Capítulo 4: Polinomios

Miguel Ángel Olalla Acosta
miguelolalla@us.es

Departamento de Álgebra
Universidad de Sevilla

Enero de 2015

Contenido

1. Introducción a los polinomios
2. Divisibilidad
3. Máximo común divisor
4. Factorización en $\mathbb{Q}[x]$
5. Factorización en $\mathbb{Z}/\mathbb{Z}p[x]$

Definición de polinomio

Definición (Polinomio)

Sea A un anillo, un **polinomio con coeficientes en** *A es una expresión de la forma*

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \text{ con } a_i \in A.$$

Dos polinomios son iguales si lo son coeficiente a coeficiente.
Se denota por $A[x]$ al conjunto de todos los polinomios cuyos coeficientes son elementos de A.

Grado de un polinomio

Definición (Grado)

El grado de un polinomio $a(x)$*, notado* $\text{grado}(a(x))$*, es el mayor entero* n *tal que* $a_n \neq 0$*. El polinomio cuyos coeficientes son todos nulos se llama* **polinomio nulo** *y se denota por* 0*. Por convención el grado del polinomio nulo es* $\text{grado}(0) = -\infty$*.*

Algunas definiciones

Notación

Sea $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$ *con* $a_n \neq 0$. *Llamaremos* **término líder** *de* $a(x)$ *al término* $a_n x^n$, **coeficiente líder** *a* a_n *y* **término constante** *a* a_0. *Un polinomio se dice* **mónico** *si su coeficiente líder es 1. El polinomio* $a(x)$ *se dice* **constante** *si es* $a(x) = a_0$, *es decir, si es nulo o de grado 0.*

El anillo $A[x]$

Teorema

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

- *Si A es un anillo conmutativo, $A[x]$ es conmutativo.*
- *Si A es un anillo con elemento unidad, $A[x]$ tiene elemento unidad.*
- *Si A es dominio de integridad, $A[x]$ es dominio de integridad.*

Unidades de $A[x]$

Teorema

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

División euclídea de polinomios

Teorema (Teorema de división)

Sea k un cuerpo y sean $f(x)$ y $g(x)$ dos polinomios de $k[x]$, con $g(x) \neq 0$. Entonces existen dos únicos polinomios $q(x)$ y $r(x)$ tales que

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

y $\text{grado}(r(x)) < \text{grado}(g(x))$.

Corolario (Teorema del resto)

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

Divisibilidad

Definición (Divisibilidad)

Sean $f(x)$ y $g(X)$ dos polinomios de $A[x]$, decimos que $g(x)$ **divide a** *$f(x)$, y lo escribimos $g(x)|f(x)$ si existe un polinomio $h(x)$ tal que $f(x) = g(x) \cdot h(x)$.*

Observación

- *Un polinomio divide a cualquier polinomio no nulo de $k[x]$ si y sólo si es una constante no nula.*
- *En $k[x]$ $g(x)|f(x)$ si y sólo si el resto de dividir $f(x)$ entre $g(x)$ es nulo.*
- *En $k[x]$, si $g(x)|f(x)$ y $f(x)|g(x)$ entonces* $\text{grado}(f(x)) = \text{grado}(g(x))$ *y $f(x) = a \cdot g(x)$ donde $a \in k \setminus \{0\}$ es una constante no nula.*

Raíz de un polinomio

Definición (Raíz de un polinomio)

Se dice que un elemento $a \in A$ es raíz del polinomio $f(x) \in A[x]$ si $f(a) = 0$. es decir, si al sustituir x por a en $f(x)$ se obtiene el valor 0.

Corolario (Teorema de la raíz)

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

Definición (Multiplicidad de una raíz)

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

Corolario (D'Alembert)

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

Máximo común divisor

Definición (Máximo común divisor)

Sean $f(x)$ y $g(x)$ dos polinomios con coeficientes en k. Un polinomio $d(x) \in k[x]$ se dice que es un **máximo común divisor** *de $f(x)$ y $g(x)$, y se escribe $d(x) = \mathrm{mcd}(f(x), g(x))$, si verifica:*

1. *$d(x)|f(x)$ y $d(x)|g(x)$.*
2. *Si $e(x)$ es otro polinomio que divide a $f(x)$ y a $g(x)$ entonces $e(x)|d(x)$.*

Proposición

El máximo común divisor de dos polinomios es único salvo producto por constantes no nulas.

Máximo común divisor

Algoritmo (de Euclides)

Sean $f(x)$ *y* $g(x)$ *dos polinomios no nulos con* $\text{grado}(f(x)) \geq \text{grado}(g(x))$. *Entonces, haciendo divisiones sucesivas se obtiene:*

$$\begin{array}{rcll}
f(x) & = & q(x)\cdot g(x) + r(x) & \text{grado}(r(x)) < \text{grado}(g(x)) \\
g(x) & = & q_0(x)\cdot r(x) + r_1(x) & \textit{grado}(r_1(x)) < \text{grado}(r(x)) \\
r(x) & = & q_1(x)\cdot r_1(x) + r_2(x) & \textit{grado}(r_2(x)) < \text{grado}(r_1(x)) \\
 & \vdots & & \\
r_{n-2}(x) & = & q_{n-1}(x)\cdot r_{n-1}(x) + r_n(x) & \textit{grado}(r_n(x)) < \text{grado}(r_{n-1}(x)) \\
r_{n-1}(x) & = & q_n(x)\cdot r_n(x). &
\end{array}$$

Este proceso es finito y $\text{mcd}(f(x), g(x)) = r_n(x)$. *Es decir, el máximo común divisor de dos polinomios siempre existe.*

Identidad de Bézout

Teorema (Identidad de Bézout)

Sean $f(x)$ y $g(x)$ dos polinomios de $k[x]$ no nulos y sea $d(x) = \mathrm{mcd}(f(x), g(x))$. Entonces existen unos polinomios $a(x), b(x) \in k[x]$ tales que

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

Polinomio irreducible

Definición (Polinomio irreducible)

Un polinomio no nulo $p(x) \in k[x]$ se dice **irreducible** *si no puede descomponerse como producto de dos polinomios no constantes.*

Si $p(x) \in k[x]$ es un polinomio irreducible y $p(x) = f(x) \cdot g(x)$ entonces uno de los dos factores es constante.

Todo polinomio de grado 1 es irreducible.
Un polinomio de $k[x]$ de grado 2 o 3 es irreducible si no tiene raíces en k.

Raíces en $\mathbb{Q}[x]$

Calcular las raíces de un polinomio $f(x) \in \mathbb{Q}[x]$ es equivalente a buscar las de cualquier polinomio $a \cdot f(x)$ con $a \in \mathbb{Z} \setminus \{0\}$. En particular podremos suponer que, a efectos del cálculo de raíces, el polinomio $f(x)$ está en $\mathbb{Z}[x]$ (es decir, todos sus coeficientes son enteros).

Proposición (Regla de Ruffini)

Sea el polinomio

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

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

Lema de Gauss

Definición (Contenido de un polinomio)

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

Teorema (Lema de Gauss)

El producto de dos polinomios primitivos es un polinomio primitivo.

Lema de Gauss

Corolario (4.4.2)

Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado $n > 0$ que se descompone, en $\mathbb{Q}[x]$, en producto de dos polinomios no constantes. Entonces $f(x)$ se descompone en $\mathbb{Z}[x]$ como producto de dos polinomios de esos mismos grados

Corolario (4.4.3)

Sea $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo de grado $n > 0$. Entonces $f(x)$ es reducible en $\mathbb{Z}[x]$ si y sólo si lo es en $\mathbb{Q}[x]$.

Criterio de Eisenstein

Proposición (Criterio de Eisenstein)

Sea $f(x)$ un polinomio de grado $n > 0$ con coeficientes enteros

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

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

Reducción a polinomios primitivos

El estudio de la irreducibilidad de polinomios en $\mathbb{Q}[x]$ se puede reducir al de polinomios primitivos con coeficientes enteros:

- **Primera reducción:** Para todo polinomio $f(x) \in \mathbb{Q}[x]$ existe un $d \in \mathbb{Z}$ tal que $d \cdot f(x) = h(x)$ es un polinomio con coeficientes enteros. Para obtener la descomposición de $f(x)$ basta calcular la de $h(x)$. Luego podemos considerar sólo polinomios con coeficientes enteros.
- **Segunda reducción:** Sea $f(x) \in \mathbb{Z}[x]$. Sabemos que $f(x) = c(f) \cdot h(x)$, donde $h(x) \in \mathbb{Z}[x]$ es primitivo. Para obtener la descomposición de $f(x)$ en $\mathbb{Q}[x]$ es suficiente calcular la de $h(x)$. Así que podemos considerar sólo polinomios con coeficientes enteros y primitivos.

Factorización en $\mathbb{Z}/\mathbb{Z}p[x]$

Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ un polinomio primitivo. Si $\overline{a_i} = a_i + \mathbb{Z}p \in \mathbb{Z}/\mathbb{Z}p$, pondremos

$$\overline{f}(x) = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}/\mathbb{Z}p[x].$$

Proposición (3.7.2)

Sea p **un primo que no divida a** *a_n. Si $\overline{f}(x)$ es irreducible en $\mathbb{Z}/\mathbb{Z}p[x]$ entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.*

Ejemplo (El recíproco no es cierto)

$f(x) = x^2 + 2$ es irreducible en $\mathbb{Q}[x]$ pero $\overline{f}(x) = x^2$ es reducible en $\mathbb{Z}/\mathbb{Z}2[x]$.