# Propiedades de los anillos de polinomios

## Definición

Sea $R$ un anillo, definimos al anillo de polinomios con coeficientes en $R$ como

$$R[\mathrm{X}] = \left\{ \sum_{k=0}^{n} a_k x^k : a_k \in \mathrm{R}, n \in \mathbb{N}_0 \right\}.$$

## Teorema

Sea $R$ anillo y $p, q \in R[\mathrm{X}]$, entonces

- $gr(p+q) \leq \text{máx}\{gr(p), gr(q)\}$.
- $gr(p \cdot q) \leq gr(p) + gr(q)$.
- Si el producto de los coeficientes principales de $p$ y $q$ no da 0 entonces $gr(p \cdot q) = gr(p) + gr(q)$. En particular, si $R$ es un cuerpo esta igualdad vale.

## Teorema

Sea $\mathbb{K}$ un cuerpo. Entonces, el conjunto de elementos inversibles de $\mathbb{K}[X]$ es $\mathbb{K}$.

## Demostración.

Sea $p \in \mathbb{K}[X]$ inversible. Vale decir, existe $q \in \mathbb{K}[X]$ tal que $pq = 1$. Luego tomando grado y usando el lema anterior tenemos que $gr(p) + gr(q) = gr(pq) = gr(1) = 0$. Por lo tanto $gr(p) = gr(q) = 0$ y entonces $p \in \mathbb{K}$. □

## Teorema

Si $\mathbb{K}$ es un cuerpo entonces $\mathbb{K}[X]$ tiene algoritmo de división. Esto es, dados $p, q \in \mathbb{K}[X]$, $q \neq 0$, existen únicos $r, t \in \mathbb{K}[X]$ tal que

1. $p = tq + r$,
2. $r = 0$ o $gr(r) < gr(q)$.

## Demostración.

*Existencia*: Si $gr(p) < gr(q)$ tomamos $t = 0$ y $r = p$. Supongamos ahora que $gr(p) \geq gr(q)$ y que $p = \sum_{i=0}^{n} a_i x^i$ y $q = \sum_{j=0}^{m} b_j x^j$, con $a_n, b_m \neq 0$. Procedemos por inducción en $n$. Si $gr(p) = 0$ entonces $m = n = 0$, $p = a_0$ y $q = b_0$, luego tomando $t = a_0 b_0^{-1}$, $r = 0$ y estamos. Para el paso inductivo notar que $h := (a_n b_m^{-1} x^{n-m})q$ es un polinomio de grado $n$ con coeficiente principal $a_n$, por lo que $gr(p - h) < n$. Aplicando la hipótesis inductiva tenemos que existen $\widetilde{t}, r \in \mathbb{K}[X]$ tal que $p - h = \widetilde{t}q + r$. Tomando $t := a_n b_m^{-1} x^{n-m} + \widetilde{t}$ tenemos que $p = tq + r$ con $gr(r) < gr(q)$. En efecto,

$$\begin{aligned} tq + r &= (a_n b_m^{-1} x^{n-m} + \widetilde{t})q + r \\ &= h + \widetilde{t}q + r \\ &= h + p - h \\ &= p. \end{aligned}$$

## Demostración (Cont.)

Unicidad: Supongamos que

$$p = t_1 q + r_1 \qquad gr(r_1) < gr(q),$$
$$p = t_2 q + r_2 \qquad gr(r_2) < gr(q).$$

Luego $(t_1 - t_2)q = r_2 - r_1$. Suponiendo $q_1 \neq q_2$ tenemos que $gr(q) \leq gr(q) + gr(t_1 - t_2) = gr((t_1 - t_2)q) = gr(r_1 - r_2) < gr(q)$ lo cual es un absurdo. Por lo tanto $t_1 = t_2$ y $r_1 = r_2$. □

## Observación

Notar que en la demostración del Teorema anterior solo necesitamos que $\mathbb{K}$ tuviera inversos para poder asegurar la existencia del inverso del coeficiente principal de $q$. La conmutatividad no fue necesaria. Más aún, vale el siguiente corolario.

## Corolario

Sea $R$ un anillo, entonces R[X] tiene algoritmo de la división si y solo si R es un anillo de división (es decir , un anillo en el cual todos sus elementos tienen inverso).

## Demostración.

Basta ver la ida ya que la vuelta sale del Teorema anteior. Supongamos que existe $a \in R \setminus \{0\}$ tal que $a$ no tiene inverso. Luego tomando $p(x) = x$ y $q(x) = ax$ tenemos que existen únicos $t, r \in R[X]$ tal que $x = p(x) = t(x)q(x) + r(x) = at(x)x + r(x)$. Como $gr(r) < gr(q) = 1$ entonces $r(x) = c$. Luego evaluando en 0 tenemos que $0 = at(0)0 + c = c$ y entonces $r = 0$. Además como $at(x) = 1$, tenemos que $t(x) = b$ con $b \in \mathbb{K}$. Por lo tanto $1 = ab$ lo que contradice el hecho de que $a$ fuese inversible. □

## Definición

Sea $\mathbb{K}$ un cuerpo y $p, q \in \mathbb{K}[X]$. Decimos que $q$ divide a $p$, lo cual lo denotaremos por $q|p$, si existe $t \in \mathbb{K}[X]$ tal que $p = qt$. Si además $p \neq 0$ y $p|q$ se dice que $p$ y $q$ son asociados.

## Proposición

Sea $\mathbb{K}$ cuerpo y $p, q \in \mathbb{K}[X] \setminus \{0\}$. Luego, $p = cq$ con $c \in \mathbb{K}$ si y solo si $p$ y $q$ son asociados.

## Demostración.

$\Rightarrow$) Por hipótesis $q|p$. Además como $p \neq 0$ y $q = c^{-1}p$ tenemos que $p|q$ y entonces $p$ y $q$ son asociados.

$\Leftarrow$) Como $p$ y $q$ son asociados tenemos que $p = rq$ y $q = r'p$ para algunos $r, r' \in \mathbb{K}[X]$. Luego $p = rq = rr'p$ y por una cuestión de grado tenemos que $r, r' \in \mathbb{K}$. $\square$

## Definición

Sea $\mathbb{K}$ un cuerpo, decimos que $p \in \mathbb{K}[X]$ es irreducible si se cumple que

- $p \notin \mathbb{K}$.
- Si $p = qt$ con $q, t \in \mathbb{K}[X]$, entonces $q \in \mathbb{K}$ o $t \in \mathbb{K}$. Es decir, $p$ no tiene divisores con grado entre 1 y $gr(p) - 1$.

## Definición

Sea $\mathbb{K}$ un cuerpo. Un elemento $p \in \mathbb{K}$ se dice primo si:

- $p \notin \mathbb{K}$.
- $p|qt$ con $q, t \in \mathbb{K}[X]$, entonces $p|q$ o $p|t$.

## Definición

Sean $\mathbb{K}$ un cuerpo y $p, q \in \mathbb{K}[X]$ con $q \neq 0$. Definimos el máximo común divisor de $p$ y $q$ como el único polinomio $d \in \mathbb{K}[X]$ tal que

1. $d|p$ y $d|q$
2. Si $r|p$ y $r|q$ entonces $r|d$.
   Denotaremos a $d$ por $d = (p, q)$.

## Teorema

Sea $\mathbb{K}$ un cuerpo y $p, q \in \mathbb{K}[X]$ con $q \neq 0$. Luego existen $r, t \in \mathbb{K}[X]$ tal que $(p, q) = rp + qt$.

## Demostración.

(Idea) La idea es repetir la misma prueba que se vió para los enteros. Es decir, se procede a realizar el algoritmo de Euclides para $p$ y $q$ y el penúltimo resto del algoritmo (que se puede probar que coincide con $(p, q)$), podremos escribirlo en la forma deseada reemplazando de forma iterativa con igualdades de los pasos previos. Notar que la prueba es en escencia la misma, ya que solamente precisamos poder utilizar en todos los pasos del Algoritmo de Euclides el algoritmo de división, que sabemos que existe en $\mathbb{K}[X]$. □

## Teorema

Sea $\mathbb{K}$ cuerpo y $p \in \mathbb{K}[X]$. Luego, $p$ es primo si y solo si $p$ es irreducible.

## Demostración.

$\Rightarrow$) Por definición de primo $p \notin \mathbb{K}$. Supongamos que $p = qt$ con $q, t \in \mathbb{K}[X]$. Entonces en particular $p|qt$. Pero como $p$ es primo o bien $p|q$ o bien $p|t$. Si $p|q$ entonces $q = pr$ para algún $r \in \mathbb{K}[X]$ y luego $p = prt$. Por lo tanto $rt = 1$ y entonces $t \in \mathbb{K}$. De manera análoga, si $p|t$ se llega a que $q \in \mathbb{K}$. Por lo tanto $p$ es irreducible.

$\Leftarrow$) Por definición de irreducible $p \notin \mathbb{K}$. Supongamos que $p|qr$ con $q, r \in \mathbb{K}[X]$. Si $p|q$ queda demostrado, supongamos entonces que $p \nmid q$. Luego al ser $p$ irreducible tenemos $p$ y $q$ serán coprimos. Por lo tanto existirán polinomios $t, s \in \mathbb{K}[X]$ tal que $1 = tp + sq$. Multiplicando en ambos lados por $r$ tenemos que $r = rtp + sqr$. Como $p|qr$ y $p|p$ tenemos que $p|rtp$ y $p|sqr$ por lo que $p|r$ y estamos. $\square$

## Definición

Decimos que $\mathbb{K}[X]$ tiene factorización única si

- Todo elemento $p \in \mathbb{K}[X] \setminus \mathbb{K}$ se puede escribir de la forma $p = q_1 \cdot \ldots \cdot q_n$ donde $q_i$ es irreducible para todo $i = 1, \ldots, n$.
- Si $p = q_1 \cdot \ldots \cdot q_n$ y $p = q'_1 \cdot \ldots \cdot q'_m$ con $q_i, q'_j$ irreducibles, entonces $n = m$ y existe una permutación de $\{1, \ldots, n\}$, digamos $\sigma$, tal que $q_i$ y $q'_{\sigma(i)}$ son asociados.

## Teorema

Sea $\mathbb{K}$ un cuerpo, entonces $\mathbb{K}[X]$ tiene factorización única.

## Demostración.

*Existencia:* Sea $p \in \mathbb{K}[X] \setminus \mathbb{K}$. Lo haremos por inducción en $gr(p)$. El caso $gr(p) = 1$ es trivial. Supongamos ahora que $gr(p) = n$. Si $p$ es irreducible entonces estamos. Si no lo es, será producto de dos polinomios de grado menor a $n$. Aplicando la hipótesis inductiva a estos polinomios obtenemos la factorización deseada. □

## Demostración (Cont.)

*Unicidad:* Supongamos que $p = q_1 \cdot \ldots \cdot q_n$ y $p = q'_1 \cdot \ldots \cdot q'_m$ con $q_i, q'_j$ irreducibles. Como $q_i$ y $q'_j$ son irreducibles entonces son primos. Luego, como $q_1 | q'_1 \cdot \ldots \cdot q'_m$ tenemos que existe $i_1$ tal que $q_1 | q'_{i_1}$. Como tanto $q_1$ y $q'_{i_1}$ son irreducibles tenemos que $q_1 = a q'_{i_1}$ con $a \in \mathbb{K}$. Es decir que $q_1$ y $q'_{i_1}$ son asociados. Luego dividiendo en ambas igualdades por $q'_{i_1}$ y realizando este proceso para todos los elementos de $q_i$ obtenemos que tiene que pasar que $n = m$ y además para cada $q_k$, con $k = 0, \ldots, n$ existirá un $q'_{i_k}$ tal que $q_k$ y $q'_{i_k}$ son asociados. Definiendo $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ como $\sigma(k) = i_k$, tenemos que se cumple que $q_i$ y $q'_{\sigma(i)}$ son asociados. Por lo tanto se cumple la unicidad (salvo asociados) de la factorización. □