomio aplicado a elemtos del anillo $K[X]$. En general, el teorema del binomio es válido en cualquier anillo conmutativo.

este teorema dice que tendremos una raíz doble, precisamente cuando esta raíz sea $\frac{-b}{2a}$ (lo que efectivamente sucede cuando $\Delta = 0$).

Ejemplo 2: Consideremos el polinomio $P(X) = X^3 - 5X^2 + 7X - 3$. Entonces $P'(X) = 3X^2 - 10X + 7$ y $P^{(2)}(X) = 6X - 10$. Entonces $X = 1$ es raíz doble, pues $P(1) = 0$, $P'(1) = 0$ y $P'(1) = -4 \neq 0$. Mientras que 3 es raíz simple, ya que $P(3) = 0$ pero $P'(3) = 4 \neq 0$. En consecuencia, la factorización de P es:

$$P(X) = (X-1)^2(X-3)$$

Ejemplo 3: Volvamos a mirar el polinomio $X^n - 1 \in \mathbb{C}[X]$, cuyas raíces son las raíces n-ésimas de la unidad ω_k. Entonces como $P'(X) = nX^{n-1}$ y $P'(\omega_k) = n\omega_k^{n-1} \neq 0$, deducimos que las ω_k son raíces simples, como también se ve a partir de la factorización (1).

Ahora demostremos el teorema 10.2:

Prueba: Supongamos primero que $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Entonces, utilizando la fórmula de Taylor tenemos que:

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k$$

Entonces sacando un factor común $(X-a)^m$, podemos escribir

$$P(X) = (X-a)^m Q(X)$$

siendo $Q(X)$ el polinomio:

$$Q(X) = \sum_{k=m}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-m}$$

y como

$$Q(a) = \frac{P^{(m)}(a)}{k!} \neq 0$$

deducimos que a es una raíz de multiplicidad m.

Ahora probaremos la afirmación recíproca, a saber que si a es una raíz de multiplicidad m, entonces: $P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$ pero $P^{(m)}(a) \neq 0$. Para ello, utilizaremos inducción en $m \in \mathbb{N}$:

Si $m = 1$, estamos suponiendo que a es una raíz simple de P, y tenemos la factorización:

$$P(X) = (X - a)Q(X)$$

con $Q(a) \neq 0$. En consecuencia, derivando con la regla del producto:

$$P'(X) = Q(X) + Q'(X)(X - a)$$

y cuando especializamos en $X = a$, obtenemos que:

$$P'(a) = Q(a) \neq 0$$

Ahora hagamos el paso inductivo: es decir supongamos que el teorema es cierto para raíces de multiplicidad $m - 1$, y probemos que entonces también es verdadero para raíces de multiplicidad m.

Si a es una raíz de P de multiplicidad m, entonces P admite la factorización

$$P(X) = (X - a)^m Q(X) \text{ con } Q(a) \neq 0$$

Derivando nuevamente con la regla del producto:

$$P'(X) = m(X - a)^{m-1}Q(X) + (X - a)^m Q'(X)$$

Sacando factor común $(X - a)^{m-1}$, obtenemos:

$$P'(X) = (X - a)^{m-1}Q_1(X)$$

donde $Q_1(X) = mQ(X) + (X - a)Q'(X)$. Luego:

$$Q_1(a) = mQ(a) \neq 0$$

En consecuencia, a es raíz de multiplicidad $m-1$ de P'. Luego, por hipótesis inductiva, las derivadas de P' se anulan en a hasta el orden $m - 2$:

$$(P')'(a) = (P')^{(2)}(a) = \ldots = (P')^{(m-2)}(a) = 0$$

pero

$$(P')^{(m-1)}(a) \neq 0$$

Pero esto precisamente significa que:

$$P(a) = P'(a) = P^{(2)}(a) = \ldots = P^{(m-1)}(a) = 0$$

pero $P^{(m)}(a) \neq 0$. En virtud del principio de inducción, esto demuestra el teorema para todo $m \in \mathbb{N}$. □

11. El Teorema Fundamental del Álgebra

Hemos visto que las ecuaciones cuadráticas siempre tienen soluciones en los números complejos. Una generalización de este hecho, es el siguiente resultado:

Teorema 11.1 (Teorema Fundamental del Álgebra) *Todo polinomio con coeficiente complejos $P \in \mathbb{C}[X]$ no constante, tiene alguna raíz en el cuerpo de los números complejos, es decir existe $\alpha \in \mathbb{C}$ tal que $P(\alpha) = 0$.*

Existen varias demostraciones diferntes de este teorema (y los estudiantes de matemática verán seguramente varias a lo largo de su carrera), pero ninguna de ellas resulta adecuada para el curso de álgebra I. Por ello, no daremos una demostración de este teorema.

Cabe mencionar sin embargo, que pese al nombre con que es conocido este teorema, no es posible demostrarlo sin utilizar de alguna manera conceptos analíticos (como la continuidad del polinomio $P(z)$ como función de la variable compleja $z \in \mathbb{C}$). También es importante destacar que ninguna de ellas es constructiva, es decir: no proporcionan un procedimiento efectivo para encontrar la raíz α, sino que demuestran reducción al absurdo la existencia de alguna raíz, suponiendo que no existe ninguna, y llegando entonces a un absurdo.

Una demostración relativamente elemental (aunque no sencilla[11]) puede encontrarse en [2] (capítulo IV, sección 18). Otra demostración diferente, basada en ideas geométricas provenientes de la topología, es expuesta en forma elemental en [3], y en [1] con un grado mayor de formalización.

Un corolario importante del teorema 11.1 es el siguiente:

Corolario 11.1 *Todo polinomio con coeficiente complejos*

$$P = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X] \ (a_i \in \mathbb{C}, a_n \neq 0)$$

no constante se factoriza como producto de polinomios lineales, en la forma:

$$P(X) = a_n(X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \cdots (X - \alpha_r)^{m_r}$$

[11] Consiste esencialmente en demostrar que la función $|P(z)|$ debe alcanzar un mínimo, para algún $z \in \mathbb{C}$ (pues es continua como función de z y tiende a más infinito cuando $|z|$ tiende a infinito), y probar (por reducción al absurdo), que en dicho mínimo $P(z)$ debe anularse.

donde $\alpha_1, \alpha_2, \ldots, \alpha_r$ son las distintas raíces complejas de P, $m_1, m_2, \ldots, m_r$ son las correspondientes multiplicidades, y a_n es el coeficiente principal del polinomio P.

Prueba: Por el corolario 10.1,

$$P(X) = (X - \alpha_1)^{m_1}(X - \alpha_2)^{m_2} \ldots (X - \alpha_r)^{m_r} Q(X)$$

donde $Q(\alpha_i) \neq 0$ para $0 \leq i \leq r$.

Afirmamos que Q debe ser constante: si suponemos que no, por 11.1, Q debe tener alguna raíz $\alpha \in \mathbb{C}$, pero toda raíz de Q es raíz de P. Luego $\alpha = \alpha_i$ para algún i, lo que es una contradicción pues $Q(\alpha_i) \neq 0$.

Como Q debe ser constante, al igualar los coeficientes principales de ambos miembros, deducimos que Q debe coincidir con el coeficiente principal de P. □

Comparando los grados de ambos miembros, en la descomposición del corolario anterior deducimos que:

$$n = \text{gr}(P) = m_1 + m_2 + \ldots + m_r$$

Observemos que esta suma representa la cantidad de raíces de P, si contamos las raíces múltiples de acuerdo con su multiplicidad. Esto nos proporciona el siguiente corolario:

Corolario 11.2 *Un polinomio $P \in \mathbb{C}[X]$ tiene exactamente n raíces complejas, si las contamos de acuerdo con su multiplicidad.*

En particular, hemmo demostrado que en $\mathbb{C}[X]$ los únicos polinomios irreducibles son los lineales (de grado 1).

12. Raíces complejas de polinomios reales

Recordamos que si $z = a + bi$ es un número complejo, su complejo conjugado $\overline{z}$ se define por $\overline{z} = a - bi$. La operación de tomar el complejo conjugado tiene varias propiedades importantes:

1. $z = \overline{z}$ si y sólo si $z \in \mathbb{R}$

2. Si $z, w \in \mathbb{C}$ entonces

$$\overline{z+w} = \overline{z} + \overline{w}$$

$$\overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

3. $z + \overline{z} = 2\text{Re}(z)$ y $z \cdot \overline{z} = |z|^2$ son números reales.

Recordemos que si $P = aX^2 + bX + c$ es un polinomio cuadrático con coeficientes reales y discriminante $\Delta = b^2 - 4ac$ negativo, P tiene dos raíces complejas conjugadas dadas por: siendo

$$\alpha_1 = \frac{-b + \sqrt{-\Delta}\, i}{2a}$$

y

$$\alpha_2 = \frac{-b - \sqrt{-\Delta}\, i}{2a}$$

Así pues, las raíces complejas de un polinomio cuadrático forman un par de raíces conjugadas.

Ahora generalizaremos este hecho a polinomios con coeficientes reales de mayor grado. Consideremos para ello un polinomio con coeficientes complejos:

$$P(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$$

y definimos el polinomio conjugado $\overline{P}$ por

$$\overline{P}(X) = \sum_{i=0}^{n} \overline{a_i}\, X^i$$

Como consecuencia de las propieedades antes mencionadas del conjugado, si $z \in \mathbb{C}$ tenemos que:

$$\overline{P}(z) = \overline{P}(\overline{z})$$

y si $P, Q \in C[X]$ son polinomios:

$$\overline{P+Q} = \overline{P} + \overline{Q}$$

$$\overline{P \cdot Q} = \overline{P} \cdot \overline{Q}$$

En particular, si los coeficientes de P son reales (esto es $P \in \mathbb{R}[X]$), tendremos que $\overline{P} = P$, y resulta que:

$$\overline{P(z)} = P(\overline{z})$$

En particular si $P(z) = 0$, tenemos que $P(\overline{z}) = 0$, es decir, hemos demostrado que las raíces complejas de un polinomio con coeficientes reales se presentan de a pares de raíces conjugadas:

Proposición 12.1 *Sea $P \in \mathbb{R}[X]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de P, entonces su complejo conjugado $z = a - bi$ también es raíz de P*

Similarmente podemos demostrar,

Proposición 12.2 *Sea $P \in \mathbb{R}[X]$ un polinomio con coeficientes reales. Si $z = a + bi$ es una raíz de P con multiplicidad m , entonces su complejo conjugado $z = a - bi$ también es raíz de P con multiplicidad m.*

Prueba: Como z es raíz de P con multiplicidad m, P admite la factorización:

$$P(X) = (X - z)^m Q(X)$$

donde $Q(z) \neq 0$. Utilizando la operación de "tomar el polinomio conjugado" que definimos antes, tenemos:

$$\overline{P}(X) = \overline{(X - z)^m Q(X)} = \overline{(X - z)^m} \cdot \overline{Q}(X) = (X - \overline{z})^m \overline{Q}(X)$$

Pero como P tiene coeficientes reales, $\overline{P} = P$ y como

$$P(\overline{z}) = 0, \overline{Q}(\overline{z}) \neq 0$$

esto dice que $\overline{z}$ es una raíz de P de multiplicidad m. □

Podemos utilizar este hecho para obtener la factorización de un polinomio en $\mathbb{R}[X]$ a partir de su factorización compleja.

Sea como antes $P \in \mathbb{R}[X]$ y llamemos $\alpha_1, \alpha_2, \ldots \alpha_r$ a sus raíces reales (distintas). También consideremos sus raíces complejas (con parte imaginaria

no nula), que por el razonamiento anterior, se presentan en pares de raíces conjugadas:

$$\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \ldots, \beta_s, \overline{\beta_s}$$

Por otra parte, llameos m_i a la multiplicidad de α_i como raíz de P y f_i a la multiplicidad de β_i como raíz de P (que por la proposición 12.2 también es la multiplicidad de $\overline{\beta_i}$. Entonces: P admite en $C[X]$ la factorización dada por el corolario 11.1:

$$P = a_n(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_r)^{m_r}$$
$$\cdot(X-\beta_1)^{f_1}(X-\overline{\beta_1})^{f_1}(X-\beta_2)^{f_2}(X-\overline{\beta_2})^{f_2}\cdots(X-\beta_s)^{f_2}(X-\overline{\beta_s})^{f_s}$$

Para obtener su factorización en $\mathbb{R}[X]$, debemos agrupar los factores correspondientes a cada par de raíces conjugadas: para ello observamos que

$$Q_{\beta_i}(X) = (X-\beta_i)(X-\overline{\beta_i}) = X^2 - 2\,\mathrm{Re}(\beta_i)X + |\beta_i|^2$$

es un polinomio cuadrático con coeficientes reales (y discriminante negativo, pues no tiene raíces reales).

En definitiva, hemos demostrado el teorema siguiente:

Teorema 12.1 *Si $P \in \mathbb{R}[X]$ es un polinomio con coeficientes reales, entonces P admite la factorización:*

$$P = a_n(X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_r)^{m_r}\cdot Q_{\beta_1}^{f_1}Q_{\beta_2}\cdots Q_{\beta_s}^{f_s}$$

donde a_n es el coeficiente principal de P, las α_i son las raíces reales de P y los Q_{β_i} son polinomios cuadráticos con coeficientes reales y discriminante negativo (correspondientes a cada par de raíces complejas de P).

En particular, vemos que en $\mathbb{R}[X]$ los polinomios irreducibles son los lineales (grado 1) y los polinomios cuadráticos (grado 2) con discriminante negativo.

Ejemplo: Consideremos por ejemplo el polinomio $P = X^6 - 1$, cuyas raíces son las raíces sextas de la unidad:

$$\omega_k = e^{2\pi i k/6}\ (k = 0, 1, \ldots, 5)$$

Más explicitamente vienen dadas por:

$$\omega_0 = 1, \quad \omega_1 = \frac{1+\sqrt{3}}{2}, \quad \omega_2 = \frac{-1+\sqrt{3}}{2}$$

$$\omega_3 = -1, \quad \omega_4 = \frac{-1-\sqrt{3}}{2}, \quad \omega_5 = \frac{1-\sqrt{3}}{2}$$

Entonces, la factorización de P en $\mathbb{C}[X]$ es:

$$P(X) = (X-\omega_0)(X-\omega_1)(X-\omega_2)(X-\omega_3)(X-\omega_4)(X-\omega_5)$$

Pero ω_0 y ω_3 son la raíces reales, y $\omega_5 = \overline{\omega_1}$, $\omega_4 = \overline{\omega_2}$, de modo que agrupando cada raíz compleja conjugada con su con su conjugada, obtenemos los polinomios cuadráticos:

$$Q_{\omega_1} = (X-\omega_1)(X-\omega_5) = X^2 - X + 1$$

(Las raíces de este polinomio son las raíces sextas primitivas de la unidad), y

$$Q_{\omega_2} = (X-\omega_2)(X-\omega_4) = X^2 + X + 1$$

(Las raíces de este polinomio son las raíces cúbicas primitivas de la unidad).

Entonces, P admite la siguiente factorización en $\mathbb{R}[X]$:

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1)$$

13. Raíces irracionales cuadráticas

Proposición 13.1 *Sea $P \in \mathbb{Q}[X]$ un polinomio con coeficientes racionales, y $d \in \mathbb{N}$ un entero que no es el cuadrado de otro entero. Entonces si $\alpha_1 = a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$ y $b \neq 0$ es una raíz de P, $\alpha_2 = a - b\sqrt{d}$ también lo es.*

Prueba: Notemos que como d no es un cuadrado, $\sqrt{d} \notin \mathbb{Q}$, esto es: es un número irracional. En consecuencia, α_1 y α_2 son también irracionales, ya que sino:

$$\sqrt{d} = \frac{\alpha_1 - a}{b} = \frac{\alpha_2 - a}{(-b)}$$

sería racional. Sin embargo, el polinomio

$$D(X) = (X-\alpha_1)(X-\alpha_2) = X^2 - 2aX + a^2 - db^2$$

tiene coeficientes racionales. Efectuemos la división de polinomios de P por D (en $\mathbb{Q}[X]$), obteniendo un cociente Q y un resto R:

$$P = QD + R \text{ con } R = 0 \text{ o } \mathrm{gr}(R) < \mathrm{gr}D = 2$$

Notemos que entonces, Q y R tienen entonces coeficientes racionales, y que como R tiene grado 1 o 0, deberá escribirse en la forma:

$$R(X) = cX + d \text{ con } c, d \in \mathbb{Q}$$

Si especializamos esta igualdad en $X = \alpha_1$, como por hipótesis P anula a α_1, y por construcción $D(\alpha_1) = 0$, tenemos que:

$$R(\alpha_1) = 0$$

Pero, esto no puede suceder si $R \neq 0$, pues si no,

$$\alpha_1 = -\frac{d}{c} \in \mathbb{Q}$$

(si $c \neq 0$) sería racional (Si $c = 0$, debería ser $d = 0$, y por lo tanto también $R = 0$).

En cualquier caso, concluimos que $R = 0$, y por lo tanto que D divide a Q:

$$P = QD$$

pero como α_2 también es raíz de D; especializando ahora en $X = \alpha_2$, obtenemos que que $P(\alpha_2) = 0$.

□

Ejercicio: Dar una demostración diferente de la proposición 12.1, imitando la idea de la prueba de la proposición 13.1.

14. El algoritmo de Euclides

Como en el anillo de polinomios $K[X]$, tenemos un algoritmo de división, podemos extender a los polinomios el algoritmo de Euclides para el cálculo del máximo común divisor. Comenzamos definiendo esta noción, por analogía con la caracterización del máximo común divisor que teníamos en los enteros:

Definición 14.1 *Sean A, B dos polinomios en $K[X]$. Diremos que un polinomio $D \in K[X]$ es un máximo común divisor entre A y B, si cumple las siguientes condiciones:*

i) D es un divisor común de A y B, es decir $D|A$ y $D|B$.

ii) Si $\tilde{D}$ es otro divisor común de A y B, o sea $\tilde{D}|A$ y $\tilde{D}|B$ entonces $\tilde{D}|D$.

Estas condiciones no determinan unívocamente al máximo común divisor, ya que si D y $\tilde{D}$ son dos máximo comunes divisores entre A y B, lo mejor que podemos decir es que se dividen recíprocamente, o sea $D|\tilde{D}$ y $\tilde{D}|\tilde{D}$, y por lo tanto difieren en una constante no nula de K como factor.

Ejemplo: Consideremos (en $\mathbb{Q}[X]$) los polinomios

$$A(X) = (X-1)(X-2) = X^2 - 3X + 2$$

$$B(X) = (X-1)(X-3) = X^2 - 4X + 3$$

entonces $D = X - 1$ es un máximo común divisor entre A y B, pero $\tilde{D} = 2X - 2 = 2(X-1)$ es otro.

Para eliminar esta ambigüedad, a veces se requiere una condición adicional:

iii) D es mónico

Si pedimos esta condición, el máximo común divisor (si existe, lo cual vamos a ver que siempre ocurre) queda unívocamente determinado.

Ahora podemos enunciar el algoritmo de Euclides, en completa analogía con la aritmética de $\mathbb{Z}$. Dados dos polinomios $A, B \in K[X]$ (y supongamos que $\text{gr}(A) \geq \text{gr}(B)$), para hallar su máximo común divisor, se divide $R_0 = A$ por $R_1 = B$, obteniendo un primer cociente Q_1 y un primer resto R_2, de modo que[12]:

$$A = Q_1 B + R_2 \text{ donde } R_2 = 0 \text{ o } \text{gr}(R_2) < \text{gr}(B)$$

Si $R_2 \neq 0$, podemos volver a dividir $R_1 = B$ por R_2, obteniendo un nuevo cociente Q_2 y un nuevo resto R_3, de modo que se verifica:

$$B = Q_2 R_2 + R_3 \text{ donde } R_3 = 0 \text{ o } \text{gr}(R_3) < \text{gr}(R_2)$$

[12]Utilizamos esta notación procurando ser coherentes con la que utilizamos antes al exponer el algoritmo de Euclides en los números enteros.

Mientras $R_i \neq 0$ podemos continuar este proceso (inductivamente), dividimos a R_{i-1} por R_i obteniendo un nuevo cociente Q_i y un nuevo resto R_{i+1},

$$R_{i-1} = Q_i R_i + R_{i+1} \text{ donde } R_{i+1} = 0 \text{ o } \operatorname{gr}(R_{i+1}) < \operatorname{gr}(R_i)$$

Dado que la sucesión de los restos tiene grado estrictamente decreciente:

$$\operatorname{gr}(A) \geq \operatorname{gr}(B) > \operatorname{gr}(R_2) > \ldots > \operatorname{gr}(R_i) > \operatorname{gr}(R_{i+1}) > \ldots$$

y que los grados son enteros, en virtud del principio del mínimo entero, tarde o temprano debemos tener que $R_n = 0$, es decir que el algoritmo de Euclides termina después de un número finito de pasos. Cuando esto ocurre, podemos demostrar (repitiendo exactamente la cuenta que hicimos para la aritmética de $\mathbb{Z}$), que $R_{n-1} = \operatorname{mcd}(A, B)$, y exactamente igual que en los enteros, se obtiene el teorema siguiente:

Teorema 14.1 *Sean $A, B \in K[X]$ dos polinomios. Entonces su máximo común divisor $D = mcd(A, B)$ siempre existe, y se puede calcular utilizando el algoritmo de Euclides. Además, existen polinomios $\alpha, \beta \in K[X]$ tales que:*

$$\alpha A + \beta B = D$$

Es decir que el máximo común divisor se escribe como una combinación lineal de A y B, pero los coeficientes α y β no son ahora números sino polinomios.

Ejemplo: Calculemos el máximo común divisor entre $A = X^5 - 1$ y $B = X^3 - 1$. Comenzamos dividiendo A por B:

$$X^5 - 1 = X^2(X^3 - 1) + (X^2 - 1)$$

luego $Q_1 = X^2$, $R_2 = X^2 - 1$. Ahora dividimos a B por R_2:

$$X^3 - 1 = X(X^2 - 1) + (X - 1)$$

luego $Q_2 = X$, $R_3 = X - 1$. Finalmente, dividimos a R_2 por R_3:

$$X^2 - 1 = (X + 1)(X - 1)$$

luego $Q_3 = X + 1$ y $R_3 = 0$. En consecuencia, en este caso $D = \operatorname{mcd}(A, B) = X - 1$

Para encontrar los coeficientes α, β tales que $\alpha A + \beta B = D$, procedemos como sigue; de las ecuaciones anteriores obtenemos que:

$$D = (X-1) = 1 \cdot (X^3 - 1) + (-X) \cdot (X^2 - 1)$$

pero

$$X^2 - 1 = 1 \cdot (X^5 - 1) + (-X^2) \cdot (X^3 - 1)$$

Sustituyendo:

$$\begin{aligned} X - 1 &= 1(X^3 - 1) + (-X)\left[1 \cdot (X^5 - 1) + (-X^2) \cdot (X^3 - 1)\right] \\ &= (-X) \cdot (X^5 - 1) + (X^3 + 1) \cdot (X^3 - 1) \end{aligned}$$

Luego $\alpha(X) = -X$ y $\beta(X) = X^3 + 1$.

Observación 14.1 *Sean $A, B \in K[X]$ y $D = mcd(A, B)$ su máximo común divisor. Entonces $a \in K$ es una raíz en común de A y B, si y sólo si a es raíz de D.*

Prueba: Por el corolario 8.1, a es raíz de D si y sólo sí $X - a$ divide a D, lo cual ocurre si y sólo si $X - a$ divide simultáneamente a A y B, lo cual a su vez sucede si y sólo si a es raíz de ambos polinomios. □

Ejemplo: En el ejemplo anterior vimos que $\mathrm{mcd}(X^3 - 1, X^5 - 1) = X - 1$, esto significa precisamente que 1 es la única raíz en común entre estos polinomios (ya que $G_3 \cap G_5 = \{1\}$).

Ejercicio: Probar que en general

$$\mathrm{mcd}(X^n - 1, X^m - 1) = X^d - 1$$

donde $d = \mathrm{mcd}(n, m)$ (en $\mathbb{Z}$)

15. Factorización como producto de polinomios irreducibles

Como consecuencia del algoritmo de Euclides, obtenemos como en el caso de la aritmética de los enteros las siguientes consecuencias:

Corolario 15.1 *Sean $P, Q, R \in K[X]$. Si $P|QR$ y P es coprimo con Q, entonces $P|R$.*

Corolario 15.2 *Sean $P, Q, R \in K[X]$. Si $P|QR$ y P es irreducible en $K[X]$, entonces $P|Q$ o $P|R$.*

Entonces, podemos obtener (imitando el razonamiento que hicimos en los enteros), el siguiente teorema de factorización única:

Teorema 15.1 *Cada polinomio $P \in K[X]$ se puede factorizar de manera única en la forma:*

$$P = kP_1P_2 \cdots P_r$$

siendo k una constante no nula de K, y los P_i polinomios irreducibles en $K[X]$.

La factorización es única en el sentido de que cualquier otra factorización sólo puede diferir en el orden de los factores, en el valor de la constante k y en la multiplicación de alguno de los factores P_i por una constante no nula de K (ajustando adecuadamente el valor de la constante k).

Ejercicio: Escribir una prueba detallada de este teorema, imitando la demostración del teorema de factorización única para los enteros.

Podemos eliminar la ambigüedad en la factorización que surge en la factorización por el hecho de que es posible multiplicar un factor P_i por una constante no nula arbitraria de K (ajustando el valor de k), requiriendo que los polinomios P_i sean mónicos. De esta manera se obtiene el enunciado siguiente:

Teorema 15.2 *Cada polinomio $P \in K[X]$ se puede factorizar de manera única en la forma:*

$$P = a_nP_1P_2 \cdots P_r$$

siendo a_n el coeficiente principal de P, y los P_i polinomios mónicos irreducibles en $K[X]$.

La factorización es única en el sentido de que cualquier otra factorización sólo puede diferir en el orden de los factores.

Ejemplo 1: Si $K = \mathbb{C}[X]$, los únicos polinomios irreducibles son los lineales, y se obtiene la factorización dada por el teorema 11.1.

Ejemplo 2: Si $K = \mathbb{R}[X]$, los polinomios irreducibles son los lineales, y los cuadráticos de discriminante negativo; y se obtiene la factorización dada por el teorema 12.1.

Si $K = \mathbb{Q}$, no se dispone de una caracterización sencilla de qué polinomios son irreducibles.

16. Relaciones entre coeficientes y raíces

Consideremos nuevamente un polinomio cuadrático $P(X) = aX^2 + bX + c \in \mathbb{C}[X]$, y llamemos α_1, α_2 a sus raíces. Entonces sabemos que P admite la factorización:

$$P(X) = a(X - \alpha_1)(X - \alpha_2)$$

Si efectuamos el producto utilizando la propiedad distributiva, obtenemos que:

$$P(X) = a(X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2)$$

Igualando los coeficientes, obtenemos las siguientes relaciones entre coeficientes y raíces:

$$\alpha_1 + \alpha_2 = -\frac{b}{a}$$

$$\alpha_1\alpha_2 = \frac{c}{a}$$

Ahora generalizaremos este hecho para polinomios de mayor grado: empecemos considerando un polinomio cúbico:

$$P(X) = a_3X^3 + a_2X^2 + a_1X + a_0$$

y llamemos α_1, α_2, α_3 a sus raíces, de modo que P admite la factorización:

$$P(X) = a(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

Efectuando la distributiva tenemos que:

$$P(X) = a(X^3 - S_1X^2 + S_2X - S_3)$$

siendo

$$S_1 = \alpha_1 + \alpha_2 + \alpha_3$$

$$S_2 = \alpha_1\alpha_2 + \alpha_1\alpha_2 + \alpha_2\alpha_3$$

$$S_3 = \alpha_1\alpha_2\alpha_3$$

e igulando los coeficientes obtenemos que:

$$S_1 = -\frac{a_2}{a_3}$$

$$S_2 = \frac{a_1}{a_3}$$

$$S_3 = -\frac{a_0}{a_3}$$

Podemos generalizar este hecho, para polinomios de grado arbitrario del siguiente modo. Sea $P \in \mathbb{C}[X]$ un polinomio de grado n

$$P(X) = \sum_{i=0}^{n} a_i X^i \ (a_n \neq 0)$$

y llamemos a $\alpha_1, \alpha_2, \ldots, \alpha_n$ a sus n raíces en $\mathbb{C}$, donde repetimos cada raíz tantas veces como indique su multiplicidad. Entonces, el polinomio P admite la factorización:

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n)$$

Efectuamos ahora la distributiva. Para ello, notamos que el término en X^k en este producto se debe formar sumando todos los productos que se obtienen eligiendo el término "X" en k de los factores, y el término "$-\alpha_i$" en $n - k$ de los factores. Es decir que el coeficiente de X^k debe ser:

$$(-1)^{n-k} S_{n-k}$$

donde notamos por S_k a la suma de todas los productos que se puedan formar considerando k de las n raíces $\alpha_1, \alpha_2, \ldots, \alpha_n$. Es decir que:

$$S_k = S_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i_1, i_2, \ldots, i_k} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$$

donde $1 \leq i_1, i_2, \ldots, i_k \leq n$, y los índices $i_1, i_2, \ldots, i_k$ son todos distintos.

Por ejemplo:

$$S_n = \alpha_1 \alpha_2 \ldots \alpha_n$$

es el producto de todas las raíces.

$$S_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n$$

es la suma de todas las raíces. Y

$$S_2 = \sum_{i<j} \alpha_i \alpha_j$$

es la suma de todos los posibles productos de dos de las raíces.

Las funciones S_k son polinomios en varias variables (de grado k), en las variables $\alpha_1, \alpha_2, \ldots, \alpha_n$. Y tienen la propiedad de que su valor no cambia si permutamos en cualquier orden las raíces (son polinomios simétricos). Reciben el nombre de **funciones simétricas elementales**.

Entonces tenemos:

$$P(X) = a_n \sum_{k=0}^{n} (-1)^{n-k} S_{n-k} X^k \tag{3}$$

de donde, igualando los coeficiente, obtenemos la siguiente fórmula que relaciona los coeficientes del polinomio P con las funciones simétricas elementales de sus raíces:

$$S_{n-k} = (-1)^{n-k} \frac{a_k}{a_n}$$

En particular para la suma de las raíces tenemos (tomando $k = n - 1$)que:

$$S_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n = -\frac{a_{n-1}}{a_0} \tag{4}$$

y para el producto (tomando $k = 0$) que:

$$S_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n = (-1)^n \frac{a_0}{a_n}$$

Ejemplo: Notemos que (por su definición) hay exactamente $\binom{n}{k}$ términos en la suma S_k. Si tomamos como P el polinomio

$$P = (X - \alpha)^n$$

(Es decir elegimos las n raíces iguales a α), tendremos que:

$$S_k = \binom{n}{k}\alpha^k$$

y como $a_n = 1$ la fórmula (3) nos da que:

$$(X-\alpha)^n = \sum_{k=0}^{n}(-1)^{n-k}\alpha^{n-k}X^k$$

Es decir, que se obtiene como caso particular la fórmula del binomio de Newton.

Las funciones simétricas elementales pueden utilizarse para calcular otras funciones simétricas de las raíces. Por ejemplo, conisderemos la suma de los cuadrados de las raíces:

$$C = \sum_{i=1}^{n}\alpha_i^2$$

Esta expresión C es un polinomio simétrico en $\alpha_1, \alpha_2, \ldots, \alpha_n$ de grado 2.

Podemos expresar a este polinomio C en términos de S_1 y S_2 como sigue:

$$S_1^2 = \left(\sum_{i=1}^{n}\alpha_i\right)^2 = \sum_{i=1}^{n}\alpha_i^2 + 2\sum_{1\leq i<j\leq n}\alpha_i\alpha_j = C + 2S_2$$

En consecuncia,

$$C = S_1^2 - 2S_2$$

y por lo tanto C puede expresarse en función de los coeficientes del polinomio P:

$$C = \frac{a_{n-1}^2}{a_n^2} - 2\frac{a_{n-2}}{a_n}$$

En general, es posible probar que cualquier función polinomial simétrica de las raíces puede expresarse en función de las funcions simétricas elementales S_i, y por consiguiente como una función racional[13] de los coeficientes del polinomio P.

16.1. Aplicación a las raíces de la unidad

Los resultados de la sección anterior tienen utilidad para calcular la suma y el producto de las raíces n-ésimas de la unidad [14] de una forma sencilla, ya

[13] Una función racional es un cociente de polinomios.

[14] Ejercicio 18 de la práctica 6

que dichas raíces n-ésimas son exactamente las raíces del polinomio $X^n - 1$ (ver ecuación (1). Y se tiene

$$S_1 = \omega_0 + \omega_1 + \ldots + \omega_{n-1} = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases} \tag{5}$$

Más difícil, resulta calcular la suma de las raíces primitivas n-ésimas[15]. Una manera de hacerlo, es la siguiente: llamemos $f(n)$ a la suma de las raíces primitivas n-ésimas de la unidad.

Si notamos por G_n al conjunto de las raíces n-ésimas, y por G_n^* al de las raíces n-ésimas primitivas, recordamos que tenemos la descomposición de G_n como unión disjunta:

$$G_n = \bigcup_{d|n} G_d^* \tag{6}$$

En consecuencia, teniendo en cuenta la ecuación (5):

$$\sum_{d|n} f(d) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad n > 1 \end{cases} \tag{7}$$

Esta relación permite calcular recursivamente los valores de $f(n)$: hagámoslo por ejemplo en los casos que aparence en el ejercicio 19 de la práctica 6:

$$\begin{gathered} f(1) = 0 \\ f(1) + f(2) = 0 \;\Rightarrow\; f(2) = -1 \\ f(1) + f(3) = 0 \;\Rightarrow\; f(3) = -1 \\ f(1) + f(2) + f(4) = 0 \;\Rightarrow\; f(4) = 0 \\ f(1) + f(2) + f(4) + f(8) = 0 \;\Rightarrow\; f(8) = 0 \\ f(1) + f(5) = 0 \;\Rightarrow\; f(5) = -1 \\ f(1) + f(3) + f(5) + f(15) = 0 \;\Rightarrow\; f(15) = 1 \end{gathered}$$

Ejercicio: Probar que f coincide con la función μ de Möbius, definida en uno de los ejercicios del final de la apunte de enteros por:

[15] ver ejercicio 19 de la práctica 6

$$\mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ 0 & \text{si} \quad \text{si } n \text{ es divisible por el cuadrado de algún primo} \\ (-1)^k & \text{si} \quad n = p_1 p_2 \dots p_k \text{ siendo los } p_i \text{ primos distintos} \end{cases}$$

Sugerencia: Recordar que, de acuerdo al citado ejercicio, μ también satisface la relación (7). A partir de allí, es fácil probar por inducción que $f(n) = \mu(n)$ para todo $n \in \mathbb{N}$.

A. Polinomios y raíces primitivas de la unidad

Para algunas cuestiones[16], es conveniente conocer qué ecuación satisfacen las raíces de primitivas la unidad. Definamos el polinomio[17] $\Phi_n(X)$ como el polinomio mónico cuyas raíces son exactamente las raíces primitivas n-ésimas de la unidad:

$$\Phi_n(X) = \prod_{\omega_k \in G_n^*} (X - \omega_k)$$

Por ejemplo:

$$\Phi_1(X) = X - 1$$
$$\Phi_2(X) = X + 1$$
$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1$$

También anteriormente vimos que las raíces cúbicas primitivas de la unidad, son raíces de

$$\Phi_3(X) = X^2 + X + 1$$

y que las raíces primitivas sextas de la unidad son raíces de

$$\Phi_6(X) = X^2 - X + 1$$

[16]Este tema es extra a la materia, pero proporciona algunas herramientas que pueden ser útiles en ejercicios relacionados con raciones primitivas de la unidad, y conecta este tema con el de polinomios.

[17]$\Phi_n(X)$ se conoce como el n-ésimo polinomio ciclotómico.

En general, la relación (6), proporciona la factorización:

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{8}$$

Por ejemplo, antes encontramos la factorización:

$$X^6-1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1) = \phi_1(X)\phi_2(X)\phi_3(X)\phi_6(X)$$

que proviene de la descomposición:

$$G_6 = G_1^* \cup G_2^* \cup G_3^* \cup G_6^*$$

de G_6; o por ejemplo, si $n = 4$, tenemos la factorización

$$X^4 - 1 = (X-1)(X+1)(X^2+1) = \phi_1(X)\phi_2(X)\phi_4(X)$$

que corresponde a la descomposición:

$$G_4 = G_1^* \cup G_2^* \cup G_4^*$$

Los polinomios $\Phi_n(X)$ se pueden calcular recursivamente a partir de la relación (8). Por ejemplo, calculemos $\Phi_5(X)$ y $\Phi_{15}(X)$. Como

$$X^5 - 1 = \phi_1(X)\phi_5(X)$$

tenemos, efectuando la división de polinomios que que:

$$\Phi_5(X) = \frac{X^5-1}{X-1} = X^4 + X^3 + X^2 + X + 1$$

y como

$$X^{15} - 1 = \Phi_1(X)\Phi_3(X)\Phi_5(X)\Phi_{15}(X) = (X^5-1)(X^2+X+1)\Phi_{15}(X)$$

tenemos que:

$$\Phi_{15}(X) = \frac{X^{15}-1}{(X^5-1)(X^2+X+1)} = \frac{X^{10}+X+1}{X^2+X+1}$$

y efectuando la división de polinomios, finalmente encontramos que:

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

Se puede demostrar (por inducción a partir de 8) que $\Phi_n(X)$ es siempre un polinomio con coeficientes enteros.

Como sabemos que hay exactamente $\varphi(n)$ raíces primitivas de la unidad (siendo φ la función de Euler), deducimos que el grado del polinomio $\Phi_n(X)$ es exactamente $\varphi(n)$.

Resumiendo, podemos hacer una pequeña tabla de los polinomios Φ_n que hemos calculado:

n	$\Phi_n(X)$
1	$X - 1$
2	$X + 1$
3	$X^2 + X + 1$
4	$X^2 + 1$
5	$X^4 + X^3 + X^2 + X + 1$
6	$X^2 - X + 1$
15	$X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$

Ejercicio: Completar la tabla de los valores de $\Phi_n(X)$ para $n \leq 15$, y usarlos para resolver por ejemplo el ejercicio 19 de la práctica 6 de otra manera, a partir de la relación (4).

Referencias

[1] G. Birkoff, S. Mc. Lane. Álgebra Moderna.

[2] J. Rey Pastor, P. Pi Calleja. C. A. Trejo. Análisis Matemático. Volumen I. Capítulo IV ("Algoritmo Algebraico"). Octava edición, julio de 1969.

[3] R. Courant, H. Robbins, ¿Qué es la matemática?. Editorial Aguilar, 1964.