



## → Clase 5



# Polinomios: Algoritmo de Euclides

➤ **Definición:** Si  $a(x), b(x) \in K[x]$ , decimos que  $b(x)$  divide a  $a(x)$  si existe  $c(x) \in K[x]$  con:

➤ 
$$a(x) = b(x) c(x)$$

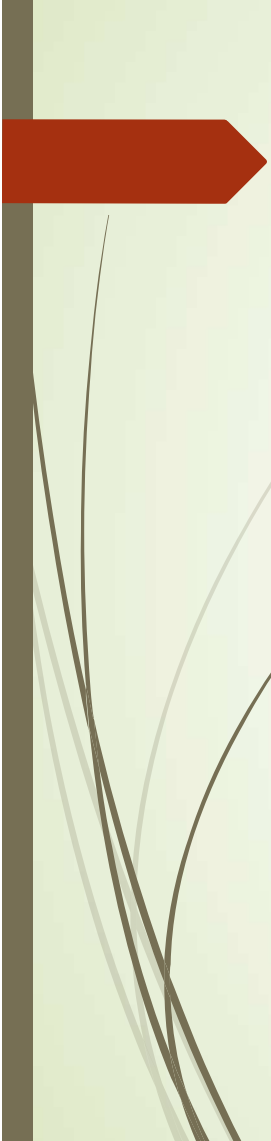
➤ Y lo denotamos  $b(x) \mid a(x)$ .

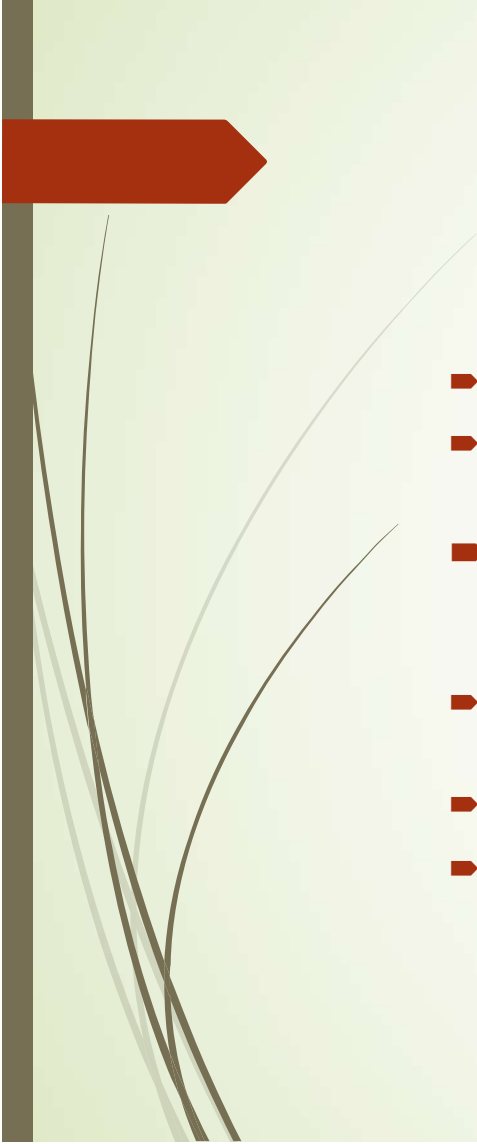
➤ En este caso decimos que  $b(x)$  es un divisor de  $a(x)$ .


➤ Ejemplos:

➤ (i)  $b(x) \mid 1$  equivale a decir que  $b(x)$  tiene inverso, y esto sabemos que equivale a que  $b(x)$  es constante y no nulo.

➤ (ii)  $x-1$  divide a  $x^2 - 1$  en  $\mathbb{R}[x]$ .

- 
- **Lema 1:** Si  $P(x) \in K[x]$  es un polinomio no nulo, los polinomios constantes  $c \in K$  no nulos y los de la forma  $c \cdot P(x)$  con  $c$  constante no nula dividen a  $P(x)$ .
  - **Demostración:** Basta con escribir las igualdades triviales:
    - $P(x) = c \cdot (c^{-1} \cdot P(x))$ , y:  $P(x) = c^{-1} \cdot (c \cdot P(x))$
  - **Propiedades de la divisibilidad:** Sean  $a(x), b(x), c(x), s(x), t(x) \in K[x]$ 
    - (i) Si  $a(x) \mid b(x)$  y  $a(x) \mid c(x) \Rightarrow a(x) \mid s(x)b(x) + t(x)c(x)$
    - (ii) Si  $a(x) \mid b(x)$  y  $b(x) \mid c(x) \Rightarrow a(x) \mid c(x)$
    - (iii) Si  $a(x) \mid b(x) \Rightarrow a(x)s(x) \mid b(x)s(x)$ . La recíproca es cierta si  $s(x) \neq 0$ .
  - **Definición 3:** Si  $P(x) \in K[x]$ , los polinomios de la forma  $c \cdot P(x)$  con  $c$  constante no nula se llaman polinomios **ASOCIADOS** a  $P(x)$ . Es fácil ver que la relación “ser asociado de” es una relación de equivalencia.

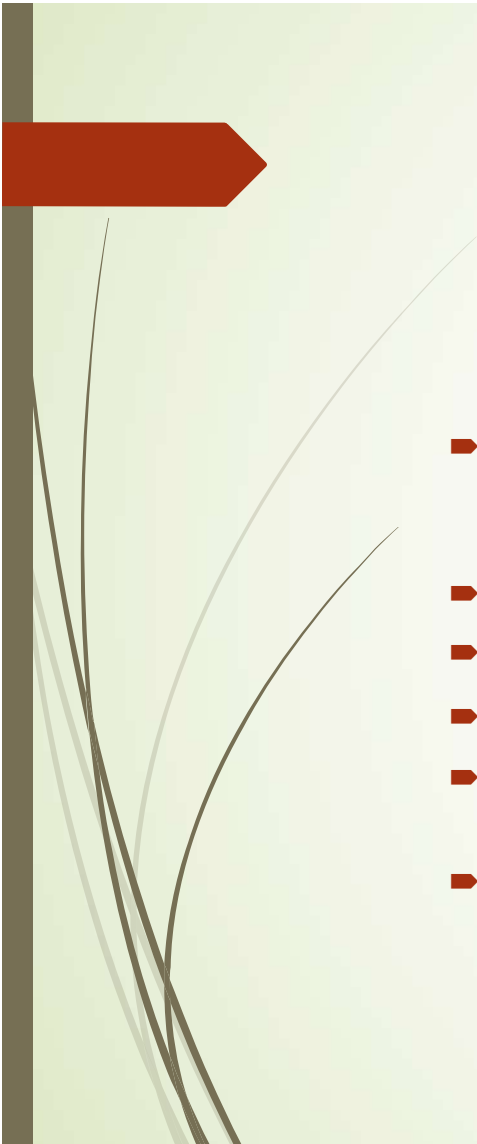
- 
- **Proposición 4:** Si  $a(x), b(x) \in K[x]$ , entonces:
  - $a(x)$  es asociado a  $b(x) \Leftrightarrow$  se dividen mutuamente, es decir:  $a(x) \mid b(x)$  y  $b(x) \mid a(x)$
  - **Demostración:** Supongamos que son asociados. Como  $a(x) = c \cdot b(x)$  ya vimos en el lema 1 que  $a(x)$  divide a  $b(x)$ , por otro lado, que  $b(x)$  divide a  $a(x)$  es trivial.
  - Recíprocamente, si suponemos que se dividen mutuamente, tenemos que existen  $u(x), v(x) \in K[x]$  con:
  - $b(x) = a(x) u(x)$ , y  $a(x) = b(x) v(x)$ , de donde:  $b(x) = b(x) v(x) u(x)$
  - Si fuera  $b(x)$  el polinomio nulo, entonces claramente  $a(x)$  tiene que ser también el polinomio nulo y no hay nada que demostrar. Por lo tanto podemos suponer que no lo es y cancelándolo nos queda:



$$1 = u(x) v(x)$$

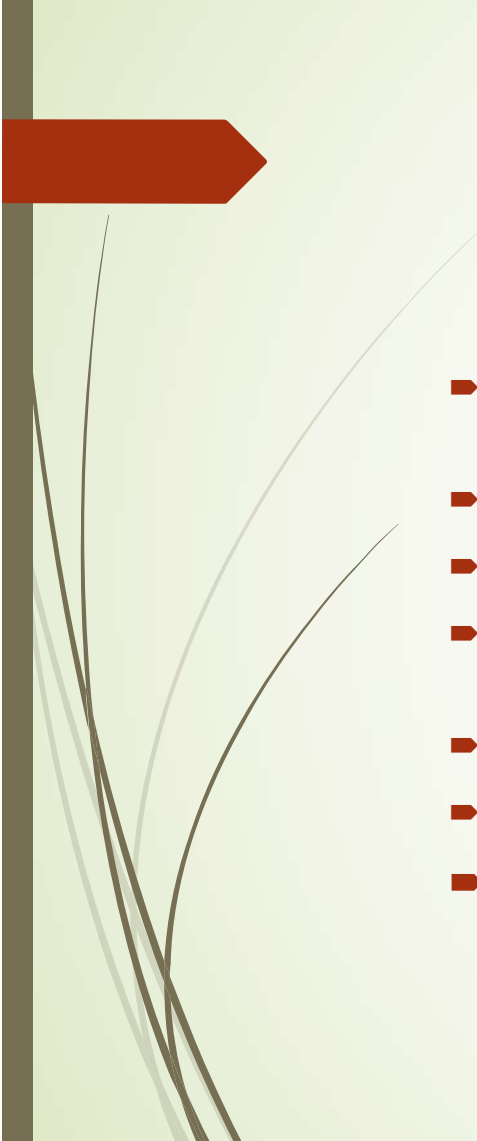
- Es decir que  $u(x)$  y  $v(x)$  tienen inverso, y por lo tanto son ambos constantes y no nulos, lo que prueba que  $a(x)$  y  $b(x)$  son asociados.

Q.E.D.

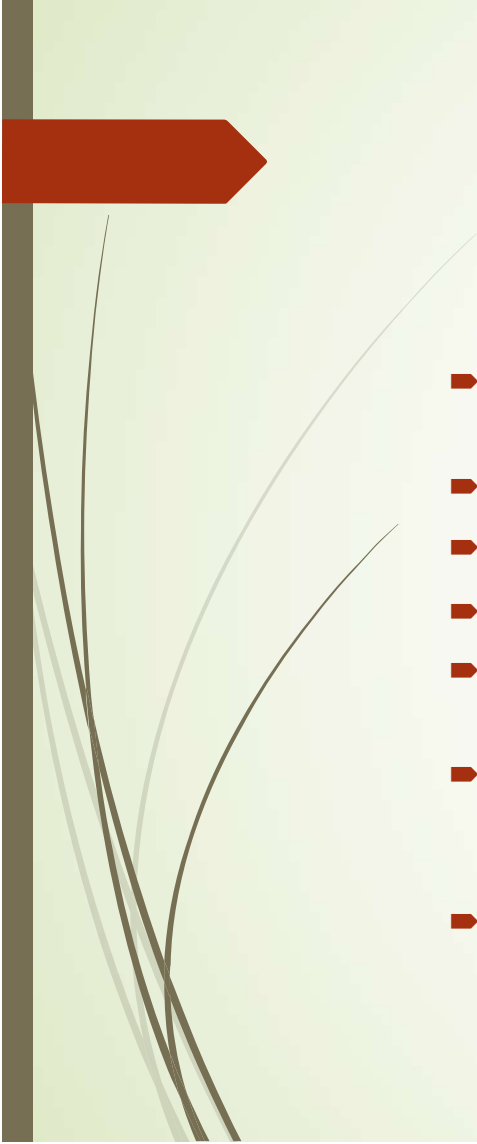
- Proposición 5:** Dos polinomios asociados tienen el mismo conjunto de divisores.
- Demostración: Por la proposición previa dos polinomios  $a(x)$  y  $b(x)$  asociados se dividen mutuamente: luego si  $d(x) \mid a(x)$ , como  $a(x) \mid b(x)$ , se tiene que  $d(x) \mid b(x)$ . Análogamente, todo  $d(x)$  que divide a  $b(x)$  tiene que dividir a  $a(x)$ .

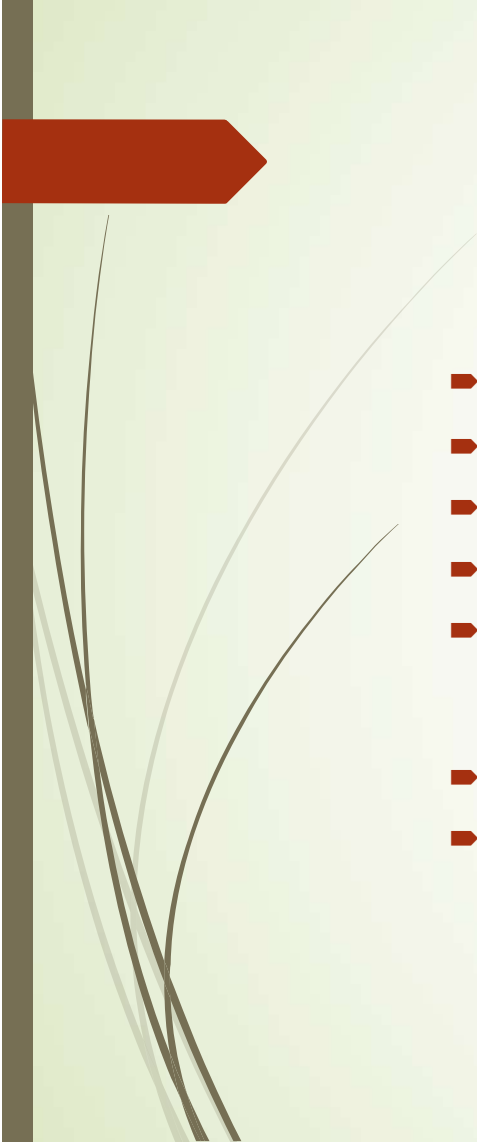
- 
- **Definición 6: Máximo Común Divisor de Polinomios:** Si  $a(x), b(x) \in K[x]$  no ambos nulos, un polinomio  $d(x) \in K[x]$  es máximo común divisor de  $a(x)$  y  $b(x)$  si:
    - (i)  $d(x) \mid a(x)$  y  $d(x) \mid b(x)$
    - (ii) para todo  $s(x) \in K[x]$  tal que  $s(x) \mid a(x)$  y  $s(x) \mid b(x) \Rightarrow s(x) \mid d(x)$
  - Denotaremos  $\text{mcd}(a(x), b(x))$  a un máximo común divisor de  $a(x)$  y  $b(x)$ .
  - **Proposición 7:** (i) Si  $d(x)$  y  $d'(x) \in K[x]$  son ambos máximo común divisor de  $a(x), b(x) \in K[x]$ , entonces  $d(x)$  y  $d'(x)$  son asociados.
  - (ii) Si  $d(x)$  es máximo común divisor de  $a(x)$  y  $b(x)$ , entonces todo asociado de  $d(x)$  también lo es.

- 
- Demostración: (i) Como  $d(x)$  es  $\text{mcd}(a(x), b(x))$  y  $d'(x)$  es un divisor común, se tiene:  $d'(x) \mid d(x)$ . Análogamente (mismo argumento, intercambiando los papeles de  $d(x)$  y  $d'(x)$ ):  $d(x) \mid d'(x)$ .
  - Por la proposición 4, concluimos que  $d(x)$  y  $d'(x)$  son asociados.
  - (ii) Sea  $d(x)$  un  $\text{mcd}(a(x), b(x))$ , y sea  $c \in K$  constante no nula. Consideramos  $c d(x)$ . Como  $d(x) \mid a(x)$ , vemos que  $d(x) \mid c^{-1} a(x)$ . De aquí:  $c d(x) \mid a(x)$ .
  - Análogamente, como  $d(x) \mid b(x)$ , concluimos que  $c d(x) \mid b(x)$ .
  - Es decir que  $c d(x)$  es un divisor común de  $a(x)$  y  $b(x)$ .
  - Sea  $s(x)$  un divisor común de  $a(x)$  y  $b(x)$ . Luego,  $s(x) \mid d(x)$ , de donde se tiene que  $s(x) \mid c d(x)$ . Es decir que todo divisor común de  $a(x)$  y  $b(x)$  divide a  $c d(x)$ . Queda pues probado que  $c d(x) = \text{mcd}(a(x), b(x))$ .

- 
- Conclusión: Los mcd de dos polinomios forman exactamente una clase de equivalencia módulo la relación “asociados”.
  - **Proposición:** Si  $a(x), b(x), c(x) \in K[x]$  no nulos, se tiene que:
  - $\text{mcd}(a(x), b(x)) = \text{mcd}(a(x)-c(x)b(x), b(x))$
  - Demostración: Es fácil ver que los divisores comunes de ambos lados son los mismos, por las propiedades de la divisibilidad:
  - $d \mid a$  y  $d \mid b \Rightarrow d \mid a-cb$ .
  - Recíprocamente: si  $d \mid a-cb$  y  $d \mid b \Rightarrow d \mid a-cb$  y  $d \mid cb \Rightarrow d \mid a$
  -



- 
- **Algoritmo de Euclides en  $K[x]$ :** Sean  $a(x), b(x) \in K[x]$  no nulos, con  $\text{gr}(a) \geq \text{gr}(b)$ . Dividiendo:
  - $a(x) = b(x) q(x) + r_0(x)$ , con  $\text{gr}(r_0(x)) < \text{gr}(b(x))$ .
  - Por la proposición previa:
  - $\text{mcd}(a(x), b(x)) = \text{mcd}(a(x) - b(x)q(x), b(x)) = \text{mcd}(b(x), r_0(x))$ .
  - Si  $r_0(x) = 0 \Rightarrow b(x) \mid a(x)$  y  $\text{mcd}(a(x), b(x)) = \text{mcd}(b(x), 0) = b(x)$ , y aquí acaba el algoritmo.
  - Si  $r_0(x) \neq 0 \Rightarrow$  dividimos  $b(x)$  entre  $r_0(x)$ , y si  $r_1(x)$  es el resto de esta división, si este resto es 0 deducimos que  $\text{mcd}(a(x), b(x)) = \text{mcd}(b(x), r_0(x)) = \text{mcd}(r_0(x), r_1(x)) = \text{mcd}(r_0(x), 0) = r_0(x)$ .
  - Si  $r_1(x) \neq 0$  procedemos con la división de  $r_0(x)$  entre  $r_1(x)$  y así sucesivamente.

- 
- En fórmulas:
  - $b(x) = r_0(x)q_1(x) + r_1(x)$ , con  $\text{gr}(r_1(x)) < \text{gr}(r_0(x))$
  - $r_0(x) = r_1(x)q_2(x) + r_2(x)$ , con  $\text{gr}(r_2(x)) < \text{gr}(r_1(x))$ , .....
  - $r_i(x) = r_{i+1}(x)q_{i+2}(x) + r_{i+2}(x)$ , con  $\text{gr}(r_{i+2}(x)) < \text{gr}(r_{i+1}(x))$
  - Hasta llegar a  $r_{n+1}(x) = 0$ , cosa que ocurrirá pues el grado va decreciendo en la sucesión de los  $r_i(x)$ , con lo cual tras un número finito de pasos se llegará al polinomio nulo, que es el de menor grado.
  - Concluimos de la proposición previa que:
  - $\text{mcd}(a(x), b(x)) = \text{mcd}(b(x), r_0(x)) = \text{mcd}(r_0(x), r_1(x)) = \dots = \text{mcd}(r_n(x), 0) = r_n(x)$ , es decir, el mcd es el último resto no nulo que aparece en el Algoritmo de Euclides.

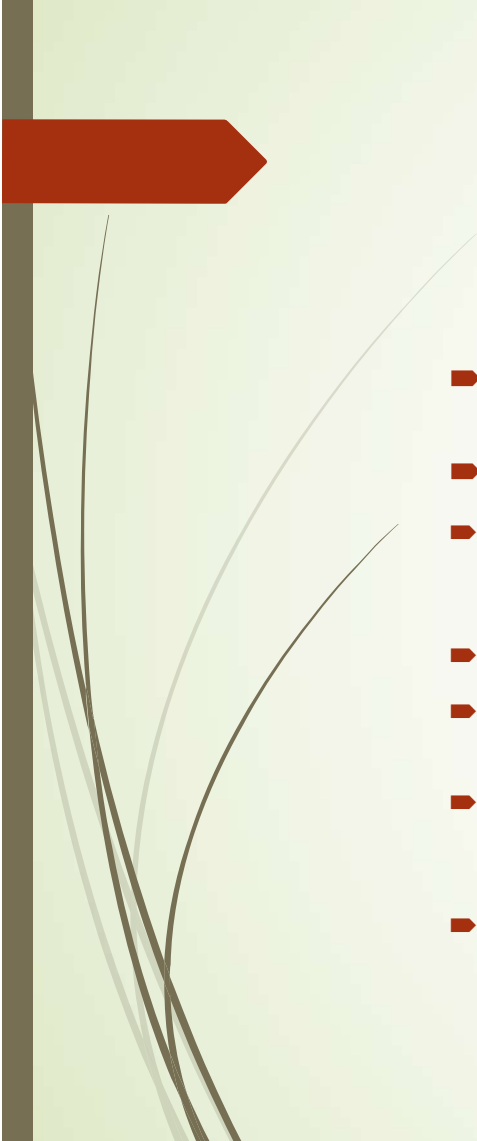


➤ Con idéntica demostración a la vista en el caso de  $\mathbb{Z}$ , de aquí se deduce:

➤ **Proposición (Identidad de Bézout):** Si  $a(x), b(x) \in K[x]$  no ambos 0 y  $d(x)$  es máximo común divisor de  $a(x)$  y  $b(x)$ , entonces existen  $s(x), t(x) \in K[x]$  tales que:  $s(x) a(x) + t(x) b(x) = d(x)$ .

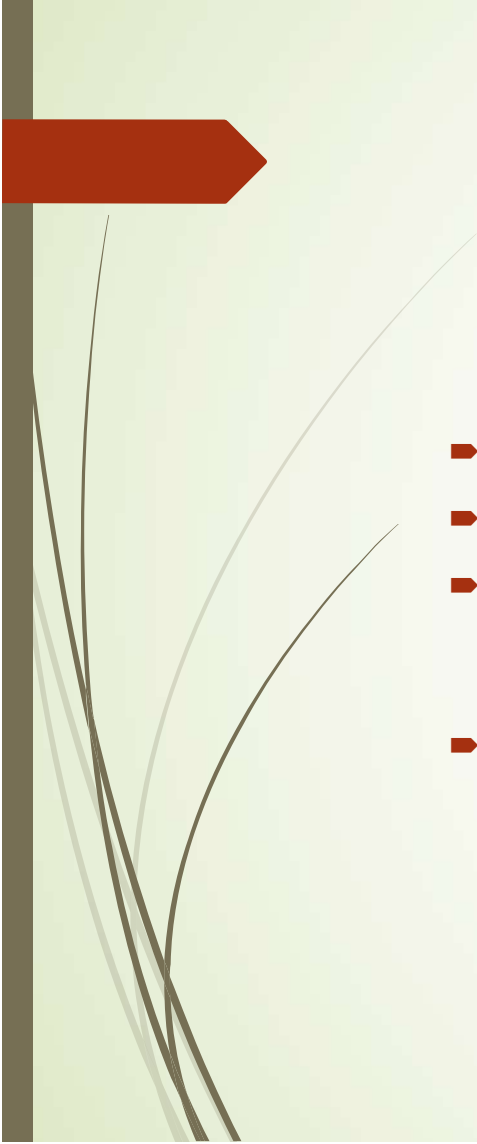
➤ **Polinomios Irreducibles y descomposición**


➤ Recordar que en  $K[x]$  las unidades, es decir, los polinomios que admiten un polinomio que sea su inverso multiplicativo, son los polinomios constantes no nulos (es decir, los de grado 0).

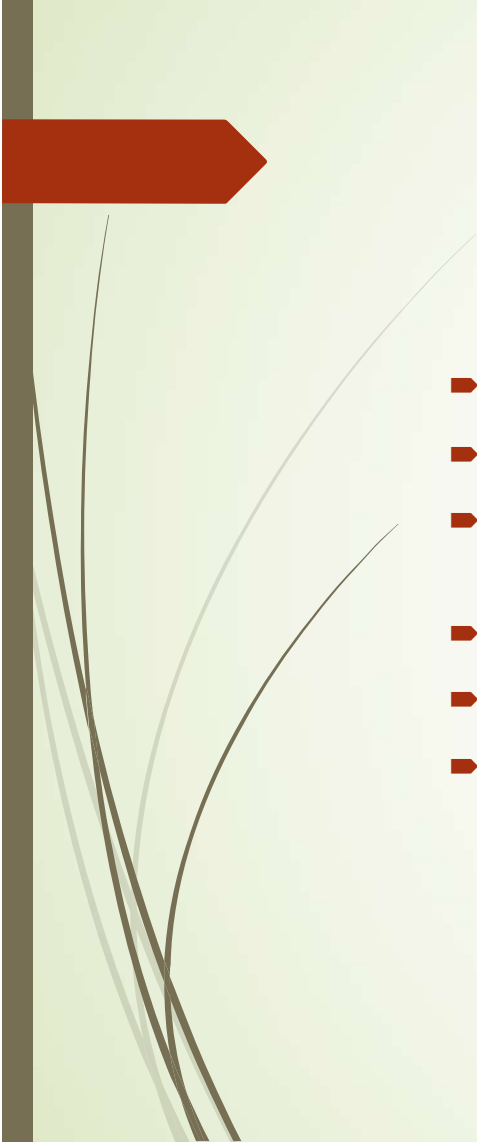
- 
- **Definición:** Sea  $P(x) \in K[x]$  de grado mayor que 0, decimos que  $P(x)$  es irreducible si no puede descomponerse como:
  - $P(x) = f(x) g(x)$  con  $\text{gr}(f(x)) < \text{gr}(P(x))$  y  $\text{gr}(g(x)) < \text{gr}(P(x))$ .
  - **Propiedad:** Un polinomio  $P(x)$  de grado 1 siempre es irreducible, pues en este caso de la fórmula  $P(x) = f(x)g(x)$  se ve que los grados de  $f$  y  $g$  tienen que ser 0 y 1.
  - Ejemplo: El polinomio  $x^2+1$  es irreducible en  $\mathbb{Q}[x]$  y en  $\mathbb{R}[x]$ .
  - **Proposición:** Si  $P(x) \in K[x]$  es irreducible, sus únicos divisores son los polinomios constantes  $c$  y los asociados  $c \cdot P(x)$ , con  $c \in K$  no nulo.
  - Demostración: Ya vimos (Lema 1) que estos son divisores de  $P(x)$ . Por otro lado, por ser irreducible sus únicas descomposiciones posibles serán con un factor de grado 0 y otro de grado  $n = \text{gr}(P(x))$ , luego serán de la forma:
  - $P(x) = c \cdot (c^{-1}P(x))$ , con lo cual sus únicos divisores son constantes o asociados.




## → Clase 6

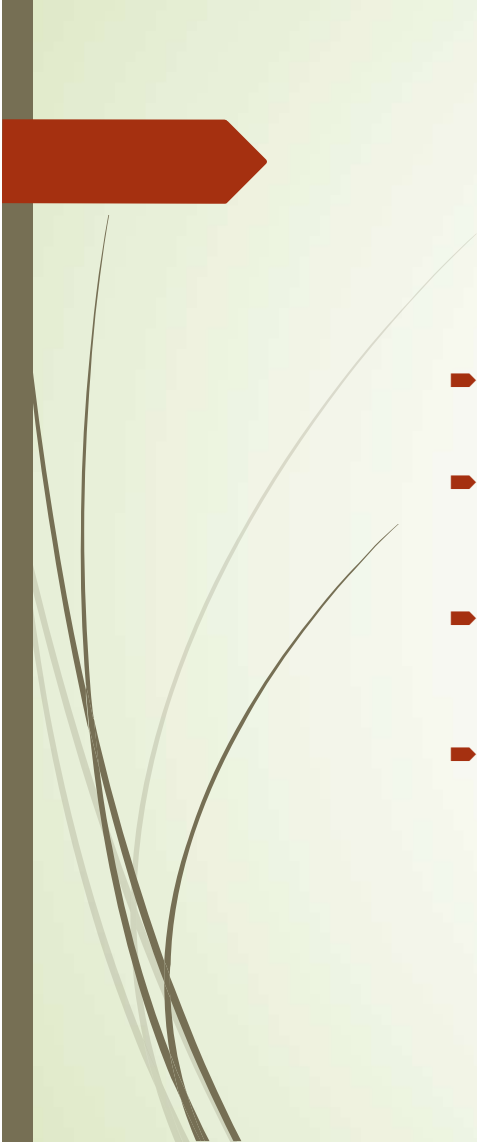
- 
- **Proposición:** Si  $P(x) \in K[x]$ ,  $c \in K$  no nulo, se tiene:
  - $P(x)$  irreducible  $\Leftrightarrow c \cdot P(x)$  irreducible
  - Demostración: Si  $c \cdot P(x)$  es irreducible, es claro que  $P(x)$  también pues una descomposición no trivial:  $P(x) = f(x) \cdot g(x)$  con  $\text{gr}(f) < \text{gr}(P)$  y  $\text{gr}(g) < \text{gr}(P)$  daría lugar a una descomposición no trivial de  $c \cdot P(x)$ :
  - $c \cdot P(x) = (c \cdot f(x)) \cdot g(x)$ . La recíproca se prueba con el mismo argumento, de hecho  $P(x)$  y  $c \cdot P(x)$  son asociados, que es una relación simétrica.

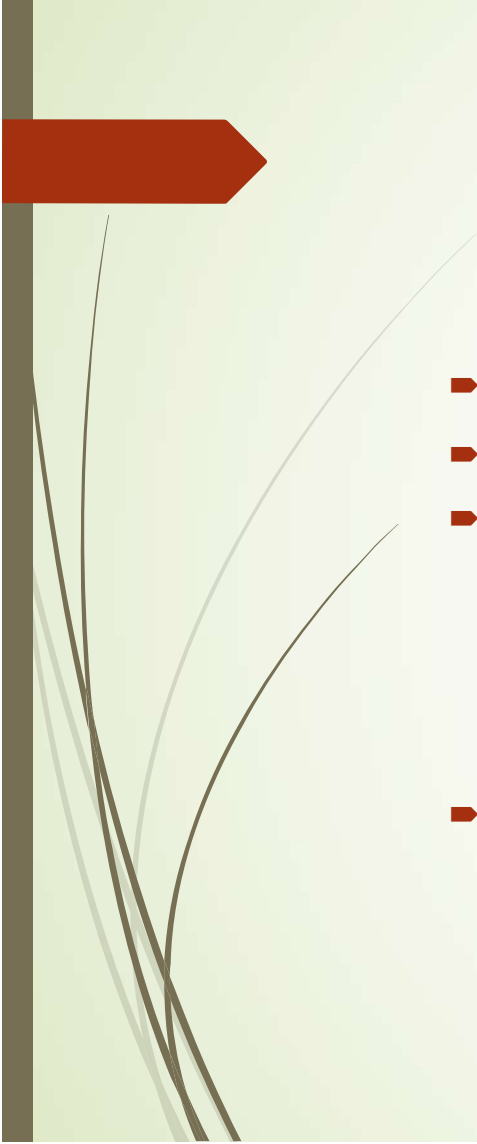
- 
- **Proposición:** Sean  $P(x)$  irreducible en  $K[x]$ . Sea  $a(x) \in K[x]$ . Entonces:
  - O bien  $P(x) \mid a(x)$ , o bien  $\text{mcd}(P(x), a(x)) = 1$ .
  - Demostración: Sea  $d(x) = \text{mcd}(P(x), a(x))$ . Como  $d(x) \mid P(x)$ , sabemos que es constante  $c$  (no nulo) o un polinomio  $c \cdot P(x)$  asociado a  $P(x)$ .
  - Si  $d(x) = c$  es constante, podemos tomar  $d(x) = 1$  (pues  $c$  y  $1$  son asociados: recordar que los mcd de dos polinomios son toda una clase de equivalencia de la relación asociados).
  - Si  $d(x) = c \cdot P(x)$ , también podemos tomar  $\text{mcd}(P(x), a(x)) = P(x)$ . En este caso concluimos que  $P(x)$  divide a  $a(x)$ .
  - Veamos ahora el análogo al Lema Fundamental de la Aritmética:


- 
- **Proposición:** Sea  $P(x)$  irreducible en  $K[x]$ . Si  $P(x) \mid a(x) \cdot b(x) \Rightarrow$
  - $P(x) \mid a(x)$  o  $P(x) \mid b(x)$ .
  - Demostración: Supongamos que  $P(x)$  no divide a  $a(x)$ . Por la proposición previa, tenemos que  $\text{mcd}(P(x), a(x)) = 1$ . Aplicando la identidad de Bézout:
  - Existen  $s(x), t(x)$  tales que:  $P(x) s(x) + a(x) t(x) = 1$ .
  - Multiplicando por  $b(x)$  obtenemos:
  - $P(x) b(x) s(x) + a(x) b(x) t(x) = b(x)$ , y aquí vemos que el primer sumando (de la suma que está a la izquierda del  $=$ ) es divisible por  $P(x)$ , y el segundo también lo es por la hipótesis  $P(x) \mid a(x)b(x)$ , luego concluimos que  $P(x)$  divide a la suma, es decir:  $P(x) \mid b(x)$ .



- 
- Aplicando inducción sobre el número de factores, de aquí se deduce fácilmente (tal como hicimos en  $\mathbb{Z}$ ):
  - **Corolario:** Sea  $P(x) \in K[x]$  irreducible. Si se tiene que:
  - $P(x) \mid a_1(x) \cdot a_2(x) \cdot \dots \cdot a_r(x)$ , entonces para algún  $i \in \{1, 2, \dots, r\}$  se tiene que:
  - $P(x) \mid a_i(x)$ .
  - Finalmente, deducimos de aquí el Teorema de Descomposición en factores Irreducibles, que es el análogo para polinomios del Teorema Fundamental de la Aritmética.

- 
- **Teorema:** Sea  $f(x) \in K[x]$  de grado mayor que 0. Entonces,  $f(x)$  descompone como producto de polinomios irreducibles:  $f(x) = P_1(x) \cdot P_2(x) \cdot \dots \cdot P_r(x)$ .
  - Si se tiene otra descomposición en producto de irreducibles:  $f(x) = Q_1(x) \cdot Q_2(x) \cdot \dots \cdot Q_s(x)$ , entonces  $r=s$  y, tras reordenar apropiadamente, se tiene que  $P_i(x)$  y  $Q_i(x)$  son asociados, para todo  $i=1,2,\dots,r$ .
  - **Demostración: Existencia:** Lo hacemos por inducción. Si  $f(x)$  es irreducible el resultado es trivial, en particular esto prueba lo que queremos para todo polinomio de grado 1 (base de la inducción).
  - Si  $f(x)$  no es irreducible, entonces:  $f(x) = f_1(x) \cdot f_2(x)$ , con ambos factores de grado menor al grado de  $f$ . Por lo tanto, podemos aplicar la hipótesis de inducción para afirmar que tanto  $f_1(x)$  como  $f_2(x)$  se pueden descomponer como producto de irreducibles. Por lo tanto, está claro que  $f(x)$  también se puede descomponer de este modo.

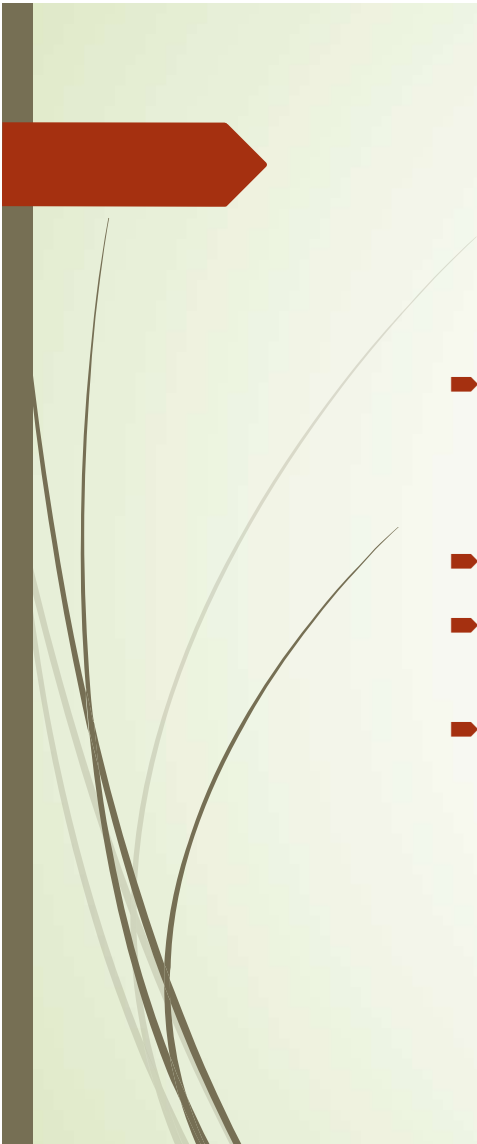
- 
- Unicidad: Se prueba como en el caso de  $\mathbb{Z}$ , partiendo del corolario previo.
  - En la igualdad:
  - $P_1(x) \cdot P_2(x) \cdot \dots \cdot P_r(x) = Q_1(x) \cdot Q_2(x) \cdot \dots \cdot Q_s(x)$ , como  $P_1(x)$  es irreducible y divide a un producto, tiene que dividir a algún  $Q_i(x)$ , por simplicidad pongamos que  $P_1(x) \mid Q_1(x)$ . Como  $Q_1(x)$  es irreducible y  $P_1(x)$  tiene grado positivo (por definición de irreducible), tienen que ser asociados:  $P_1(x) = c_1 Q_1(x)$ . Por lo tanto, cancelo  $P_1$  y  $Q_1$  en la igualdad anterior, poniendo la constante  $c_1$  al inicio:  $c_1 \cdot P_2(x) \cdot P_3(x) \cdot \dots \cdot P_r(x) = Q_2(x) \cdot Q_3(x) \cdot \dots \cdot Q_s(x)$ .
  - Iterando el razonamiento, concluimos que  $P_2(x)$  es asociado de  $Q_2(x)$  y así sucesivamente que cada  $P_i(x)$  es asociado de un  $Q_i(x)$ . Es fácil ver que tiene que ser  $r=s$  pues si no fuera así se llegaría a una igualdad entre una constante y un producto de polinomios de grado positivo.

- 
- Observación: Si trabajamos con polinomios irreducibles mónicos, logramos que los factores irreducibles queden unívocamente determinados. Es decir, vemos que:
  - Si  $f(x) \in K[x]$  tiene grado mayor que 0, y coeficiente principal  $a_n$ , se tiene:
  - $f(x) = a_n \cdot P_1(x) \cdot P_2(x) \cdot \dots \cdot P_r(x)$  donde los  $P_i$  son mónicos e irreducibles. Una tal descomposición en mónicos e irreducibles es única excepto por el orden de los factores.




## ➤ Raíces de Polinomios (aplicadas a la descomposición)

- Podemos ver a un polinomio  $P(x)$  como una función de  $K$  en  $K$ , es decir, sustituyendo la  $x$  por un valor  $k \in K$  obtenemos su imagen  $P(k) \in K$ . Son particularmente útiles las raíces de un polinomio, que son aquellos valores  $k \in K$  tales que  $P(k)=0$  (si es que los hay).
- **Teorema del resto:** Si  $k \in K$  y  $P(x) \in K[x]$ , el valor  $P(k)$  coincide con el resto de dividir  $P(x)$  por  $(x - k)$ .
- Demostración: Como  $x - k$  es de grado 1, está claro que el resto de dividir  $P(x)$  por  $(x - k)$  será un polinomio constante  $r$ . Se tiene:
- $P(x) = (x - k) Q(x) + r$ . En esta igualdad, evaluando ambos miembros en  $k$ , obtenemos:  $P(k) = 0 + r = r$ .

- 
- En particular,  $P(k) = 0$  (o sea,  $k$  raíz de  $P$ ) equivale a que el resto de dividir  $P(x)$  por  $(x - k)$  es 0, es decir, a que  $(x - k) \mid P(x)$ . Es decir, se tiene:

- $k \text{ es raíz de } P(x) \Leftrightarrow (x - k) \mid P(x)$

- Por lo tanto, cada vez que se tiene una raíz  $k \in K$  de  $P(x)$ , ésta da lugar a un factor de grado 1, y por lo tanto irreducible, de  $P(x)$ .
- Ejemplo: Esto explica porqué  $x^2 + 1$  es irreducible en  $\mathbb{R}[x]$ . Como es de grado DOS, si fuera reducible en  $\mathbb{R}[x]$ , tendría que tener un factor de grado 1, que si lo tomamos mónico sería un factor de la forma  $(x - k) \in \mathbb{R}[x]$ , y por el resultado anterior tendríamos que  $k \in \mathbb{R}$  es raíz de  $x^2 + 1$ . Como esto es falso, pues  $k^2 + 1 \geq 1, \forall k \in \mathbb{R}$ , deducimos la irreducibilidad del polinomio.

- 
- Observación: En el ejemplo anterior, por ser un polinomio de grado DOS, ser reducible en  $K[x]$  equivale a tener un factor de grado 1 en  $K[x]$ , y por lo tanto equivale a tener una raíz en  $K$ . Para polinomios de grado mayor (en realidad es fácil ver que para grado 3 el argumento también funciona, es a partir de grado 4 donde no es cierto) la equivalencia no se cumple: un polinomio puede no tener raíces en  $K$  pero a pesar de ellos ser reducible, lo que pasa es que sus factores irreducibles no serán de grado 1.
  - **Definición:** Si  $c \in K$  es raíz de  $P(x) \in K[x]$ , decimos que tiene multiplicidad  $i$  si  $i$  es la mayor potencia tal que:  $(x - c)^i \mid P(x)$ . Está claro que se tiene  $i \geq 1$ .
  - Observación: Por lo tanto, si se tienen  $s$  raíces  $c_1, c_2, \dots, c_s$  de  $P(x) \in K[x]$  con multiplicidades  $e_1, e_2, \dots, e_s$ , respectivamente, se tiene que existe un polinomio  $Q(x) \in K[x]$  con:
  - $P(x) = (x - c_1)^{e_1} \cdot (x - c_2)^{e_2} \cdot \dots \cdot (x - c_s)^{e_s} \cdot Q(x)$ , en particular, vemos que:  $e_1 + e_2 + \dots + e_s \leq \text{gr}(P(x))$ .