Polinomios

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Parte I

Introducción

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 (real o complejo) 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.

Introducción (2)

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.

Introducción (3)

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:

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

$$P(X) = \left(X - \frac{5}{2} - \frac{1}{2}\right)\left(X - \frac{5}{2} + \frac{1}{2}\right) = (X - 2)(X - 3)$$

Introducción (4)

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 conexión entre el problema de encontrar los ceros o raíces de un polinomio, y el problema de factorizarlo. Exploraremos esta conexión más en detalle en lo sucesivo. ´

Parte II

Algunas definiciones del álgebra abstracta

Distintos tipos de polinomios

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

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

Anillos

Para poder tratar todos estos casos de una manera unificada, utilizaremos la la estructura algebraica de anillo conmutativo. Recordamos que informalmente, un anillo es un conjunto A en el que están definidas de alguna manera las operaciones de suma, resta, producto y multiplicación, y satisfacen las reglas usuales.

Definición formal de anillo

Un anillo es un conjunto A donde están definidas dos operaciones

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

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

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

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

Definición de anillo (2)

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

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

2. 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:

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

3. Propiedad asociativa del producto

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

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

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

Definición formal de anillo (3)

1. 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.
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).

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.

Dominios íntegros

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

Definición

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).

Notemos que esta fue la propiedad clave que usamos en el razonamiento que hicimos al comienzo sobre la relación entre factorizar un polinomio y encontrar sus raíces.

Cuerpos

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

Definición

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).

Definiciones sobre polinomios

Un polinomio en una variable (o indeterminada) X con coeficientes en un anillo conmutativo A es una expresión formal de la forma

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

donde los $a_k \in A$ son ciertos coeficientes.
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 $\mathrm{gr}(P)$ al grado de P.
El polinomio nulo es el polinomio especial donde todos los a_k son 0. El grado de un polinomio nulo no está definido.
Si $a_n = 1$ diremos que P es un polinomio mónico.
Por ejemplo,

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

es un polinomio mónico con coeficientes en $\mathbb{Z}$ de grado 3.
Notamos $A[X]$ al conjunto de todos los posibles polinomios en la indeterminada X con coeficientes en el anillo A.

Algunos ejemplos

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

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

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

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

Naturalmente,

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

Igualdad de polinomios

Convenimos en decir que dos polinomos:

$$P = \sum_{i=0}^{n} a_i\, X^i, \quad Q = \sum_{i=0}^{m} b_i\, X^i$$

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:

$$P = 0X^3 + 3X^2 + 2X + 1, \quad Q = 3X^2 + 2X + 1$$

Polinomios constantes

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.

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.

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

Evaluación de polinomios (2)

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.

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

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

Suma y resta de polinomios (2)

Si P y Q son dos polinomios:

$$P = \sum_{i=0}^{m} a_i X^i, \quad Q = \sum_{i=0}^{n} b_i X^i$$

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

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

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

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

Suma y resta de polinomios (3)

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

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:

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

Producto de polinomios (2)

Consideremos dos polinomios,

$$P = \sum_{j=0}^{m} a_j \cdot x^j, \quad Q = \sum_{k=0}^{n} b_k \cdot x^k$$

El producto entre ellos se define usando la propiedad distributiva

$$P \cdot Q = \sum_{j=0}^{m} \sum_{k=0}^{n} a_j \cdot b_k x^j x^k$$

Si agrupamos los términos que tienen el mismo exponente $j + k = r$, nos queda

$$P \cdot Q = \sum_{r=0}^{n+m} c_r x^r$$

donde

$$c_r = \sum_{\substack{0 \leq j \leq m, 0 \leq k \leq n \\ j+k=r}} a_j \cdot b_k = \sum_{j=0}^{r} a_j \cdot b_{r-j}$$

Producto de polinomios (3)

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 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:

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

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

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 $\frac{-b}{a}$.

Raíces de un polinomio cuadrático

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 [1]:

Primero sacamos a como factor común:

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

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

o sea:

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

[1] Siempre que $1 + 1 \neq 0$ en K

Raíces de un polinomio cuadrático (2)

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

$$X^2 = \Delta$$

(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:

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

y factorizarlo como:

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

O sea:

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

Raíces de un polinomio cuadrático (3)

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 $K = \mathbb{R}$.

Raíces de un polinomio en general

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 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.

Raíces reales de un polinomio de grado impar

Teorema

Si $P \in \mathbb{R}[X]$ es un polinomio de grado impar, P tiene alguna raíz real.

Demostración.

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 $P(\alpha) = 0$. □

Otros ejemplos

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

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

Otros ejemplos (2)

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

$$X-1 \equiv 0 (\text{mod } 5) \quad \text{o} \quad X+1 \equiv 0 (\text{mod } 5) \Leftrightarrow X \equiv 1 \vee X \equiv -1 \equiv 4 \ (\text{mod } 5)$$

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

Otros ejemplos (3)

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

$$X^2 \equiv 1 \quad (\text{mód } 8)$$

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

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

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:

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

Divisibilidad de polinomios (2)

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

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.

Divisibilidad de polinomios (3)

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.

Divisibilidad de polinomios (4)

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 $\mathbb{Z}$.

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.

El algoritmo de división para polinomios

Teorema

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 $gr(R) < gr(D)$.

Demostración

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 $R = P$.

Demostración (2)

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.

Demostración (3)

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:

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