Capítulo 4: Polinomios

Miguel Ángel Olalla Acosta
miguelolalla@us.es

Departamento de Álgebra
Universidad de Sevilla

Diciembre de 2017

Contenido

Ejemplo 1

a) Consideremos el polinomio $f(x) = x^4 + 2x^3 - x^2 + x - 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Ejemplo 1

a) Consideremos el polinomio $f(x) = x^4 + 2x^3 - x^2 + x - 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Las posibles raíces de $f(x)$ son ± 1, ± 2. No tiene raíces ni es producto de dos polinomios de grado 2, luego **es irreducible**.

Ejemplo 1

a) Consideremos el polinomio $f(x) = x^4 + 2x^3 - x^2 + x - 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Las posibles raíces de $f(x)$ son ± 1, ± 2. No tiene raíces ni es producto de dos polinomios de grado 2, luego **es irreducible**.

b) Consideremos ahora el mismo polinomio sobre $\mathbb{F}_3[x]$. Pongamos $\overline{f}(x) = x^4 + 2x^3 + 2x^2 + x + 1$ ¿es irreducible en $\mathbb{F}_3[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Ejemplo 1

a) Consideremos el polinomio $f(x) = x^4 + 2x^3 - x^2 + x - 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Las posibles raíces de $f(x)$ son ± 1, ± 2. No tiene raíces ni es producto de dos polinomios de grado 2, luego **es irreducible**.

b) Consideremos ahora el mismo polinomio sobre $\mathbb{F}_3[x]$. Pongamos $\overline{f}(x) = x^4 + 2x^3 + 2x^2 + x + 1$ ¿es irreducible en $\mathbb{F}_3[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

No tiene raíces entre los elementos de $\mathbb{F}_3 = \{0, 1, 2\}$ pero sí es producto de dos polinomios de grado 2, luego $\overline{f}(x) = (x^2 + x + 2)^2$ **es reducible**.

Ejemplo 2

a) Consideremos el polinomio $f(x) = x^4 + 3x^3 + 5x^2 + 4x + 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Ejemplo 2

a) Consideremos el polinomio $f(x) = x^4 + 3x^3 + 5x^2 + 4x + 2 \in \mathbb{Z}[x]$. ¿Es irreducible en $\mathbb{Z}[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Las posibles raíces de $f(x)$ son ± 1, ± 2. No tiene raíces pero sí es producto de dos polinomios de grado 2, luego $f(x) = (x^2 + x + 1)(x^2 + 2x + 2)$ **es reducible**.

Ejemplo 2

b) Consideremos ahora el mismo polinomio sobre $\mathbb{F}_5[x]$. Pongamos $\overline{f}(x) = x^4 + 3x^3 + 4x + 2$ ¿es irreducible en $\mathbb{F}_5[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

Ejemplo 2

b) Consideremos ahora el mismo polinomio sobre $\mathbb{F}_5[x]$. Pongamos $\overline{f}(x) = x^4 + 3x^3 + 4x + 2$ ¿es irreducible en $\mathbb{F}_5[x]$? En caso negativo descomponerlo como producto de polinomios irreducibles.

En un primer paso, podemos trasladar la factorización sobre $\mathbb{Z}$ a este caso. Es decir, $\overline{f}(x) = (x^2 + x + 1)(x^2 + 2x + 2)$ también en $\mathbb{F}_5[x]$. Además el segundo factor tiene raíces 1 y 2, el primer factor no tiene raíces entre los elementos de $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Luego $\overline{f}(x) = (x^2 + x + 1)(x + 4)(x + 3)$ en $\mathbb{F}_5[x]$.

Ejemplo 3

a) Sea el polinomio $f(x) = x^6 - 2x^5 + x^4 + 2x^3 - 8x^2 + 12x - 12$, Sabiendo que $\alpha = 1 + i$ es una raíz de $f(x)$, descomponerlo en factores irreducibles sobre $\mathbb{Z}$, $\mathbb{R}$ y $\mathbb{C}$.

Ejemplo 3

a) Sea el polinomio $f(x) = x^6 - 2x^5 + x^4 + 2x^3 - 8x^2 + 12x - 12$, Sabiendo que $\alpha = 1 + i$ es una raíz de $f(x)$, descomponerlo en factores irreducibles sobre $\mathbb{Z}$, $\mathbb{R}$ y $\mathbb{C}$.

Sabemos que si $\alpha = a + ib \in \mathbb{C} \setminus \mathbb{R}$ es raíz de $f(x)$ entonces $\overline{\alpha} = a - ib$ también. Además $\alpha + \overline{\alpha} = 2a \in \mathbb{R}$ y $\alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{R}$. Luego el polinomio **real** $(x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$ es un factor de $f(x)$.

Ejemplo 3

En nuestro caso $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2x + 2$ es un factor de $f(x)$. Dividiendo se tiene $f(x) = (x^2 - 2x + 2)(x^4 - x^2 - 6)$. El segundo factor es bicuadrado y es fácil descomponerlo como producto de dos polinomios de grado dos, quedando $f(x) = (x^2 - 2x + 2)(x^2 + 3)(x^2 - 2)$. Como $f(x)$ no tiene raíces enteras, esa es su descomposición en factores irreducibles sobre $\mathbb{Z}$.

Ejemplo 3

Las raíces de cada uno de los tres factores son, respectivamente, $1+i$ y $1-i$, $\pm\sqrt{3}i$, $\pm\sqrt{2}$. Las cuatro primeras son raíces complejas no reales, pero $\pm\sqrt{2} \in \mathbb{R}$. Luego la factorización de $f(x)$ sobre $\mathbb{R}$ es $f(x) = (x^2 - 2x + 2)(x^2 + 3)(x + \sqrt{2})(x - \sqrt{2})$.

Ejemplo 3

Las raíces de cada uno de los tres factores son, respectivamente, $1+i$ y $1-i$, $\pm\sqrt{3}i$, $\pm\sqrt{2}$. Las cuatro primeras son raíces complejas no reales, pero $\pm\sqrt{2} \in \mathbb{R}$. Luego la factorización de $f(x)$ sobre $\mathbb{R}$ es $f(x) = (x^2 - 2x + 2)(x^2 + 3)(x + \sqrt{2})(x - \sqrt{2})$.

Por último, el polinomio $f(x)$ de grado 6 se descompone en otros tantos factores sobre $\mathbb{C}$:
$f(x) = (x - (i + i))(x - (1 - i))(x + \sqrt{3}i)(x - \sqrt{3}i)(x + \sqrt{2})(x - \sqrt{2})$.

Definición de polinomio

Definición (Polinomios con coeficientes en A)

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

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

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

Grado 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, su grado es* $grado(0) = -\infty$*.*

Algunas definiciones

Definición

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

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 dominio de integridad, $A[x]$ es dominio de integridad.*

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 dominio de integridad, $A[x]$ es dominio de integridad.*

Observación

Sean los polinomios $a(x) = \sum_{i=0}^{n} a_i x^i$ y $b(x) = \sum_{i=0}^{m} b_i x^i$. Entonces:

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

Unidades de $A[x]$

Teorema

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

División euclídea de polinomios

Teorema (Teorema de división)

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

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

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

Algoritmo de división

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

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

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

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

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

Ejemplo de división

Dividir el polinomio $f(x) = x^6 - 7x^2 + 6$ entre $g(x) = x^4 + 4x^2 + 3$ en $\mathbb{Q}[x]$:

$$\begin{array}{rrr|l} x^6 & -7x^2 & +6 & = \left(x^4 + 4x^2 + 3\right)\left(x^2 - 4\right) + 6x^2 + 18 \\ -x^6 - 4x^4 & -3x^2 & & \\ \hline & -4x^4 - 10x^2 & +6 & \\ & 4x^4 + 16x^2 & +12 & \\ \hline & & 6x^2 + 18 & \end{array}$$

División euclídea de polinomios

Corolario (4.2.2)

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

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

División euclídea de polinomios

Corolario (4.2.2)

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

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

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 $f(x) = g(x) \cdot h(x)$.*

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.*

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.*

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.

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 $x - a$.*

Multiplicidad de una raíz

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 $f(x)$.

Multiplicidad de una raíz

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

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

Máximo común divisor

Observación (Nota 4.3.1)

El máximo común divisor de dos polinomios no es único. Si $p(x) = mcd(f(x), g(x))$, *entonces, para cualquier* $a \in k \setminus \{0\}$, $ap(x) = mcd(f(x), g(x))$.

Máximo común divisor

Observación (Nota 4.3.1)

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

Máximo común divisor

Proposición (4.3.2)

Sean $f(x), g(x) \in k[x]$ *dos polinomios. Si* $f(x) = q(x)g(x) + r(x)$, *entonces se tiene que*

$$\mathrm{mcd}(f(x), g(x)) = \mathrm{mcd}(g(x), r(x))$$

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:*

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:*

$$f(x) = q(x) \cdot g(x) + r(x) \qquad \text{grado}(r(x)) < \text{grado}(g(x))$$

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:*

$$\begin{array}{lcll} f(x) & = & q(x) \cdot g(x) + r(x) & \text{grado}(r(x)) < \text{grado}(g(x)) \\ g(x) & = & q_0(x) \cdot r(x) + r_1(x) & \textit{grado}(r_1(x)) < \text{grado}(r(x)) \end{array}$$

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:*

$$\begin{array}{rcll} f(x) & = & q(x) \cdot g(x) + r(x) & \text{grado}(r(x)) < \text{grado}(g(x)) \\ g(x) & = & q_0(x) \cdot r(x) + r_1(x) & \textit{grado}(r_1(x)) < \text{grado}(r(x)) \\ r(x) & = & q_1(x) \cdot r_1(x) + r_2(x) & \textit{grado}(r_2(x)) < \text{grado}(r_1(x)) \\ & \vdots & & \end{array}$$

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:*

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

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:*

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

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, con las notaciones anteriores, $\text{mcd}(f(x), g(x)) = r_n(x)$.

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

Polinomio irreducible

Definición (Polinomio irreducible)

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

Proposición (4.4.1)

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

Irreducibilidad

Proposición (Teorema de Euclides)

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

Irreducibilidad

Teorema (Descomposición en factores irreducibles)

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

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

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

Irreducibilidad

Proposición (4.4.3)

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

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

Derivada de un polinomio

Notación

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

Derivada de un polinomio

Notación

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

Definición (Derivada de un polinomio)

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

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

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

Propiedades de la derivada de polinomios

Proposición (4.4.4)

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

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

Factores múltiples de un polinomio

Teorema (Factores múltiples de un polinomio)

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

Factores múltiples de un polinomio

Teorema (Factores múltiples de un polinomio)

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

Observación (Nota 4.4.5)

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

Teorema fundamental del álgebra

Teorema (Teorema fundamental del álgebra)

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

Teorema fundamental del álgebra

Teorema (Teorema fundamental del álgebra)

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

Corolario (4.5.1)

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

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

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

Factorización en $\mathbb{R}[x]$

Proposición (4.5.2)

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

Polinomios de grado 2 o 3

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

Polinomios de grado 2 o 3

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

Naturalmente, lo anterior no funciona para grados mayores. Un polinomio de grado 4 se puede descomponer, por ejemplo, en dos factores irreducibles de grado 2, como $x^4 + 3x^2 + 2 = (x^2 + 2)(x^2 + 1)$ en $\mathbb{Q}$, luego no tiene por qué tener raíces en k

Regla de Ruffini

Proposición (4.6.1)

Sea el polinomio

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

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

Lema de Gauss

Definición (Contenido de un polinomio)

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

Lema de Gauss

Definición (Contenido de un polinomio)

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

Teorema (Lema de Gauss)

El producto de dos polinomios primitivos es primitivo.

Consecuencias del Lema de Gauss

Corolario (4.6.2)

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

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

Consecuencias del Lema de Gauss

Corolario (4.6.2)

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

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

Corolario (4.6.3)

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

Consecuencias del Lema de Gauss

Corolario (4.6.2)

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

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

Corolario (4.6.3)

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

Corolario (4.6.4)

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

Criterio de Eisenstein-Schönemann

Proposición (Criterio de Eisenstein-Schönemann)

Sea un polinomio de grado $n > 0$

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

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

Una aplicación del criterio de Eisenstein-Schönemann

Ejercicio

Sean k un cuerpo y $f(x) \in k[x]$ un polinomio. Demostrar que $f(x)$ es irreducible si y sólo si lo es $f(x+a)$ para todo $a \in k$.

Una aplicación del criterio de Eisenstein-Schönemann

Ejemplo

Vamos a probar que para cada primo p el polinomio

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$$

es irreducible.

Una aplicación del criterio de Eisenstein-Schönemann

Ejemplo

Vamos a probar que para cada primo p el polinomio

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$$

es irreducible.
Si realizamos el cambio x por $x + 1$ se obtiene el polinomio

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p,$$

cuyos coeficientes, salvo el líder, son divisibles por p y tal que p^2 no divide al término constante.

Una aplicación del criterio de Eisenstein-Schönemann

Ejemplo

Vamos a probar que para cada primo p el polinomio

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$$

es irreducible.
Si realizamos el cambio x por $x + 1$ se obtiene el polinomio

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p,$$

cuyos coeficientes, salvo el líder, son divisibles por p y tal que p^2 no divide al término constante.
Por tanto, en aplicación del criterio de Eisenstein-Schönemann, el polinomio $\Phi_p(x+1)$ es irreducible. Lo que implica, por el ejercicio anterior, que lo es $\Phi_p(x)$ para cada p primo.

Factorización en $\mathbb{F}_p[x]$

Sea

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

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

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

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

Factorización en $\mathbb{F}_p[x]$

Sea

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

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

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

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

Proposición (4.7.2)

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

Ejemplo 4.7.3

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

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

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

Ejemplo 4.7.3

Como otras veces, operando e igualando coeficientes obtenemos el sistema

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

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

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

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

El recíproco no es cierto

Observación (Nota 4.7.4)

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