

Lista 1. Anillo de Polinomios.

1. Sea A un anillo comutativo con identidad, y sea $I = \{f \in A[[x]] \mid o(f) > 0\} \cup \{0\}$

Pruebe lo siguiente:

- a) $I = \langle x \rangle$.
- b) $I^n = \{f \in A[[x]] \mid o(f) \geq n\} \cup \{0\}$ para cada $n \in \mathbb{N}$.
- c) $\bigcap_{n \geq 1} I^n = \{0\}$.

Dem:

De a): Seu $f \in I$ Serie de potencias no cero, entonces $o(f) > 0$. Por una proposición, $\exists g \in A[[x]]$ m $o(g) = 0$ y $f = x^{o(f)} g$, donde $x^{o(f)} g \in \langle x \rangle$ (pues $o(f) \geq 1$ y $\langle x \rangle$ es un ideal de $A[[x]]$). Así $f \in \langle x \rangle$.

Seu ahora $g \in \langle x \rangle$ Serie de potencias no cero. Se tiene que:

$$g = h \cdot x, \text{ con } h \in A[[x]]$$

donde h es una serie de potencias no cero. Por una proposición:

$$\begin{aligned} o(g) &= o(h \cdot x) \\ &\geq o(h) + o(x) \\ &\geq 1 \\ &> 0 \end{aligned}$$

Luego $g \in I$.

De b): Procederemos por inducción sobre n . Para $n=2$ se cumple, en efecto:

$$\begin{aligned} I^2 &= \left\{ \sum_{i=1}^n f_i g_i \mid f_i, g_i \in I, \forall i \in [1, n] \right\} \cup \{0\} \\ &= \left\{ \sum_{i=1}^n f_i g_i \mid o(f_i), o(g_i) \geq 1, \forall i \in [1, n] \right\} \cup \{0\} \end{aligned}$$

Pero $o\left(\sum_{i=1}^n f_i g_i\right) \geq \min_{i \in [1, n]} \{o(f_i g_i)\} \geq \min_{i \in [1, n]} \{o(f_i) + o(g_i)\} \geq \min_{i \in [1, n]} \{2\} = 2$. Luego:

$$I^2 \subseteq \{f \in A[[x]] \mid o(f) \geq 2\}$$

Si $h \in \{f \in A[[x]] \mid o(f) \geq 2\}$, entonces $o(h) \geq 2$, así $\exists f_i \in A[[x]]$ m $o(f_i) = 0$ y:

$$h = x^{o(h)} f_i$$

$$= x^{o(h)-1} \cdot (x f_1)$$

donde $x^{o(h)-1}, x f_1 \in I$, pues $o(x^{o(h)-1}) = o(h)-1 \geq 1 > 0$ y $o(x f_1) \geq o(x) + o(f_1) = 1 + 0 = 1 > 0$.

Así, $h \in I^2$.

El paso inductivo es análogo.¹⁾

D) Claramente $\{0\} \subseteq \bigcap_{n=1}^{\infty} I^n$. Si $f \in \bigcap_{n=1}^{\infty} I^n$ con f serie de pot. no cero, entonces $o(f) \geq n, \forall n \in \mathbb{N}$, lo cual no puede suceder pues \mathbb{N} no es acotado sup. Luego $f=0$. □

2. Sea A un anillo comunitativo con identidad. Pruebe que si A es anillo local, entonces también lo es $A[[x]]$.

Dem:

Suponga que A es anillo local, entonces A admite un único ideal maximal. Como $A[[x]]$ es finitamente generado (pues $A[[x]] = \langle 1 \rangle$), entonces $A[[x]]$ admite la existencia de ideales maximales.

Sean $M', M'' \subseteq A[[x]]$ ideales maximales. Probaremos que $M' = M''$.

Definu:

$$N' = \{a \in A \mid f(0) = a, \text{ con } f \in M'\}$$

$$N'' = \{a \in A \mid f(0) = a, \text{ con } f \in M''\}$$

Claramente $N' \neq \emptyset \neq N''$, pues $0 \in N', N''$. Probaremos que N' y N'' son ideales maximales de A .

1) Son ideales: Sean $a_1, b_1 \in N'$, $a_2, b_2 \in N''$ y $r \in A$, entonces $\exists f_1, g_1 \in N'$ y $f_2, g_2 \in N''$ m

$$a_1 = f_1(0), b_1 = g_1(0) \quad y \quad a_2 = f_2(0), b_2 = g_2(0)$$

Como N' y N'' son ideales de $A[[x]]$, entonces $f_1 - g_1 \in N'$, $f_2 - g_2 \in N''$ y $rf_1 \in N'$, $rf_2 \in N''$. Por tanto:

$$(f_1 - g_1)(0) = a_1 - b_1 \in N' \quad rf_1(0) = ra_1 \in N'$$

$$(f_2 - g_2)(0) = a_2 - b_2 \in N'' \quad rf_2(0) = ra_2 \in N''$$

2) Son maximales.

3. Sea A un anillo comutativo con identidad. Deduzca lo siguiente:

- a) Ningún polinomio mónico en $A[x]$ es un divisor de cero;
- b) Si el polinomio $f(x) = a_0 + a_1x + \dots + a_nx^n$ es un divisor de cero en $A[x]$, entonces existe un elemento $a \in A$, $a \neq 0$, tal que $af(x) = 0$. (Sugerencia: Supóngase que $f(x)g(x) = 0$. Use el polinomio $a_k g(x)$ para obtener un polinomio $h(x)$ de $A[x]$, $h(x) \neq 0$, tal que $h(x)f(x) = 0$ con $\deg(h) < \deg(f)$).

Dem:

De a): Sea $f(x) \in A[x]$ un polinomio mónico, i.e. $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$. Si $g(x) = b_m x^m + \dots + b_0 \in A[x] \setminus \{0\}$, entonces:

$$\begin{aligned} f(x)g(x) &= (x^n + \dots + a_0)(b_m x^m + \dots + b_0) \\ &= (1 \cdot b_m)x^{m+n} + \dots + a_0 b_0 \\ &= b_m x^{m+n} + \dots + a_0 b_0 \end{aligned}$$

El cual es un polinomio el cual no puede ser 0, pues $b_m \neq 0$. Luego $f(x)$ no es div. de cero.

De b): Como $f(x)$ es div. de cero, $\exists g(x) \in A[x] \setminus \{0\}$ m $f(x)g(x) = 0$. Sea $g(x)$ el polinomio de grado mínimo m $f(x)g(x) = 0$, i.e si $h(x) \in A[x]$ es tal que:

$$f(x)h(x) = 0$$

ent. $h(x) = 0$ o $\text{grad}(g(x)) \leq \text{grad}(h(x))$. Supongamos que no se cumple el resultado, ent. $\text{grad}(g(x)) \geq 1$.

Veamos que $\exists K \in [0, n]$ m $a_K g(x) \neq 0$.

Si $a_K g(x) = 0$, $\forall K \in [0, n]$, ent. $a_K b_m = 0$, $\forall K \in [0, n] \Rightarrow b_m f(x) = 0 \nparallel_c$. Por tanto, tal $K \in [0, n]$ existe. Tomamos $K_0 \in [0, n]$ el máx. m $a_{K_0} g(x) \neq 0$.

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1 x + \dots + a_{K_0} x^{K_0} + \dots + a_n x^n)g(x) \\ &= a_0 g(x) + a_1 g(x)x + \dots + a_{K_0} g(x)x^{K_0} + \dots + a_n g(x)x^n \\ &= (a_0 + a_1 x + \dots + a_{K_0} x^{K_0})g(x) \\ &= 0 \end{aligned}$$

$\Rightarrow a_{K_0} b_m = 0$, luego $\text{grad}(a_{K_0} g(x)) < \text{grad}(g(x))$ y $f(x) \cdot a_{K_0} g(x) = 0 \nparallel_c$, por mínima.

Lidad de g . Luego, $\exists a \in A \setminus \{0\}$ m $a f(x) = 0$.



4. Sea A un anillo comutativo con identidad. Pruebe que el polinomio $1+ax$ es unidad en $A[x]$ si, y solo si a es elemento nilpotente de A .

Dem:

$\Rightarrow)$ Suponga que $1+ax$ es unidad en $A[x]$, i.e. $\exists g(x) \in A[x]$ m $(1+ax)g(x)=1$. Digamos que

$g(x) = b_0 + b_1 x + \dots + b_n x^n$. Se tiene entonces que (con $b_n \neq 0$):

$$(1+ax)g(x) = (1+ax) \cdot (b_0 + b_1 x + \dots + b_n x^n)$$

$$= b_0 + b_1 x + \dots + b_n x^n + ab_0 x + ab_1 x^2 + \dots + ab_n x^{n+1}$$

$$= b_0 + (b_1 + ab_0)x + \dots + (b_i + ab_{i-1})x^i + \dots + (b_n + ab_{n-1})x^n + ab_n x^{n+1}$$

$$= 1$$

Luego, $b_0 = 1$, $b_k + ab_{k-1} = 0$, $\forall k \in [1, n]$ y $ab_n = 0$. Tenemos entonces el sistema de ecs:

$$\left\{ \begin{array}{l} b_0 = 1 \\ b_1 + ab_0 = 0 \\ b_2 + ab_1 = 0 \\ \vdots \\ b_n + ab_{n-1} = 0 \\ ab_n = 0 \end{array} \right.$$

de donde $b_1 + a = 0 \Rightarrow b_1 = -a$, $b_2 = a^2$, ..., $b_n = (-a)^n$ y $ab_n = (-1)^n a^{n+1} = 0$. Así, $\exists m \in \mathbb{N}$ m $a^m = 0$ ($m = n+1$).

Luego a es nilpotente.

$\Leftarrow)$ Suponga que a es nilpotente, $\exists m \in \mathbb{N}$ m $a^m = 0$. Veamos que:

$$(1+ax)(1-ax+a^2x^2+\dots+(-1)^m a^m x^m) = (1-ax+a^2x^2+\dots+(-1)^m a^m x^m)$$

$$+ ax-a^2x^2+\dots+(-1)^{m-1} a^m x^m + (-1)^m a^{m+1} x^{m+1}$$

$$= 1 + (ax-ax) + (ax^2-a^2x^2) + \dots + (-1)^m (a^m x^m - a^m x^m) + (-1)^m a^{m+1} x^{m+1}$$

$$= 1$$

Por tanto, $1+ax$ es unidad de $A[x]$.



en $A[x]$ si, y solo si a es elemento nilpotente de A .

5. Sean A y B anillos arbitrarios. Pruebe lo siguiente:

- Si I es un ideal de A , entonces $I[x]$ es un ideal de $A[x]$.
- Si A es isomorfo a B , entonces $A[x]$ y $B[x]$ también lo son.
- $\text{car}(A) = \text{car}(A[x]) = \text{car}(A[[x]])$.
- Si I es un ideal de A consistente de elementos nilpotentes, entonces el ideal $I[x]$ de $A[x]$ también consiste de elementos nilpotentes. (Sugerencia: Use inducción sobre el grado de los polinomios de $I[x]$).

Dem:

De a): Como $I \neq \emptyset$, $I[x] \neq \emptyset$. Sean $f(x) = a_0 + \dots + a_n x^n$, $g(x) = b_0 + \dots + b_m x^m \in I[x]$ y $r(x) = c_0 + \dots + c_s x^s \in A[x]$, entonces $a_i, b_j, c_k \in I$, $\forall i \in [0, n]$ y $\forall j \in [0, m]$. Por tanto si $S = \max\{n, m\}$, definimos (en caso de no estarlo) $a_k = 0$ y $b_k = 0$, $\forall k \in [0, S]$, entonces:

$$f(x) - g(x) = \sum_{i=0}^s (a_i - b_i) x^i \in I[x]$$

Pues $a_i, b_i \in I$, $\forall i \in [0, s]$, luego $a_i - b_i \in I$, $\forall i \in [0, s]$. Ahora:

$$f(x) r(x) = d_0 + d_1 x + \dots + d_{l+n} x^{l+n}$$

donde $d_k = \sum_{i=0}^k a_i b_{k-i}$, $\forall k \in [0, l+n]$. Claramente $d_k \in I$, $\forall k \in [0, l+n]$, pues $a_i b_{k-i} \in I$, $\forall i \in [0, k]$ y así $d_k = \sum_{i=0}^k a_i b_{k-i} \in I$. Luego $f(x) r(x) \in I[x]$.

De b): Como $A \cong B$, $\exists \varphi: A \rightarrow B$ isomorfismo de anillos. Defina $\phi: A[x] \rightarrow B[x]$ dada como sigue:

$$\forall f(x) = a_0 + a_1 x + \dots + a_n x^n \in A[x], \phi(f(x)) = \varphi(a_0) + \varphi(a_1)x + \dots + \varphi(a_n)x^n \in B[x]$$

ϕ está bien definido y:

i) ϕ es homeomorfismo. Sean $f(x) = a_0 + \dots + a_n x^n$ y $g(x) = b_0 + \dots + b_m x^m$, entonces si $S = \max\{n, m\}$ y definimos (en caso de no estarlo) $a_k = 0 = b_k$, $\forall k \in [0, S]$, tenemos que:

$$\begin{aligned} \phi(f(x) + g(x)) &= \phi(a_0 + b_0 + (a_1 + b_1)x + \dots + (a_S + b_S)x^S) \\ &= \varphi(a_0 + b_0) + \dots + \varphi(a_S + b_S)x^S \\ &= \varphi(a_0) + \dots + \varphi(a_S)x^S + \varphi(b_0) + \dots + \varphi(b_S)x^S \\ &= \phi(f(x)) + \phi(g(x)), \text{ por ser } \varphi \text{ homomorfismo.} \end{aligned}$$

Si $f(x)g(x) = c_0 + \dots + c_{n+m} x^{n+m}$, donde $c_k = \sum_{i=0}^k a_i b_{k-i}$, $\forall k \in [0, n+m]$. Entonces:

$$\begin{aligned}
\phi(f(x)g(x)) &= \varphi(c_0) + \varphi(c_1)x + \dots + \varphi(c_{n+m})x^{n+m} \\
&= \varphi(a_0b_0) + \varphi(a_1b_0 + a_0b_1)x + \dots + \varphi(a_nb_m)x^{n+m} \\
&= (\varphi(a_0) + \varphi(a_1)x + \dots + \varphi(a_n)x^n) \cdot (\varphi(b_0) + \varphi(b_1)x + \dots + \varphi(b_m)x^m) \\
&= \phi(f(x)) \cdot \phi(g(x))
\end{aligned}$$

ii) φ es monomorfismo. Sea $f(x) \in A[x]$ y $\phi(f(x)) = 0 \in B[x]$, entonces si $f(x) = a_0 + \dots + a_n x^n$:
 $\Rightarrow \varphi(a_i) = 0, \forall i \in [1, n] \Rightarrow a_i = 0, \forall i \in [1, n] \Rightarrow f(x) = 0$. Por tanto $\text{ker}(\varphi) = \langle 0 \rangle$, luego f es monomorfismo.

iii) $\forall g(x) = b_0 + \dots + b_n x^n \exists f(x) = \varphi^{-1}(b_0) + \dots + \varphi^{-1}(b_n)x^n \in A[x]$ y $\phi(f(x)) = g(x)$.

De c): Tenemos 2 casos:

i) $\text{car}(A) = 0$, entonces $\forall m \in \mathbb{N} \exists a_m \in A$ y $a_m \neq 0$. Luego $\forall m \in \mathbb{N} \exists f(x) = a_m \in A[x]$ y $f = a_m \in A((x))$ y:

$$ma_m = m f(x) = mf \neq 0$$

Por tanto, $\text{car}(A) = \text{car}(A[x]) = \text{car}(A((x)))$.

ii) $\text{car}(A) = n \in \mathbb{N}$, entonces $\forall a \in A, na = 0$. Luego $\forall f(x) = a_0 + \dots + a_n x^n \in A[x]$ y $g = b_0 + b_1 x + \dots \in A((x))$ se cumple:

$$nf(x) = na_0 + \dots + na_n x^n = 0 + \dots + 0x^n = 0$$

$$ng = nb_0 + nb_1 x + \dots = 0 + 0x + \dots = 0$$

Por tanto, $0 < \text{car}(A[x]), \text{car}(A((x))) \leq n$. Pero como $A \hookrightarrow A[x], A((x))$ entonces

$$\text{car}(A) = n = \text{car}(A[x]) = \text{car}(A((x)))$$

De d): Procederemos por inducción sobre el grado n de los polinomios de $I[x]$. Sea $f(x) \in I[x]$ y $\text{grad}(f(x)) = 0$, entonces $f(x) = a$, con $a \in I$. Entonces $\exists m \in \mathbb{N}$ tal que $a^m = 0$, luego:

$$f(x)^m = a^m = 0$$

Por tanto, $f(x) \in I[x]$ es nilpotente. Supongamos que el resultado se cumple para $n=0, 1, \dots, k$. Si $f(x) \in I[x]$

y $\text{grad}(f(x)) = k+1$, ent. si $f(x) = a_0 + \dots + a_k x^k + a_{k+1} x^{k+1}$, donde $a_{k+1} \neq 0$, se tiene que $\exists m_1 \in \mathbb{N}$

ta $a_{k+1}^{m_1} = 0$, y tomando a $g(x) = a_0 + \dots + a_k x^k \in \mathbb{I}[x]$ donde $\text{grad}(g(x)) \leq k$, por hip. de inducción $\exists m_2 \in \mathbb{N}$ ta $g(x)^{m_2} = 0$. Entonces:

$$\begin{aligned} f(x)^m &= f(x)^{m_1 \cdot m_2} \\ &= (a_{k+1} x^{k+1} + g(x))^{m_1 \cdot m_2} \\ &= \left(\sum_{i=0}^{m_2} (a_{k+1} x^{k+1})^i g(x)^{m_2-i} \right)^{m_1} \\ &= \left(g(x)^{m_2} + \sum_{j=1}^{m_1} (a_{k+1} x^{k+1})^j g(x)^{m_2-j} \right)^{m_1} \\ &= \left(a_{k+1} x^{k+1} \cdot \sum_{j=1}^{m_1} (a_{k+1} x^{k+1})^{j-1} g(x)^{m_2-j} \right)^{m_1} \\ &= (a_{k+1} x^{k+1})^{m_1} \cdot \left(\sum_{j=1}^{m_1} (a_{k+1} x^{k+1})^{j-1} g(x)^{m_2-j} \right)^{m_1} \\ &= 0 \end{aligned}$$

Pues A es conmutativo y $(a_{k+1} x^{k+1})^{m_1} = a_{k+1}^{m_1} (x^{k+1})^{m_1} = 0$, con $m = m_1 m_2$. Luego $f(x)$ es nilpotente. □

6. Pruebe las siguientes afirmaciones en el anillo $\mathbb{Z}[x]$:

- a) El ideal $\langle x \rangle$ es un ideal primo de $\mathbb{Z}[x]$, pero no es ideal maximal.
- b) $\mathbb{Z}[x]$ no es un DIP.
- c) El ideal primario $\langle 4, x \rangle$ de $\mathbb{Z}[x]$ no es potencia de ningún ideal primo de $\mathbb{Z}[x]$.

Dem:

De a): Veamos que es primo. Sean $f(x), g(x) \in \mathbb{Z}[x]$ ta $f(x)g(x) \in \langle x \rangle$, entonces $\exists p(x) \in \mathbb{Z}[x]$ tal que:

$$f(x)g(x) = x p(x)$$

Pues $\langle x \rangle = x A(x)$. Si $f(x) = a_0 + \dots + a_n x^n$ y $g(x) = b_0 + \dots + b_m x^m$, entonces $f(x)g(x) = a_0 b_0$

$+ \dots + a_n b_m x^{n+m} = x p(x)$, por tanto como \mathbb{Z} es dominio entero, $a_0 b_0 = 0$, i.e $a_0 = 0$ o $b_0 = 0 \Rightarrow$

$f(x) = a_0 x + \dots + a_n x^n = x(a_0 + \dots + a_n x^{n-1})$ o $g(x) = b_0 x + \dots + b_m x^m = x(b_0 + \dots + b_m x^{m-1})$, i.e $f(x)$

$\in \langle x \rangle$ o $g(x) \in \langle x \rangle$. Por tanto, $\langle x \rangle$ es ideal primo de $\mathbb{Z}[x]$.

De b): Tome:

$$\mathbb{I}[x] = \{ f(x) = a_0 + \dots + a_n x^n \mid a_i \in \mathbb{Z} \text{ y } 2 \nmid a_0, \forall i \in [0, n] \}$$

$\mathbb{I}[x]$ es ideal de $\mathbb{Z}[x]$ (es inmediato), pero no es generado por un elemento, ya que si $g(x) \in \mathbb{Z}[x]$ fuera tal que $\mathbb{I}[x] = \langle g(x) \rangle$, entonces como $2 \in \mathbb{I}[x]$, debe pasar al ser \mathbb{Z} dominio entero que $\text{grad}(g(x)) = 0$, i.e. $g(x) = a_0$, donde $2 \nmid a_0$, pero $2 \in \mathbb{I}[x]$, ent. $a_0 | 2 \Rightarrow 2 = a_0$, pero $\langle 2 \rangle \neq \mathbb{I}[x]$, pues $x+2 \in \mathbb{I}[x]$ pero $x+2 \notin \langle 2 \rangle$. Por tanto $\mathbb{I}[x]$ no es ideal principal, luego $\mathbb{Z}[x]$ no es DIP.

De c):

7. Sea A un anillo commutativo con identidad, y sea P un ideal primo de A . Pruebe que $P[x]$ es ideal primo de $A[x]$. Si M es ideal maximal de $A[x]$, ¿es cierto que $M[x]$ es ideal maximal de $A[x]$?

8. Sea K un campo y $a \in K$. Sea $M_a = \{f(x) \in K[x] \mid f(a) = 0\}$. Pruebe que M_a es ideal maximal de $K[x]$ tal que $K[x]/M_a \cong K$.

Dem:

$M_a \neq \emptyset$ pues $f(x) = 0 \in M_a$ ($f(a) = 0$). Sean $f(x), g(x) \in M_a$ y $r(x) \in K[x]$, ent.

$$f(a) - g(a) = (f-g)(a) = 0 - 0 = 0$$

$$(f \cdot r)(a) = f(a)r(a) = 0$$

$\therefore f(x) - g(x), f(x)r(x) \in M_a$, así M_a es ideal de $K[x]$. Probaremos que es maximal. Sea $h(x) \in K[x] \setminus M_a$, i.e. $h(a) = b \neq 0$ ($b \in A$). Como K es campo, por el algoritmo de la div. $\exists! q(x), r(x) \in K[x]$ m

$$h(x) = (x-a)q(x) + r(x)$$

donde $r(x) = h(a) = b$, ent.

$$\Rightarrow h(x) - (x-a)q(x) = b$$

$$\Rightarrow b^{-1}h(x) - b^{-1}(x-a)q(x) = 1$$

pues $b \neq 0$. Así $b^{-1}h(x) - b^{-1}(x-a)q(x) \in \langle M_a, h(x) \rangle$, pues $b^{-1}(a-a)q(a) = 0$. Luego como M_a es ideal propio de $K[x]$, ent. M_a es maximal.

Sea $H: K[x] \rightarrow K$ dado como:

$$\forall f(x) \in K[x], H(f(x)) = f(a)$$

Claramente $M_a = \text{Ker } H$ y H es epimorfismo. Por el P.T. I:

$$K[x]/_{M_a} \cong K$$

□

9. Dado un polinomio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$, denotamos por $\bar{f}(x) = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$, donde \bar{a}_k denota el conjugado complejo de a_k . Pruebe lo siguiente:

- a) $z \in \mathbb{C}$ es raíz de $f(x)$ si, y solo si \bar{z} es raíz de $\bar{f}(x)$.
- b) Si $f(x) \in \mathbb{R}[x] \subset \mathbb{C}[x]$ y z es raíz de $f(x)$, entonces también lo es \bar{z} .

Dem:

D_e a): $z \in \mathbb{C}$ es raíz de $f(x) \Leftrightarrow f(z) = a_0 + a_1 z + \dots + a_n z^n = 0 \Leftrightarrow \bar{a}_0 + \bar{a}_1 \bar{z} + \dots + \bar{a}_n \bar{z}^n = 0$
 $\Leftrightarrow \bar{a}_0 + \bar{a}_1 \bar{z} + \dots + \bar{a}_n (\bar{z})^n = 0 \Leftrightarrow \bar{f}(\bar{z}) = 0 \Leftrightarrow \bar{z} \text{ es raíz de } \bar{f}(x).$

D_e b): Si $f(x) = a_0 + \dots + a_n x^n \in \mathbb{R}[x]$, ent. $a_i \in \mathbb{R}, \forall i \in [0, n]$, luego $a_i = \bar{a}_i, \forall i \in [0, n] \Rightarrow$
 $\bar{f}(x) = \bar{f}(x)$. Por lo cual, si z es raíz de $f(x)$, por a) \bar{z} es raíz de $\bar{f}(x) = f(x)$.

□

10. Sea A un anillo comutativo con identidad, y sea $D : A[x] \rightarrow A[x]$ dada por $D(f(x)) = a_1 + 2a_2 x + 3a_3 x^2 + \dots + na_n x^{n-1}$ para cada $f(x) = a_0 + a_1 x + \dots + a_n x^n \in A[x]$. Regularmente, se usa $f'(x)$ para denotar a $D(f(x))$, y es llamada la **derivada** de $f(x)$. Pruebe que se cumplen las siguientes relaciones para $f(x), g(x) \in A[x]$ y para cada $a \in A$:

- a) $(f(x) + g(x))' = f'(x) + g'(x)$.
- b) $(af(x))' = af'(x)$.
- c) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Dem:

D_e a): Si $f(x) = a_0 + \dots + a_n x^n$ y $g(x) = b_0 + \dots + b_m x^m$, sea $s = \max\{n, m\}$ y definir (en caso de no estarlo) $a_i = 0, b_i = 0, \forall i \in [0, s]$. Entonces:

$$\begin{aligned} (f(x) + g(x))' &= (a_0 + b_0 + (a_1 + b_1)x + \dots + (a_s + b_s)x^s)' \\ &= (a_1 + b_1) + 2(a_2 + b_2)x + \dots + s(a_s + b_s)x^{s-1} \\ &= (a_1 + 2a_2 x + \dots + sa_s x^{s-1}) + (b_1 + \dots + sb_s x^{s-1}) \\ &= f'(x) + g'(x) \end{aligned}$$

D_e b): Se tiene que:

$$\begin{aligned} (af(x))' &= (a(a_0 + \dots + a_n x^n))' \\ &= (aa_0 + aa_1 x + \dots + aa_n x^n)' \\ &= aa_1 + 2aa_2 x + \dots + naa_n x^{n-1} \\ &= a(a_1 + 2a_2 x + \dots + na_n x^{n-1}) \\ &= a(f(x))' \end{aligned}$$

D_e c): Se probará primero cuando el $g(x)$ es moníaco. Si $g(x)$ el resultado es inmediato de

b), pues $(g(x))' = 0$, así $(g(x)f(x))' = g(x)(f(x))' + (g(x))'f(x) = 0(f(x))' \quad (g(x)=0)$.

Si $g(x) = b_m x^m \quad (m \in \mathbb{N})$, entonces:

$$\begin{aligned}
 (g(x)f(x))' &= (b_m x^m \cdot (a_0 + \dots + a_n x^n))' \\
 &= b_m (a_0 x^m + \dots + a_n x^{n+m})' \\
 &= b_m (m a_0 x^{m-1} + \dots + a_n (n+m) x^{n+m-1}) \\
 &= b_m (m+0) a_0 x^{m-1} + b_m (m+1) a_1 x^m + \dots + b_m (m+n) a_n x^{m+n-1} \\
 &= m b_m x^{m-1} (a_0 + a_1 x + \dots + a_n x^n) + b_m x^m (0 a_0 + 1 a_1 + \dots + n a_n x^{n-1}) \\
 &= (g(x))' f(x) + g(x)(f(x))' \\
 &= g(x)(f(x))' + (g(x))' f(x)
 \end{aligned}$$

Si $g(x) = b_0 + \dots + b_m x^m$:

$$\begin{aligned}
 (f(x)g(x))' &= (f(x)b_0 + \dots + f(x)b_m x^m)' \\
 &= (f(x)b_0)' + \dots + (f(x)b_m x^m)' \\
 &= f(x) \cdot 0 + b_0 (f(x))' + \dots + f(x) m b_m x^{m-1} + b_m x^m (f(x))' \\
 &= f(x) (b_0 + \dots + m b_m x^{m-1}) + (b_0 + b_1 x + \dots + b_m x^m) (f(x))' \\
 &= f(x) (g(x))' + (f(x))' g(x)
 \end{aligned}$$

□

11. Sea A un anillo commutativo con identidad, y sea $a \in A$ raíz de un polinomio no cero $f(x) \in A[x]$. Decimos que a es **raíz múltiple** de $f(x)$ si $f(x) = (x-a)^n g(x)$ con $n > 1$ y $g(x) \in A[x]$ tal que $g(a) \neq 0$. Pruebe que a es raíz múltiple de $f(x)$ si, y solo si a es raíz común de los polinomios $f(x)$ y $f'(x)$.

Dem:

⇒) Si a es raíz múltiple de $f(x)$, entonces $\exists n \in \mathbb{N}, n > 1$ en $f(x) = (x-a)^n g(x)$, con $g(x) \in A[x]$ y $g(a) \neq 0$.

0. Por el ejercicio ant.

$$\begin{aligned}
 (f(x))' &= ((x-a)^n g(x))' \\
 &= (x-a)^n (g(x))' + ((x-a)^n)' g(x)
 \end{aligned}$$

donde $((x-a)^n)' = \sum_{k=1}^n (x-a)^k (x-a)^{n-k} = n(x-a)^{n-1}$ (se prueba por inducción). Por tanto:

$$\begin{aligned}
 &= (x-a)^n (g(x))' + n(x-a)^{n-1} g(x) \\
 &= (x-a)^{n-1} ((x-a)(g(x))' + ng(x))
 \end{aligned}$$

donde $n-1 > 0$. Luego $f'(a)=0 \Rightarrow a$ es raíz de $f'(x)$.

\Leftarrow) Supongamos que a es raíz de $f(x)$ y $(f(x))'$, ent. $x-a | f(x), (f(x))'$. Por tanto $\exists q_1(x), q_2(x) \in A[x]$

ta:

$$f(x) = (x-a)q_1(x) \quad y \quad (f(x))' = (x-a)q_2(x)$$

Luego $(f(x))' = q_1(x) + (x-a)(q_1(x))'$, por tanto:

$$\Rightarrow q_1(x) = (x-a)(q_2(x) - (q_1(x))')$$

así, a es raíz de $q_1(x)$. Luego $\exists q_3(x) \in A[x]$ m $q_1(x) = (x-a)q_3(x)$. Así:

$$f(x) = (x-a)^2 q_3(x)$$

Como $\text{grad}(q_3(x)) < \infty$, $(x-a) \nmid q_3(x)$ ó $\exists m_0 \in \mathbb{N}$ m $(x-a)^{m_0} | q_3(x)$. Para el primer caso, tome $n=2$ y al segundo, $n=2+m_0$. Así $\exists q(x) \in A[x]$ m

$$f(x) = (x-a)^n q(x)$$

donde $q(a) \neq 0$ y $n > 1$.

□

12. Sea K un campo y $f(x)$ un polinomio en $K[x]$ de grado 2 o 3. Pruebe que $f(x)$ es un polinomio irreducible en $K[x]$ si, y solo si $f(x)$ no tiene raíces en K . De un ejemplo en el cual demuestre que esta afirmación no es cierta si el grado del polinomio es ≥ 4 .

Supongamos que $\text{grad}(f(x)) = 3$.

\Rightarrow) Supongamos $f(x)$ un polinomio irreducible. Si $f(x)$ tuviera raíces en K , tendría al menos una, digamos $a \in K$, luego $\exists q(x) \in K[x]$ m

$$f(x) = (x-a)q(x)$$

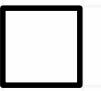
Con $(x-a) \in K[x]$ m $\text{grad}(x-a) \geq 1$ y $\text{grad}(q(x)) \geq 1$ $\forall x \in K$, pues $f(x)$ es pol. irreducible, luego no tiene raíces en K .

\Leftarrow) Supongamos que $f(x)$ no tiene raíces en K . Si $h(x), g(x) \in K[x]$ son tales que:

$$f(x) = h(x)g(x)$$

ent. como $f(x)$ no tiene raíces en K , no puede suceder que el grado de alguno de los pols. sea 1 o 2,
luego $h(x) \in K$ o $g(x) \in K$, i.e $f(x)$ es pol. irreducible.

Cuando $\text{grad}(f(x)) = 2$, la prueba es análoga al ant.



13. Sea K un campo de característica cero, y sea $f(x) \in K[x]$ un polinomio irreducible.

Pruebe que todas las raíces de $f(x)$ en cualquier campo que contenga a K son distintas. (Sugerencia: Pruebe que el máximo común divisor de $f(x)$ y $f'(x)$ es 1).

Dem:

Sea F una extensión de campo de K , i.e $K \subseteq F$. Probaremos que $\text{mcd}\{f(x), f'(x)\} = 1$ en el campo F .

Si $\exists g(x) \in F$ s.t. $\text{grad}(g(x)) \geq 1$, y $g(x) = \text{mcd}\{f(x), f'(x)\}$, entonces $g(x) | f(x)$ y $g(x) | f'(x)$

14. Pruebe que todo polinomio $f(x) \in \mathbb{C}[x]$, se factoriza como un producto de polinomios lineales y/o cuadráticos con coeficientes reales.

Dem:

No es correcto, tome $f(x) = x+i$, es pol. irreducible con un coef. imaginario. Es cierto cuando Se cambia a \mathbb{C} por \mathbb{R} .

Basta probar el caso cuando $f(x)$ es de grado par, pues si $f(x)$ es de grado impar, $f(x)$ tiene una raíz $r \in \mathbb{R}$, i.e:

$$f(x) = (x-r) g(x)$$

Con $\text{grad}(g(x))$ un número par. Suponga que $\text{grad}(f(x)) = 2m+2$, $m \in \mathbb{N}$ (si $\text{grad}(f(x)) = 2$, el resultado se tiene)

15. Sea A un dominio entero y $f(x) \in A[x]$ un polinomio de grado positivo. Pruebe lo siguiente:

- a) Si $\text{car}(A) = 0$, entonces $f'(x) \neq 0$.
- b) Si $\text{car}(A) = p \neq 0$, entonces $f'(x) = 0$ si, y solo si existe $g(x) \in A[x]$ tal que $f(x) = g(x^p)$; es decir,

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{np} x^{np}.$$

Dem:

De a): Supongamos $f(x) = a_0 + a_1 x + \dots + a_n x^n$ (con $n \geq 1$), ent.

$$f'(x) = a_1 + 2a_2 x + \dots + n a_n x^{n-1}$$

Como A es dominio entero, entonces $a b = 0 \Leftrightarrow a = 0 \circ b = 0$, como $n a_n = (n \cdot 1) \cdot a_n$, y $a_n \neq 0$ y $(n \cdot 1) \neq 0$ (pues A es de característica 0) entonces $n a_n \neq 0$, luego $f'(x) \neq 0$.

De b):

\Leftarrow) Supongamos $\exists g(x) \in A[x]$ m $f(x) = g(x^p)$, i.e:

$$\begin{aligned} f(x) &= a_0 + a_p x^p + a_{2p} x^{2p} + \dots + a_{np} x^{np} \\ \Rightarrow f'(x) &= p a_p x^{p-1} + 2p a_{2p} x^{2p-1} + \dots + np a_{np} x^{np-1} \\ &= 0 + \dots + 0 \\ &= 0 \end{aligned}$$

\Rightarrow) Supongamos $f'(x) = 0$, ent. si $f(x) = a_0 + a_1 x + \dots + a_n x^n$:

$$\Rightarrow f'(x) = a_1 + 2a_2 x + \dots + n a_n x^{n-1}$$

$\Rightarrow \sum a_i = 0, \forall i \in [1, n]$. Afirmando que si $p \nmid i$, ent. $a_i = 0$, en efecto, $\exists! q, r \in \mathbb{Z}$ m $i = pq + r$, $0 < r < p$, asr:

$$\begin{aligned} \sum a_i &= (pq+r)a_i \\ &= p(qa_i) + ra_i \\ &= ra_i = 0 \end{aligned}$$

Como p es primo y $\{a_i, 2a_i, \dots, ra_i\}$ es subgrupo de $(A, +)$, ent si j es el máximo elemento m $j a_i \neq 0 \Rightarrow j \mid p \Rightarrow j = 1 \circ j = p$, con $j \leq r$, luego $j = 1$, asr $a_i = 0$.

$$\text{Luego } f(x) = a_0 + a_{1p} x^p + \dots + a_{mp} x^{mp}. \text{ Tome } g(x) = a_0 + a_{1p} x + \dots + a_{mp} x^m \in A(x)$$

$$\Rightarrow f(x) = g(x^p)$$

□

16. Sea A un anillo commutativo con identidad, y sea I un ideal propio de A . Pruebe lo siguiente:

- Si $\varphi : A[x] \rightarrow (A/I)[x]$ es el homomorfismo reducción módulo I , entonces $\ker(\varphi) = I[x]$. Deducza que $A[x]/I[x] \cong (A/I)[x]$;
- Si $f(x) \in A[x]$ con $\varphi(f(x))$ polinomio irreducible en $(A/I)[x]$, entonces $f(x)$ es polinomio irreducible en $A[x]$;
- $f(x) = x^3 - x^2 + 1$ es polinomio irreducible en $\mathbb{Z}[x]$. (Sugerencia: Reducir coeficientes módulo 2).

Dem:

De a): Si $f(x) \in \ker(\varphi)$

$$\varphi(f(x)) = 0$$

donde $\varphi(f(x)) = a_0 + I + (a_1 + I)x + \dots + (a_n + I)x^n$, si $f(x) = a_0 + \dots + a_n x^n$. Luego:

$$f(x) \in \ker(\varphi) \Leftrightarrow I + a_i = 0, \forall i \in [0, n]$$

$$\Leftrightarrow a_i \in I, \forall i \in [0, n]$$

$$\Leftrightarrow f(x) \in I[x]$$

$\therefore \ker(\varphi) = I[x]$. Como φ es suproyectivo, por el P.T. I: $A[x]/I[x] \cong (A/I)[x]$.

De b): Supongamos que $f(x)$ no es pol. irreducible en $A[x]$, ent. $\exists g(x), h(x) \in A[x]$ m

$$f(x) = g(x)h(x)$$

Con $\text{grad}(g(x)), \text{grad}(h(x)) \geq 1$. Entonces:

$$\Rightarrow \varphi(f(x)) = \varphi(g(x))\varphi(h(x))$$

$$F(x) = G(x)H(x)$$

Como $F(x) \in (A/I)[x]$ es pol. irreducible, debe suceder que $G(x) \in A/I$ o $H(x) \in A/I$ (pues, $\text{grad}(F(x)) \geq 1$).

ent.

$$f(x) = (g(x) + i_1(x)) \cdot (h(x) + i_2(x)).$$

Con $i_1, i_2(x)$ conten. en \mathbb{I} . Por ser f no irreducible, $\text{grad}(g(x) + i_1(x)) = 0$.

on el otro. Supongu $\text{grad}(g(x) + i_1(x)) = 0$

$$\begin{aligned} \text{grad}(G(x)) &= \text{grad}(Q(g(x)) + Q(i_1(x))) \\ &= \text{grad}(Q(g(x) + i_1(x))) \leq 0. \end{aligned}$$

Son \mathbb{I}

$$Q(f(x)) = G(x)H(x)$$

donde

$$G(x) = b_0 + I + (b_1 + I)x + \dots + (b_m + I)x^m \quad \text{grad}(Q(f(x))) \geq 1, \text{ e } j_0 \in [0, n]$$

$$H(x) = c_0 + I + \dots + (c_1 + I)x + \dots + (c_n + I)x^n \quad \text{es el m\'aximo para el cual, } a_i \notin \mathbb{I}.$$

Podemos suponer que $f(x) = a_0 + \dots + a_n x^n$ en $\mathbb{I} \neq \mathbb{I}$.

Si $f(x) \in \mathbb{I}$, $a_i \in [0, n]$

$\Rightarrow Q(f(x)) = 0$, claro que si $f(x)$ no lo es, tampoco $Q(f(x))$ lo es.

Si $\exists i \in [0, n]$ en $a_i \notin \mathbb{I} \Rightarrow$

$\text{grad}(Q(f(x))) \geq i$. Supongamos que

$\text{grad}(Q(f(x))) \geq 1$, e $j_0 \in [0, n]$

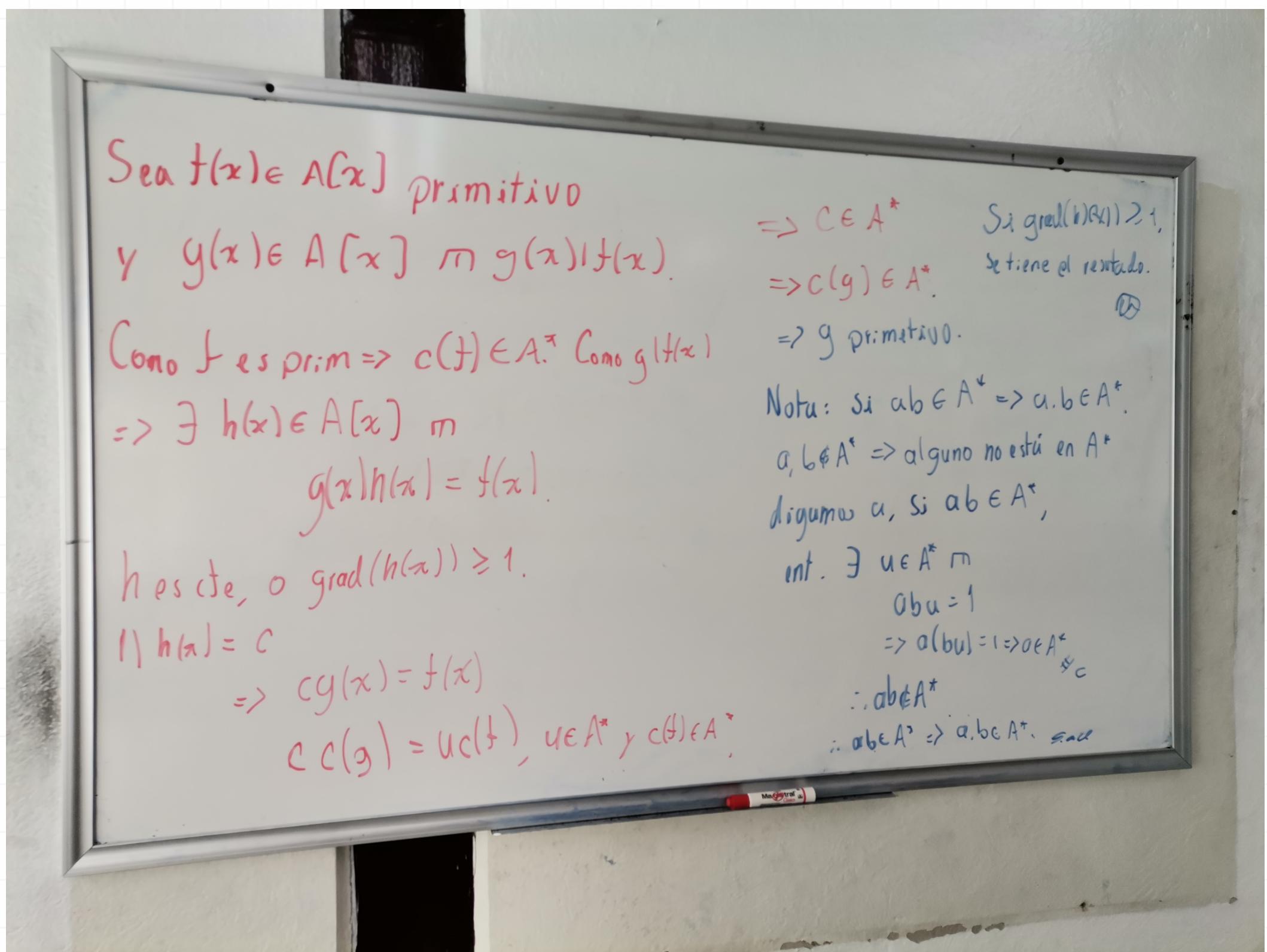
i.e. $Q(f(x)) = A + a_0 + \dots + (A + a_{j_0})x^{j_0}$

17. Sean A un DFU, $a \in A$ y $f(x) \in A[x]$. Pruebe que $c(af) = ac(f)$ salvo asociados.

18. Sean A un DFU. Dado b una división de a entre los constantes de un polinomio unitario.

18. Sea A un DFU. Pruebe que cualquier divisor no constante de un polinomio primitivo

en $A[x]$ es también un polinomio primitivo.



19. Sea A un anillo comutativo con identidad, y sea $f(x) = a_0 + a_1x + \dots + a_nx^n \in A[x]$.

Pruebe que $f(x)$ es una unidad en $A[x]$ si, y solo si a_0 es una unidad de A y a_1, \dots, a_n son elementos nilpotentes de A .

Dem:

\Rightarrow) Procedemos por inducción sobre n . Supongamos que $n=1$, i.e. $f(x) = a_0 + a_1x$. Como $f(x)$ es unidad,

$$\exists g(x) = b_0 + b_1x + \dots + b_mx^m \text{ s.t.}$$

$$f(x)g(x) = 1$$

$$= a_0g(x) + a_1xg(x)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1)x^2 + (a_0b_3 + a_1b_2)x^3 + \dots + (a_0b_m + a_1b_{m-1})x^m + a_1b_m x^{m+1}$$

Ent. $a_0b_0 = 1 \Rightarrow a_0 \in A^* \Rightarrow b_0 = a_0^{-1}$, luego como

$$a_0b_k + a_1b_{k-1} = 0, \forall k \in [1, m]$$

$$\Rightarrow a_0b_1 + a_1b_0 = 0 \Rightarrow b_1 = -a_1a_0^{-2}, \quad a_0b_2 + a_1b_1 \Rightarrow b_2 = -a_0^{-1}a_1(-a_1a_0^{-2}) = a_1^2a_0^{-3},$$

en general:

$$b_k = (-1)^k a_1^k a_0^{-(k+1)}, \forall k \in [1, m]$$

$$y a_1b_m = 0 \Rightarrow a_1^{k+1} \cdot (a_0^{-(k+1)}) (-1)^k = 0 \Rightarrow a_1^{k+1} \cdot a_0^{-(k+1)} (-1)^k = 0 \Rightarrow a_1^{k+1} = 0 \Rightarrow a_1 \text{ es nilpotente.}$$

Supongamos que se cumple para $n=k$, probaremos que se cumple para $n=k+1$. Si $f(x) = a_0 + \dots + a_{k+1}x^{k+1}$

es invertible, ent. $\exists g(x) \in A[x]$ pol. no cero s.t.

$$f(x)g(x) = 1$$

Si $g(x) = b_0 + \dots + b_mx^m$, ent.

$$c_0 + \dots + c_u x^u = 1$$

donde $C_l = \sum_{i=0}^l a_i b_{l-i}$, en part.

$$c_l = 0, \forall l \in [1, u]$$

Con $c_0 = a_0b_0 = 1 \Rightarrow a_0 \in A^*$. Si $k \leq l$

20. Sean p un número primo, K un campo y $a \in K$. Pruebe que $x^p - a$ es polinomio irreducible en $K[x]$ si, y solo si $x^p - a$ no tiene raíces en K . (Sugerencia: Considere dos casos: $\text{car}(K) = 0$ y $\text{car}(K) = p > 0$).

21. Aplique el criterio de Eisenstein para probar que los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$:

- a) $f(x) = x^2 + 1$.
- b) $g(x) = x^2 - x + 1$.
- c) $h(x) = 2x^5 - 6x^3 + 9x^2 - 15$.

(Sugerencia: Considere $f(x+1)$ y $g(-x)$)

22. (**Criterio de Eisenstein**) Sea A un DFU con campo de cocientes K . Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ con $\deg(f) \geq 1$, y sea p un elemento irreducible de A tal que $p \nmid a_n$, $p \mid a_i$ para cada $i = 0, 1, \dots, n-1$, y $p^2 \nmid a_0$. Pruebe que $f(x)$ es un polinomio irreducible en $K[x]$. Además, pruebe que si $f(x)$ es polinomio primitivo, entonces $f(x)$ es polinomio irreducible en $A[x]$.

23. Sea A un DFU, y sea K su campo de cocientes. Sea a/b un elemento de K , con a y b primos relativos, tal que es raíz del polinomio $f(x) = a_0 + a_1x + \dots + a_nx^n \in A[x]$. Pruebe que $a | a_0$ y $b | a_n$.

A DFU, $K = \text{coc}(A)$ $\frac{a}{b} \in K$

m es raíz de $a_0 + \dots + a_nx^n = f(x) \in A[x]$. $\Rightarrow b^n a_0 + \sum_{k=1}^{n-1} b^{n-k} a^k a_k + a^n a_n = 0$

P. 1) $a | a_0$ y $b | a_n$.

Como es raíz:

$$\Rightarrow a_0 + \frac{a_1 a}{b} + \dots + \frac{a_n a^n}{b^n} = 0$$

$$\Rightarrow \frac{b^n a_0 + b^{n-1} a a_1 + \dots + a^n a_n}{b^n} = 0$$

$$\Rightarrow \sum_{k=0}^n b^{n-k} a^k a_k = 0$$

$$\Rightarrow b^n a_0 + \sum_{k=1}^{n-1} b^{n-k} a^k a_k + a^n a_n = 0$$

$$\Rightarrow b(b^{n-1} a_0 + a^n) = a^n a_n$$

$$\Rightarrow b | a^n \circ b | a_n$$

pero $(a, b) = 1 \Rightarrow (a^n, b) = 1 \Rightarrow b | a_n$

de formaanáloga, $a | a_0$

24. Pruebe lo siguiente:

- a) El polinomio $f(x) = 1 + x$ es unidad en $\mathbb{Z}[[x]]$, pero no es unidad en $\mathbb{Z}[x]$.
- b) El polinomio $f(x) = 2 + 3x + x^2$ es elemento irreducible en $\mathbb{Z}[[x]]$, pero en $\mathbb{Z}[x]$.

Notas: