Tema 8. Polinomios

8.0. Contenido y documentación

H8_Polinomios.pdf

8.1. Grupos, anillos y cuerpos

*Definición. Decimos que $(G, *)$ es un **grupo** si $*$ es una operación asociativa en G, existe un elemento neutro en G para $*$ y para todo $a \in G$ existe un elemento inverso $a^{-1} \in G$.*
Nota. En tal caso se dice que a es **invertible** en G.

*Definición. Decimos que un grupo $(G, *)$ es **conmutativo** o **abelino** si $\forall a, b \in G$ se tiene que $a * b = b * a$.*

*Definición. Decimos que $(A, +, \cdot)$ es un **anillo** si $(A, +)$ es un grupo conmutativo, la operación producto escalar $(\cdot)$ es asociativa en A y se satisfacen las leyes distributivas.*
Nota. Si además la operación producto escalar $(\cdot)$ es conmutativa, decimos que A es un **anillo conmutativo**; y si además, existe un elemento neutro, decimos que A es un **anillo conmutativo unitario**.

8.2. Polinomios

*Definición. Dado un cuerpo K. Definimos un **polinomio** en x con coeficientes en K como una expresión de la forma $p(x) = \sum_{i=0}^{n} a_i x^i$, con $a_i \in K$.*

Definición. Dado un polinomio $p(x)$ definido en un cuerpo K. Si $a_n \neq 0$, decimos que el polinomio tiene grado n.

Notación. $\text{gr}(p) = \partial(p) = n$.

*Definición. Dado un polinomio $p(x)$ definido en un cuerpo K. Decimos que p es un **polinomio mónico** si $a_n = 1$.*

Denotamos por $K[x]$ al conjunto de todos los polinomio con coeficiente en K. Decimos que dos polinomios $p(x), q(x) \in K[x]$ son iguales si y solo si $a_i = b_i$ para todo $i = 0, 1, ..., n$.

8.2.1. Operaciones con polinomios

Dados dos polinomios $p(x), q(x) \in K[x]$, definimos las operaciones suma ($+$) y producto escalar ($\cdot$) como:

1. $p(x) + q(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k$.
2. $p(x)q(x) = \sum_{k=0}^{n+m} C_k x^k$, con $C_k = \sum_{i=0}^{k} a_i b_{k-i}$.

Así, el conjunto $(K[x], +, \cdot)$ es un anillo conmutativo.

> Propiedad. Dados dos polinomios $p(x), q(x) \in K[x]$ tenemos que $\text{gr}(p + q) \leq \max\{\text{gr}(p), \text{gr}(q)\}$ y $\text{gr}(pq) \leq \text{gr}(p) + \text{gr}(q)$.

8.3. División de polinomios

Dados dos polinomios $p(x), q(x) \in K[x]$, el **máximo común divisor** de ambos es un polinomio mónico (su coeficiente principal es 1), $d(x) \in K[x]$, que divide a ambos polinomios y tal que cualquier otro divisor común de $p(x)$ y $q(x)$ también divide a $d(x)$.

> Teorema (Algoritmo de la División). Sean $p(x), q(x) \in K[x]$ dos polinomios con $q(x) \neq 0$. Entonces, existen otros dos polinomios únicos $c(x), r(x) \in K[x]$, tales que $p(x) = c(x)q(x) + r(x)$, con $\text{gr}(r(x)) < \text{gr}(q(x)) \vee r(x) = 0$.

Demostración.
Si $\text{gr}(p(x)) < \text{gr}(q(x))$, entonces la demostración es trivial, ya que $p(x) = 0 \cdot q(x) + p(x)$, con lo que $c(x) = 0$ y $r(x) = p(x)$.
De lo contrario, siendo $n = \text{gr}(p(x))$, suponemos que $n = 0$, de forma que $p(x) = a_0$, por lo que $q(x) = b_0 \neq 0$. Luego, $p(x) = \frac{a_0}{b_0} \cdot q(x)$. Asumimos que esto se cumple para $\text{gr}(p(x)) = n$ y comprobamos qué pasa con $\text{gr}(p(x)) = n + 1$.
Sea $p(x) = a_{n+1}x^{n+1} + a_n x^n + ... + a_1 x + a_0$, con $a_{n+1} \neq 0$. y $q(x)$ un polinomio con $\text{gr}(q(x)) = m \leq n + 1$. Entonces, $p(x) - \frac{a_{n+1}}{b_m} \cdot x^{n+1-m} \cdot q(x)$ es un polinomio con grado menor o igual que n.
Luego, por la hipótesis de inducción, $\exists c_1(x), r_1(x) \in K[x] : p(x) - \frac{a_{n+1}}{b_m} \cdot x^{n+1-m} \cdot q(x) = c_1(x) \cdot q(x) + r_1(x)$. Luego, $p(x) = \left(\frac{a_{n+1}}{b_m} \cdot x^{n+1} + c_1(x)\right) \cdot q(x) + r_1(x)$, por lo que $c(x) = \frac{a_{n+1}}{b_m} \cdot x^{n+1} + c_1(x)$ y $r(x) = r_1(x)$.

Por otra parte, suponemos que $\exists c_1(x), c_2(x), r_1(x), r_2(x) : p(x) = c_1(x) \cdot q(x) + r_1(x) = c_2(x) \cdot$

$q(x) + r_2(x)$. De esta forma, $(c_1(x) - c_2(x)) \cdot q(x) + (r_1(x) - r_2(x)) = 0$.
- Si $c_1(x) = c_2(x)$, entonces, $r_1(x) = r_2(x)$ y ambos polinomios son únicos.
- Si $c_1(x) \neq c_2(x)$, entonces, $\text{gr}((c_1(x) - c_2(x)) \cdot q(x)) = \text{gr}(c_1(x) - c_2(x)) + \text{gr}(q(x)) \geq \text{gr}(q(x)) < \text{gr}(r_1(x) - r_2(x))$.
- Si $r_1(x) \neq r_2(x)$, entonces, no podría darse la resta anterior, por lo que $r_1(x) = r_2(x)$, de forma que $\text{gr}(r_1(x) - r_2(x)) = 0$ y $\text{gr}(q(x)) = 0$, por lo que $\text{gr}(c_1(x) - c_2(x)) = 0$ y $c_1(x) = c_2(x)$; y ambos polinomios son únicos. □

8.3.1. Divisibilidad

*Definición. Sea A un anillo y dados dos polinomios $p(x), q(x) \in A[x]$. Decimos que $q(x)$ es **divisor** de $p(x)$ si existe un polinomio $c(x) \in A[x]$ tal que $p(x) = c(x)q(x)$.*

> Proposición. Si $r(x)|p(x)$ y $r(x)|q(x)$ en $A[x]$, entonces, $r(x)|(p(x) + \lambda q(x)), \forall \lambda \in A$.

> Proposición. Si K es un cuerpo y $q(x)|p(x)$ en $K[x]$, entonces, $\text{gr}(p(x)) \geq \text{gr}(q(x))$.

> Proposición. Sea K un cuerpo y $p(x), q(x) \in K[x]$ dos polinomios. Si $p(x)q(x) = 0$, entonces, $p(x) = 0 \vee q(x) = 0$.

8.3.2. Máximo común divisor de dos polinomios

> Proposición. Sea K un cuerpo y $p(x), q(x) \in K[x]$ dos polinomios. Si $p(x)|q(x)$ y $q(x)|p(x)$. Entonces, $\exists c \in K \backslash \{0\} : p(x) = c \cdot q(x)$.

Demostración.
Si $p(x) = 0$, entonces $q(x) = 0$ y al contrario, por lo que la conclusión es trivial.
Si $p(x), q(x) \neq 0$, entonces, $\exists c(x), d(x) \in K[x]$ tales que $p(x) = c(x)q(x)$ y $q(x) = d(x)p(x)$. Por lo que $p(x) = c(x)q(x) = c(x)d(x)p(x) \Rightarrow p(x)(1 - c(x)d(x)) = 0$.
Como $p(x) \neq 0$, entonces $1 - c(x)d(x) = 0 \Rightarrow c(x)d(x) = 1$, por lo que $c(x)$ y $d(x)$ son invertibles en $K[x]$. Luego, $c(x), d(x) \neq 0$. □

> Lema. Sea K un cuerpo y $p(x), q(x), c(x), r(x) \in K[x]$ cuatro polinomios tales que $p(x) = c(x)q(x) + r(x)$. Entonces, $\text{mcd}\ (p(x), q(x)) = \text{mcd}\ (q(x), r(x))$, suponiendo que ambos sean mónicos.

Demostración.
Sean $d(x) = \text{mcd}\ (p(x), q(x))$ y $e(x) = \text{mcd}\ (q(x), r(x))$. Entonces, $d(x)|p(x)$ y $d(x)|q(x)$, de forma que $d(x)|(p(x) - c(x)q(x)) = r(x)$. Luego, $d(x)|\text{mcd}\ (q(x), r(x)) = e(x)$.
Por otra parte, $e(x)|q(x)$ y $e(x)|r(x)$, de forma que $e(x)|(c(x)q(x) - r(x)) = p(x)$. Luego, $e(x)|\text{mcd}\ (p(x), q(x)) = d(x)$. Como $d(x)|e(x)$ y $e(x)|d(x)$, se tiene que $d(x) = e(x) \Leftrightarrow \text{mcd}\ (p(x), q(x)) = \text{mcd}\ (q(x), r(x))$. □

8.4. Algoritmo de Euclides

Al igual que con los números enteros, podemos usar el **Algoritmo de Euclides** para encontrar el $\text{mcd}\ (p(x), q(x))$, para cualquier $p(x), q(x) \in K[x]$.

Caso general.
Suponemos cuatro polinomios $p(x), q(x), c_0(x), r_1(x) \in K[x]$ tales que $p(x) = c_0(x)q(x) + r_1(x)$, con $0 \leq \text{gr}(r_1(x)) \leq \text{gr}(q(x))$.
- Si $r_1(x) = 0$, entonces $q(x)|p(x)$, por lo que $\text{mcd}\ (p(x), q(x)) = q(x)$.
- Si $r_1(x) \neq 0$, entonces $\text{mcd}\ (p(x), q(x)) = \text{mcd}\ (q(x), r_1(x))$. Así, podemos decir que $q(x) = c_1(x)r_1(x) + r_2(x)$, con $0 \leq \text{gr}(r_2(x)) \leq \text{gr}(r_1(x))$ y volver a empezar.

8.4.1. Identidad de Bézout

> Teorema (Identidad de Bézout). Sean $p(x), q(x), c(x), d(x) \in K[x] \backslash \{0\}$ cuatro polinomios tales que $d(x) = \text{mcd}\ (p(x), q(x))$ y $d(x)|c(x)$. Entonces, $\exists a(x), b(x) \in K[x] : c(x) = a(x)p(x) + b(x)q(x)$.

Sean $p(x), q(x), c(x) \in K[x]$ tres polinomios, $d(x) = \text{mcd}\ (p(x), q(x))$ y $(a_0(x), b_0(x)) \in K[x] \times K[x]$ una solución particular de la ecuación diofántica $a(x)p(x) + b(x)q(x) = c(x)$. Entonces, cualquier solución de la misma es de la forma $(a(x), b(x)) = \begin{cases} a(x) = a_0(x) + \frac{q(x)}{d(x)}m(x) \\ b(x) = b_0(x) - \frac{p(x)}{d(x)}m(x) \end{cases}, m(x) \in K[x]$.

*Definición. Dados dos polinomios $p(x), q(x) \in K[x]$. Decimos que son **coprimos** si $\text{mcd}\ (p(x), q(x)) = 1$, es decir, si ningún polinomio de grado ≥ 1 divide simultáneamente a ambos polinomios.*

*Definición. Dado un polinomio $p(x) \in K[x]$ con $\text{gr}(p(x))$. Decimos que es **irreducible** si sus únicos divisores son k y $kp(x)$, con $k \in K$. Es decir, si no puede escribirse como producto de dos polinomios de grado estrictamente menor.*

8.5. Evaluación de polinomios

*Definición. Sea A un anillo y $p(x) \in A[x]$ un polinomio de la forma $p(x) = c_0 + c_1x + ... + c_nx^n$. Definimos la **función polinómica** p asociada al polinomio $p(x)$ como $p : A \to A$, con $p(a) = c_0 + c_1a + ... + c_na^n$, para $a \in A$.*

8.5.1. Lema de Bézout

> **Lema de Bézout**. Sea K un cuerpo, $a \in K$ y $p(x) \in K[x]$. Entonces, $(x - a)|p(x)$ si y solo si $p(a) = 0$.

Demostración.
Por el algoritmo de la división en $K[x]$, sabemos que $p(x) = c(x)(x - a) + b$, con $b \in A$.
$\Rightarrow$) Si $(x - a)|p(x)$, entonces $b = 0$, por lo que $p(x) = c(x)(x - a)$. Así, la función polinómica evaluada en a es $p(a) = c(a) \cdot (a - a) = c(a) \cdot 0 = 0$.

$\Leftarrow$) Si $p(a) = 0$, entonces $p(a) = c(a) \cdot (a - a) + b = b = 0$, por lo que $p(x) = c(x)(x - a)$ y $(x - a) | p(x)$. $\square$

8.5.2. Raíces de polinomios

*Definición. Dado un polinomio $p(x) \in A[x]$ y un valor $a \in A$ tales que $p(a) = 0$. Decimos que $x = a$ es una **raíz** del polinomio $p(x)$.*

*Definición. Dado un polinomio $p(x) \in A[x]$ y un valor $a \in A$ tales que a es raíz de $p(x)$. Decimos que $x = a$ es una raíz de **multiplicidad** n, con $n \geq 1$, si $(x - a)^n | p(x)$, pero $(x - a)^{n+1} \not| \, p(x)$.*

> Teorema. Sea K un cuerpo y $p(x) \in K[x]$ un polinomio tal que $\text{gr}(p(x)) = n \geq 1$. Entonces, $p(x)$ tiene, como mucho, n raíces en K, contando las multiplicidades de cada una.

Demostración.
Para $n = 1$, la afirmación es cierta, ya que si $\text{gr}(p(x)) = 1$, entonces $\exists a, b \in K : p(x) = ax + b$, por lo que existe una raíz $x = -\dfrac{b}{a} \in K$ tal que $p\left(-\dfrac{b}{a}\right) = 0$.
Ahora suponemos que todo polinomio $q(x) \in K[x]$ con $\text{gr}(q(x)) = n$ tiene, a lo sumo, n raíces en K.
Sea $p(x) \in K[x]$ un polinomio con $\text{gr}(p(x)) = n + 1$, entonces:
- Si $p(x)$ no tiene raíces en K, la afirmación es trivialmente cierta.
- Si existe un valor $a \in K$ tal que $p(a) = 0$, entonces, por el Lema de Bézout, podemos expresar $p(x)$ como $p(x) = (x - a)q(x)$, con $q(x) \in K[x]$. De esta forma, $\text{gr}(q(x)) = \text{gr}(p(x)) - 1 = (n + 1) - 1 = n$, dando como resultado la hipótesis de inducción. $\square$

> Corolario 1. Sea K un cuerpo y $p(x) \in K[x]$ un polinomio con $\text{gr}(p(x)) = n \geq 0$. Si $\exists a_1, a_2, ..., a_m \in K$ distintos entre sí, tales que $m > n$ y $p(a_1) = p(a_2) = ... = p(a_m) = 0$. Entonces $p \equiv 0$

Demostración.
Por el teorema anterior, si $n \geq 1$, entonces el número de raíces de $p(x)$ en K es $\leq n < m \leq$ que el número de raíces de $p(x)$. Por lo tanto, si $n = 0$, entonces $p(x) = c \in K$, y si $p(a_1) = 0$, entonce $c = 0$. $\square$

> Corolario 2. Sean K un cuerpo y $p(x), q(x) \in K[x]$ dos polinomios tales que $|K| > \max\{\text{gr}(p(x)), \text{gr}(q(x))\}$, y $p(a) = q(a), \forall a \in K$. Entonces, $p(x) \equiv q(x)$.

Demostración.
Consideramos el polinomio $r(x) = p(x) - q(x) \in K[x]$.
- Si $r(x) \equiv 0$, se demuestra trivialmente.
- Si $r(x) \not\equiv 0$, entonces, $r(x)$ se anula en $|K|$ valores de K y $|K| > \text{gr}(r(x))$. Por el corolario anterior, $r(x) \equiv 0$. $\square$

> Corolario 3. Sea K un cuerpo y $p(x) \in K[x]$ un polinomio de grado $n \geq 1$, expresado como $\sum_{k=0}^{n} a_k x^k$. Si $c_1, c_2, ..., c_n \in K$ son las n raíces de $p(x)$. Entonces, $p(x) = a_n \cdot (x - c_1) \cdot (x - c_2) \cdot ... \cdot (x - c_n)$.

Demotración.
Sea $q(x) = a_n \cdot (x - c_1) \cdot (x - c_2) \cdot ... \cdot (x - c_n)$. Entonces, $q(x) \in K[x]$ y $\text{gr}(q(x)) = n$. Sea $r(x) = p(x) - q(x) \in K[x]$, de forma que $\text{gr}(r(x)) \leq n - 1$ y $r(c_k) = p(c_k) - q(c_k) = 0$, para $k = 1, 2, ..., n$. Por el corolario anterior, $p(x) \equiv q(x)$. □

8.6. Teorema fundamental del álgebra

> Teorema Fundamental del Álgebra. Todo polinomio $p(x) \in \mathbb{C}[x]$ no constante tiene, al menos, una raíz en $\mathbb{C}$.

> Corolario. Todo polinomio $p(x) \in \mathbb{C}[x]$ de grado $n \geq 1$ tiene exactamente n raíces $z_1, z_2, ..., z_n \in \mathbb{C}$ (contando multiplicidades) y, por consiguiente, puede factorizarse como $p(x) = a_n \prod_{k=1}^{n} (x - z_k)$.

Demostración.

Si $\text{gr}(p(x)) = n = 1$, entonces, $p(x) = a_1 x + a_0$, con $a_0, a_1 \in \mathbb{C}$. Así, $p(x) = a_1 \left(x - \frac{x_0}{x_1} \right)$, con lo que $z_1 = \frac{a_0}{a_1}$.
Por otra parte, sea $p(x) \in \mathbb{C}[x]$ un polinomio con $\text{gr}(p(x)) = n + 1$. Entonces, por el Teorema Fundamental del Álgebra, $\exists z_{n+1} \in \mathbb{C}$ tal que $p(z_{n+1}) = 0$. Por el Lema de Bézout, $(x - z_{n+1}) | p(x)$, de forma que podemos decir que $p(x) = (x - z_{n+1}) q(x)$, con $q(x) \in \mathbb{C}[x]$. Así, $\text{gr}(q(x)) = \text{gr}(p(x)) - 1 = (n + 1) - 1 = n$. Por hipótesis de inducción, tenemos que $q(x)$ tiene n raíces en $\mathbb{C}$ que, junto con z_{n+1}, son las $n + 1$ raíces de $p(x)$. □

> Proposición. Sea $p(x) \in \mathbb{R}[x]$ un polinomio y $z \in \mathbb{C}$ una raíz de $p(x)$. Entonces, el complementario de z, $\overline{z}$, también lo es.

Demostración.

Sea $p(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio, con $a_i \in \mathbb{R}$ para todo i. Partiendo de que $0 = p(z) = a_n z^n + ... + a_1 z + a_0$, tenemos que $0 = \overline{0} = \overline{a_n z^n + ... + a_1 z + a_0} = \overline{a_n z^n} + ... + \overline{a_1 z} + \overline{a_0} = a_n \overline{z^n} + ... + a_1 \overline{z} + a_0 = a_n \overline{z}^n + ... + a_1 \overline{z} + a_0 = p(\overline{z})$. □

8.7. Raíces de polinomio en $\mathbb{Z}[x]$

> Teorema. Sea $p(x) \in \mathbb{Z}[x]$ un polinomio y $\frac{p}{q} \in \mathbb{Q}$ una raíz de $p(x)$ con $p, q \in \mathbb{Z}$ y $\text{mcd}\ (p, q) = 1$. Entonces, $p|a_0$ y $q|a_n$.

Demostración.
Por hipótesis, $a_0 + a_1\frac{p}{q} + ... + a_n\left(\frac{p}{q}\right)^n = 0$. Entonces, multiplicando por q^n, obtenemos $a_0q^n + a_1pq^{n-1} + ... + a_np^n = 0$. Luego, $p|(a_1pq^{n-1} + ... + a_np^n)$, por lo que $p|a_0q^n$ y $p|a_0$.
Por otra parte, $q|(a_0q^n + ... + a_{n-1}p^{n-1}q)$, por lo que $q|a_np^n$ y $q|a_n$. □

8.7.1. Multiplicidad de un cero

> Lema. Sea $p(x) \in \mathbb{C}[x]$ un polinomio y $a \in \mathbb{C}$ un cero de $p(x)$ de orden $n \geq 1$. Entonces, a es un cero de $p'(x)$ de orden $n - 1$.

Demostraión.
Por hipótesis, $p(x) = (x - a)^nq(x)$, con $q(x) \in \mathbb{C}[x]$ y $q(a) \neq 0$. Podemos derivar $p(x)$ de forma que $p'(x) = n(x - a)^{n-1}q(x) + (x - a)^nq'(x) = (x - a)^{n-1}(nq(x) + (x - a)q'(x))$.
Si definimos el polinomio $r(x)$ como $r(x) = nq(x) + (x - a)q'(x)$, vemos que $r(a) = nq(a) \neq 0$, ya que $n, q(a) \neq 0$. Por lo tanto, $(x - a)^{n-1}|p'(x)$, pero $(x - a)^n \not| p'(x)$, es decir, a es un cero de multiplicidad $n - 1$ de $p'(x)$. □

8.8. Polinomios reducibles e irreducibles

*Definición. Sea A un anillo conmutativo y unitario, y $p(x) \in A[x]$ un polinomio distinto de un elemento invertible de $A[x]$. Decimos que $p(x)$ es un **polinomio reducible** si $\exists q(x), r(x) \in A[x]$ tales que $p(x) \equiv q(x)r(x)$ y ninguno de los polinomios $q(x), r(x)$ es invertible en $A[x]$.*

*Definición. Sea A un anillo conmutativo y unitario, y $p(x) \in A[x]$ un polinomio distinto de un elemento invertible de $A[x]$. Decimos que $p(x)$ es un **polinomio irreducible** si dados dos polinomios $q(x), r(x) \in A[x]$ tales que $p(x) = q(x)r(x)$ esto implica que alguno de los dos sea invertible en $A[x]$.*

> Proposición. Sea K un cuerpo y $p(x) \in K[x]$ un polinomio con $\text{gr}(p(x)) \in \{2, 3\}$. Entonces, $p(x)$ es reducible en $K[x]$ si y solo si $p(x)$ tiene una raíz en K.

Demostración.
$\Leftarrow$) Suponemos que a es una raíz de $p(x)$. Por el Lema de Bézout, podemos expresar $p(x)$ como $p(x) = (x - a)q(x)$, para un $q(x) \in K[x]$. Como $\text{gr}(q(x)) = \text{gr}(p(x)) - 1$, entonces $\text{gr}(q(x)) \in \{1, 2\}$, por lo que $q(x)$ no es invertible en $K[x]$. Como $x - a$ tampoco lo es, $p(x)$ es reducible en $K[x]$.
$\Rightarrow$) Suponemos que $p(x)$ es reducible en $K[x]$. Entonces, $\exists q(x), r(x) \in K[x]$ tales que $p(x) = q(x)r(x)$, con $q(x), r(x) \neq \text{cte.}$. Como $\text{gr}(p(x)) = \text{gr}(q(x)) + \text{gr}(r(x))$ y $\text{gr}(p(x)) \in \{2, 3\}$, entonces, $\text{gr}(q(x)) = 1 \vee \text{gr}(r(x)) = 1$, por lo que al menos uno de los dos debe tener una raíz en K.
□

> Proposición. Sea $p(x) \in \mathbb{R}[x]$ un polinomio no constante. Si $p(x)$ es irreducible en $\mathbb{R}[x]$, entonces, $\text{gr}(p(x)) \in \{1, 2\}$.

Además, si $\text{gr}(p(x)) = 2$, de forma que $p(x) = ax^2 + bx + c$, con $a \neq 0$. Entonces, $\Delta = b^2 - 4ac < 0$.

8.8.1. Reducibilidad en $\mathbb{Q}[x]$ y en $\mathbb{Z}[x]$

*Definición. Dado un polinomio $p(x) \in \mathbb{Z}[x]$ de la forma $p(x) = a_n x^n + ... + a_1 x + a_0$, con $a_n \neq 0$. Definimos el **contenido de** $p(x)$ como el número $\text{C}(p(x)) = \text{mcd }(a_0, a_1, ..., a_n)$.*

*Definición. Dado un polinomio $p(x) \in \mathbb{Z}[x]$. Decimos que $p(x)$ es **primitivo** si $\text{C}(p(x)) = 1$.*

Observaciones.

1. Todo polinomio $p(x) \in \mathbb{Z}[x]$ puede escribirse como $p(x) = \text{C}(p(x))q(x)$, con $q(x)$ primitivo.
2. Si $p(x) \in \mathbb{Z}[x]$ es primitivo y $p(x) \neq 1, -1$, entonces, $\text{gr}(p(x)) \geq 1$.

> Lema de Gauss. El producto de dos polinomios primitivos también es primitivo.

Demostración.

Sean $p(x), q(x) \in \mathbb{Z}[x]$ dos polinomios primitivos tales que $p(x) = \sum_{i=0}^{n} a_i x^i$ y $q(x) = \sum_{j=0}^{m} a_j x^j$, de forma que $p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k$. Sabemos que $c_k = a_0 b_k + a_1 b_{k-1} + ... + a_k b_0$.

Suponemos que $p(x)q(x)$ no es primitivo, de forma que $\text{C}(p(x)q(x))$ es un naturale mayor que 1 y, por tanto, divisible por un primo p.

Sea r el mayor índice tal que $p \nmid a_r$ y s el menor índice tal que $p \nmid b_s$. Entonces, $p | c_{r+s} = (a_0 b_{r+s} + ... + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + ... + a_{m+n} b_0)$, de forma que $p | a_r b_s \Rightarrow p | a_r \vee p | b_s$. Luego, llegamos a una contadicción y $p(x)q(x)$ es primitivo. □

> Corolario. Sean $p(x), q(x) \in K[x]$ dos polinomios. Entonces, $\text{C}(p(x)q(x)) = \text{C}(p(x))\text{C}(q(x))$.

Demostración.

Vemos que $p(x) = \text{C}(p(x))p_1(x)$ y $q(x) = \text{C}(q(x))q_1(x)$, con $p_1(x), q_1(x) \in K[x]$ primitivos, de forma que, por el Lema de Gauss, $p_1(x)q_1(x)$ es primitivo.

Vemos también que $p(x)q(x) = \text{C}(p(x))\text{C}(q(x))p_1(x)q_1(x)$, de forma que $\text{C}(p(x)q(x)) = \text{C}(p(x))\text{C}(q(x))\text{C}(p_1(x)q_1(x)) = \text{C}(p(x))\text{C}(q(x))$. □

> Proposición. Sean $p(x), q(x) \in \mathbb{Z}[x]$ dos polinomios con $p(x)$ primitivo y $p(x) | q(x)$ en $\mathbb{Q}[x]$. Entonces, $p(x) | q(x)$ en $\mathbb{Z}[x]$.

Demostración.

Supongamos que $q(x) = p(x)r(x)$, con $r(x) \in \mathbb{Q}[x]$. Por lo visto anteriormente, $r(x) = \frac{1}{q} r_1(x)$, con

$q \in \mathbb{Z}$ y $r_1(x) \in \mathbb{Z}[x]$. Entonces, $q \cdot q(x) = q \cdot p(x)r(x) = p(x)r_1(x)$.
Generalizando el Lema de Gauss, vemos que $q\mathrm{C}(q(x)) = \mathrm{C}(q \cdot q(x)) = \mathrm{C}(p(x)r_1(x)) = \mathrm{C}(p(x))\mathrm{C}(r_1(x)) = \mathrm{C}(r_1(x))$, por lo que $q|\mathrm{C}(r_1(x))$ y $r_1(x) \in \mathbb{Z}[x]$. □

> Teorema de Gauss. Sea $p(x) \in \mathbb{Z}[x]$ un polinomio primitivo. Entonces, $p(x)$ es irreducible en $\mathbb{Q}[x]$ si y solo si $p(x)$ es irreducible en $\mathbb{Z}[x]$.

Demostración.
$\Rightarrow$) Suponemos que $p(x)$ es reducible en $\mathbb{Q}[x]$. Entonces, $\exists q(x), r(x) \in \mathbb{Q}[x]$ tales que $p(x) = q(x)r(x)$ con ninguno de los polinomios constantes.
Podemos decir que $q(x) = \dfrac{1}{q}q_1(x)$, con $q_1(x) \in \mathbb{Z}[x]$ primitivo y $q \in \mathbb{Z}$. Entonces, $q \cdot p(x) = q(q(x)r(x)) = q\left(\dfrac{1}{q}q_1(x)r(x)\right) = q_1(x)r(x)$, por lo que $q_1(x)|p(x)$ en $\mathbb{Q}[x]$. Por la proposición enterior, $q_1(x)|p(x)$ en $\mathbb{Z}[x]$ y $p(x)$ es irreducible en $\mathbb{Z}[x]$.
$\Leftarrow$) Suponemos que $p(x) \in \mathbb{Z}[x]$ es primitivo y reducible en $\mathbb{Z}[x]$. Entonces, $\exists q(x), r(x) \in \mathbb{Z}[x]$ tales que $p(x) = q(x)r(x)$ con ninguno de los dos invertibles en $\mathbb{Z}[x]$. Como $p(x)$ es primitivo, sabemos que $1 = \mathrm{C}(p(x)) = \mathrm{C}(q(x))\mathrm{C}(r(x))$, por lo que $\mathrm{C}(q(x)) = \mathrm{C}(r(x)) = 1$. Como además, $q(x), r(x) \neq \pm 1$, sabemos que $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) \geq 1$. Puesto que en $\mathbb{Q}[x]$ también tenemos la factorización $p(x) = q(x)r(x)$, se sigue que $p(x)$ es reducible en $\mathbb{Q}[x]$. □

> Teorema (criterio de Eisenstein). Sea $p(x) \in \mathbb{Z}[x]$ un polinomio primitivo se de la forma $p(x) = a_n x^n + ... + a_1 x + a_0$ y p un número primo tal que $p|a_0, a_1, ..., a_{n-1}$, pero $p \not| a_n$ y $p^2 \not| a_0$. Entonces, $p(x)$ es irreducible en $\mathbb{Z}[x]$.

Debido a la hipótesis del Teorema, $p(x)$ es primitivo. Por el Teorema de Gauss, se concluye que $p(x)$ también es irreducible en $\mathbb{Q}[x]$.

Demotración.
Suponemos que existen dos polinomios $q(x), r(x) \in \mathbb{Z}[x]$ no constantes tales que $p(x) = q(x)r(x)$.
Podemos expresar los polinomios anteriores como $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{j=0}^{m} b_j x^j$ y $r(x) = \sum_{k=0}^{s} c_k x^k$, con $m + r = n$ y $m, r \geq 1$.
Si $p(x)$ es primitivo, entonces, $q(x), r(x)$ también lo son. Por lo que $\exists p$ primo tal que $p|b_0, b_1, ..., b_{m-1}$, pero $p \not| b_m$. Por hipótesis, $p|a_j$ y $a_j = b_0 c_j + ... + b_j c_0$, de forma que $p|b_j c_0$ y $p|c_0$, ya que $p \not| b_j$. Luego, $p^2|b_0 c_0 = a_0$, llegando a una contradicción. □

> Lema. Sea A un anillo conmutativo y unitario, $p(x) \in A[x]$ un polinomio y $a \in A$ un valor. Entonces, $p(x)$ es irreducible en $A[x]$ si y solo si $p(x - a)$ es irreducible en $A[x]$.

8.9. Reducción módulo un primo

Definición. Dad un polinomio $q(x) \in \mathbb{Z}[x]$ y un primo p. Definimos el polinomio $\overline{q}(x) \in \mathbb{Z}_p[x]$ como aquel cuyos coeficientes son los de $q(x)$ reducidos a módulo p.
Nota. Todo polinomio $q(x) \in \mathbb{Z}[x]$ que es mónico, es primitivo.

> Proposición. Sea $q(x) \in \mathbb{Z}[x]$ un polinomio primitivo y $\overline{q}(x) \in \mathbb{Z}_p[x]$, con p primo, el polinomio correspondiente con los coeficientes reducidos a módulo p. Si $\mathrm{gr}(\overline{q}(x)) = \mathrm{gr}(q(x))$ y $\overline{q}(x)$ es irreducible en $\mathbb{Z}_p[x]$, entoces, $q(x)$ es ireeducible en $\mathbb{Q}[x]$.

Demotración.
Suponemos que $q(x)$ es reducible en $\mathbb{Q}[x]$. Por el Teorema de Gauss, $q(x)$ es reducible en $\mathbb{Z}[x]$, por lo que existen dos polinomios $p_1(x), p_2(x) \in \mathbb{Z}[x]$ distintos de ± 1 tale que $q(x) = p_1(x)p_2(x)$.
Reduciendo los coeficientes a módulo p, obtenemos que $\overline{q}(x) = \overline{p_1}(x)\overline{p_2}(x)$, con $\mathrm{gr}(\overline{q}(x)) \leq \mathrm{gr}(\overline{p_1}(x)) + \mathrm{gr}(\overline{p_2}(x))$, luego, $\overline{p_1}(x)$ y $\overline{p_2}(x)$ no son constantes. Por tanto, $\overline{q}(x)$ es reducible en $\mathbb{Z}_p[x]$.
$\square$