

ANILLO DE POLINOMIOS.

SERIES DE POTENCIAS.

Sea A un anillo. Denotemos por:

$$S_A = \{ f \mid f: \mathbb{N} \cup \{0\} \rightarrow A \}$$

es decir S_A es el conjunto de sucesiones de A . Si $f \in S_A$, escribimos a f de la siguiente forma:

$$f = (a_0, a_1, \dots)$$

Sobre S_A se definen dos operaciones, la suma y producto, a saber: si $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots) \in S_A$, entonces:

$$f + g = (a_0 + b_0, a_1 + b_1, \dots)$$

$$\& fg = (c_0, c_1, \dots)$$

Donde:

$$\begin{aligned} c_k &= \sum_{i=0}^k a_i b_{k-i} \\ &= a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 \\ &= \sum_{i=0}^k a_{k-i} b_i \\ &= \sum_{i+j=k} a_i b_j. \end{aligned}$$

Tenemos que S_A es anillo, con cero $(0, 0, \dots)$, $-f = (-a_0, -a_1, \dots)$. También existe un monomorfismo de A en S_A , a saber:

$$A \hookrightarrow S_A, a \mapsto (a, 0, 0, \dots)$$

Luego, podemos decir que $\forall a \in A, a = (a, 0, 0, \dots)$. Sea x un objeto tal que $x \notin A$. x es llamado **indeterminada para A** . Definimos $\forall n \in \mathbb{N} \cup \{0\}$ y $\forall a \in A$

$$ax^n := \underbrace{(0, 0, \dots, 0)}_{n+1-\text{ésima entrada}}, a, 0, \dots$$

Si A tiene identidad, entonces:

$$1x^n = \underbrace{(0, \dots, 0)}_{n+1-\text{entrada}}, 1, 0, \dots)$$

$1x = x$, y $1x^0 = 1$, y $1x^n = x^n$ (haciendo abuso de notación). Luego:

$$x^n \in S_A, \forall n \in \mathbb{N} \cup \{0\}$$

Independientemente de si A tiene identidad o no, se tiene que:

$$\begin{aligned} (a_0, a_1, a_2, \dots) &= (a_0, 0, 0, \dots) \\ &\quad + (0, a_1, 0, \dots) \\ &\quad + (0, 0, a_2, \dots) \\ &\quad + \dots \\ &= a_0 x^0 + a_1 x + a_2 x^2 + \dots \end{aligned}$$

Por lo tanto, si $f = (a_0, a_1, a_2, \dots)$:

$$\begin{aligned} f &= \sum_{i=0}^{\infty} a_i x^i \\ &= a_0 + a_1 x + a_2 x^2 + \dots \end{aligned}$$

Así pues, podemos decir que una serie es una expresión algebraica de la forma:

$$f = \sum_{i=0}^{\infty} a_i x^i = a_0 x^0 + a_1 x + a_2 x^2 + \dots$$

donde $a_0 x^0 := a_0$. Además, éstas se pueden sumar y multiplicar: si $f = \sum_{n=0}^{\infty} a_n x^n$, y $g = \sum_{n=0}^{\infty} b_n x^n$, entonces:

$$\begin{aligned} f + g &= \sum_{n=0}^{\infty} (a_n + b_n) x^n \quad \& \\ fg &= \sum_{n=0}^{\infty} c_n x^n \end{aligned}$$

donde $c_n = \sum_{i=0}^n a_i b_{n-i}, \forall n \in \mathbb{N} \cup \{0\}$. Es decir:

$$\begin{aligned} fg &= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_2 b_0 + a_0 b_2 + a_1 b_1) x^2 + \dots \\ &\quad + (a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0) x^n + \dots \end{aligned}$$

Con estas operaciones, S_A es un anillo. Pero cuando S_A es anillo, se cambia la notación por:

$A[[x]]$, y se dice que $A[[x]]$ es el anillo de series de potencias con coeficientes en A en la indeterminada x .

Si $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, los elementos $a_0, a_1, \dots, \in A$ son llamados **coeficientes** ó **términos** de la serie f . En part. a_0 es llamado **coeficiente cte.** de la serie f . El cero de $A[[x]]$ es la **serie cero** dada por:

$$0 = \sum_{n=0}^{\infty} a_n x^n, \quad a_n = 0 \quad \forall n \in \mathbb{N} \cup \{0\}. \text{ i.e}$$

$$0 = \sum_{n=0}^{\infty} 0 x^n$$

Además $f = 0 \Leftrightarrow a_n = 0, \forall n \in \mathbb{N} \cup \{0\}$. Recordar que cuando una serie $f \neq 0$ tenga coef. cero, es. tos no se expresan dentro de f , i.e., podemos tener la serie $f = a_0 + a_2 x^2 + a_4 x^4 + \dots$

Si A tiene identidad, $A[[x]]$ también lo tiene y es la identidad de A , i.e

$$1 = 1 + 0x + 0x^2 + \dots$$

y en este caso, se tiene que $(x^n := x^n, \forall n \in \mathbb{N})$. Y

$$(x^n = (1, 0, \dots,) \underbrace{(0, \dots, 0)}_{n+1-\text{ésima entrada}}, 1, 0, \dots))$$

lo cual motiva a considerar que:

$$x^n := (\underbrace{0, \dots, 0}_{n+1-\text{ésima entrada}}, 1, 0, \dots)$$

lo cual implicaría que $x \in A[[x]]$. Luego $x^n \in A[[x]], \forall n \in \mathbb{N}$. Además:

$$x^n \cdot x^m = x^{n+m}, \quad \forall n, m \in \mathbb{N}.$$

Si A es un anillo commutativo, $A[[x]]$ también lo es. Si A es un dominio entero, entonces $A[[x]]$ también lo será (como se verá más adelante).

Def. Sea A un anillo. Para cada serie $f = \sum_{n=0}^{\infty} a_n x^n \neq 0$ en $A[[x]]$, se define el **orden** de f , denotado por $\circ(f)$, como aquel entero mínimo no negativo m s.t. $a_{\circ(f)} \neq 0$. Así,

Si f es una serie de potencias no cero, entonces:

$$f = \sum_{n=0}^{\infty} a_n x^n$$

EJERCICIO.

1) Si $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, $\exists g \in A[[x]]$, $g = \sum_{n=0}^{\infty} b_n x^n$ en $\circ(g) = 0$ y $f = x^{\circ(f)} g$. (A con identidad).

Dem:

Tenemos que:

$$f = \sum_{n=0}^{\infty} a_n x^n$$

Definimos $g = \sum_{n=0}^{\infty} b_n x^n$, donde $b_n = a_{\circ(f)+n}$. $g \in A[[x]]$ (pues $b_n \in A, \forall n \in \mathbb{N}$).

Probaremos ahora que:

$$f = x^{\circ(f)} \cdot g$$

En efecto, llamemos $\sum_{n=0}^{\infty} c_n x^n = x^{\circ(f)} \cdot g$. Por def. se tiene que:

$$c_k = \sum_{n+m=k} \delta_{\circ(f)+n} b_m$$

Donde $\delta_{\circ(f)}(n) = \delta_{\circ(f),n}$ es la delta Kronecker de A . Si $k < \circ(f)$, entonces $c_k = 0$. Si $\circ(f) \leq k$, entonces:

$$c_k = 1 \cdot b_{k-\circ(f)}$$

Pero $b_{k-\circ(f)} = a_{\circ(f)+k-\circ(f)} = a_k$. Por tanto:

$$\begin{aligned} c_k &= a_k, \quad \forall k \geq \circ(f) \\ \Rightarrow \sum_{n=0}^{\infty} c_n x^n &= \sum_{n=0}^{\infty} a_n x^n \\ &= f \end{aligned}$$

□

Proposición.

Sean $f = \sum_{n=0}^{\infty} a_n x^n$ & $g = \sum_{n=0}^{\infty} b_n x^n$ dos series de potencias no cero. Entonces:

i) $f+g = 0$ si $\circ(f+g) > \min\{\circ(f), \circ(g)\}$.

ii) $f_g = 0$ ó $\circ(f_g) \geq \circ(f) + \circ(g)$.

Dem: Ejercicio. ²⁾

Corolario.

En las cond. de la prop. anterior, si A es dominio entero, entonces $\circ(f_g) = \circ(f) + \circ(g)$. en particular $f_g \neq 0$ y $A[[x]]$ es dominio entero.

Dem: Ejercicio. ³⁾

Proposición.

Sea A un anillo conmutativo con identidad y sea $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$ una serie de pot. no cero. Entonces f es unidad Ssi a_0 (el término constante) es unidad de A .

Dem:

Suponemos que f es unidad de $A[[x]]$. Sea $g \in A[[x]]$, $g = \sum_{n=0}^{\infty} b_n x^n$, tal que $f_g = 1$ (i.e., $g = f^{-1}$). Luego, $a_0 b_0 = 1$, con $b_0 \in A$. Por tanto, $a_0 \in A^*$.

Recíprocamente. Supongamos que $a_0 \in A^* \Rightarrow \exists b_0 \in A$ m $a_0 b_0 = 1$ (en part, $b_0 \neq 0$ y $a_0 = b_0^{-1} \in A$).

Definimos $b_i := -a_0 b_0^2$. Supóngase construidos b_0, \dots, b_{n-1} m $a_0 b_0 = 1$, y

$$c_i = 0 = \sum_{k=0}^{i-1} a_k b_{i-k}, \quad \forall i \in [0, n-1]$$

tomamos

$$\begin{aligned} b_n &:= -b_0 (a_0 b_0 + \dots + a_1 b_{n-1}) \\ &= -b_0 \left(\sum_{k=0}^{n-1} a_{n-k} b_k \right) \in A \end{aligned}$$

entonces:

$$a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0 = 0 = c_n$$

Aplicando inducción, hemos construido una sucesión formada por $\{b_n\}_{n=0}^{\infty}$ m $a_0 b_0 = 1$, y:

$$\sum_{k=0}^m a_k b_{m-k} = 0, \quad \forall m \in \mathbb{N}$$

Si $g = \sum_{n=0}^{\infty} b_n x^n$ entonces $f_g = 1 - g \in A[[x]]$. Por tanto, $f \in A[[x]]^*$.

□

Corolario.

Si K es campo, entonces $f = \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \setminus \{0\}$ es unidad $\Leftrightarrow a_0 \neq 0$.

Dem: es inmediata.

Corolario.

Si K es campo & $f = \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \setminus \{0\}$, entonces $\exists!$ serie de pot. $g \in K[[x]]$ invertible s.t. $f = x^{o(f)} g$.

Dem:

Por un ejercicio y el corolario ant. tenemos la existencia. Probaremos la unicidad. Sea $m \in \mathbb{N} \cup \{0\}$ & $g_1, g_2 \in K[[x]] \setminus \{0\}$ invertible s.t. $f = x^m g_1 = x^m g_2$.

Probaremos que $m = o(f)$ & $g_1 = g_2$. Como g_1 es invertible, se tiene

$$\begin{aligned} g_1 &= \sum_{n=0}^{\infty} b_n x^n \text{ donde } b_0 \neq 0 \\ \Rightarrow f &= x^m g_1 = x^m (b_0 + b_1 x + \dots) \\ &= b_0 x^m + b_1 x^{m+1} + \dots \end{aligned}$$

Por tanto, $m = o(f)$ y Como $x^{o(f)} g_1 = f$. Entonces:

$$x^{o(f)} (g_1 - g_2) = 0 \text{ donde } K[[x]] \text{ es dominio entero}$$

$$\therefore g_1 = g_2.$$

□

EJEMPLO.

1) Consideremos en $\mathbb{R}[[x]]$ la serie de potencias $f = 1 + x + x^2 + \dots = \sum_{n=0}^{\infty} x^n$. f es invertible y su inversa es $1-x \in \mathbb{R}[[x]]$. (Probar).

Proposición.

Si K es campo, el anillo $K[[x]]$ es DIP. Más aún, los ideales no triviales de $K[[x]]$

Son de la forma: $\langle x^k \rangle$, con $k \geq 1$.

Dem:

Sea I un ideal de $K[[x]]$ no trivial ($\neq K[[x]]$ y $\langle 0 \rangle$). Sea $f \in I \setminus \{0\}$, por el corolario anterior $\exists! g \in K[[x]]$ invertible y $\text{o}(f) = \text{o}(g)$ tal que $f = x^k g$.

Sea:

$$M = \{ k \in \mathbb{N} \cup \{0\} \mid f = x^k g \text{ con } f \in I, g \in K[[x]] \text{ invertible} \}$$

$M \neq \emptyset$ (pues $\text{o}(f) \in M$). Entonces $\exists k_0 \in M$ m $k_0 \leq k$, $\forall k \in M$. Así, $\exists f_k \in I$ m $\text{o}(f_k) = k_0$.

Así, $\exists g_k \in K[[x]]$ invertible m $f_k = x^{k_0} g_k$. Afirmamos que $I = \langle x^{k_0} \rangle$.

Como $f_k = x^{k_0} g_k \in I \Rightarrow x^{k_0} = f_k g_k^{-1} \in I$, luego $\langle x^{k_0} \rangle \subseteq I$. Recíprocamente, sea $h \in I \setminus \{0\}$.

Entonces $\text{o}(h) \geq k_0$, y $h = x^{\text{o}(h)} l$, con $l \in K[[x]]$ invertible. Luego:

$$\begin{aligned} h &= x^{k_0 + (\text{o}(h) - k_0)} l \\ &= x^k (x^{\text{o}(h) - k_0} l) \in \langle x^{k_0} \rangle, \text{ pues } x^{\text{o}(h) - k_0} l \in \end{aligned}$$

Así, $I \subseteq \langle x^{k_0} \rangle$.

□

Por lo tanto, tenemos que todos los ideales de $K[[x]]$ son:

$$\langle 0 \rangle \subsetneq \dots \subsetneq \langle x^{k+1} \rangle \subsetneq \langle x^k \rangle \subsetneq \dots \subsetneq \langle x \rangle \subsetneq K[[x]]$$

En part. tenemos que $K[[x]]$ es un anillo local con único ideal maximal $\langle x \rangle$. Así que

$$\langle x \rangle = K[[x]] \setminus K[[x]]^*$$

Además, se cumple lo siguiente:

$$K[[x]] / \langle x \rangle \cong K$$

En efecto, si $f \in K[[x]]$, denotamos por $f(0)$ al término constante de f , y la función $\varphi: K[[x]] \rightarrow K$, $f \mapsto f(0)$ es un homomorfismo de anillos, el cual es suprayectivo y $\langle x \rangle \subseteq \text{Ker}(\varphi)$, pues:

$$\begin{aligned}\text{Ker}(\varphi) &= \{ f \in K[[x]] \mid f(0) = 0 \} \\ &= \{ xf \mid f \in K[[x]] \} \\ &= \langle x \rangle\end{aligned}$$

Por tanto, por el P.T.I tenemos que $K((x)) / \langle x \rangle \cong K$.

Teorema.

Sea K un campo. Entonces, el dominio entero $K[[x]]$ es dominio euclíadiano.

Dem:

Puesto que $K[[x]]$, basta encontrar una función $\delta : K[[x]] \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ con las sig.

propiedades:

i) $\delta(f) \leq \delta(fg)$, $\forall f, g \in K[[x]] \setminus \{0\}$.

ii) $\forall f, g \in K[[x]]$ con $g \neq 0$, $\exists q, r \in K[[x]]$ s.t. $f = qg + r$ con $r = 0$ ó $\delta(r) < \delta(g)$.

Elegimos δ la función orden, i.e $\forall f \in K[[x]] \setminus \{0\}$, $\delta(f) := o(f)$. La condición (i) se cumple de forma inmediata (por un resultado anterior).

Probemos (ii). Sean $f, g \in K[[x]]$ con $g \neq 0$. Encontramos $q, r \in K[[x]]$ tales que $f = qg + r$ donde $r = 0$ ó $o(r) < o(g)$.

Si $f = 0$, tomemos $q, r = 0$.

Supongamos $f \neq 0$

a) Si $o(f) < o(g)$, tomemos $r = f$ y $q = 0$. Así $f = qg + r$ y $\delta(r) = o(r) = o(f) < o(g) = \delta(g)$ (pues $r \neq 0$).

b) Si $o(g) \leq o(f)$: Expresamos de manera única $f = x^{o(f)} f_1$ y $g = x^{o(g)} g_1$, donde $f_1, g_1 \in K[[x]]^*$. Definimos $q := x^{o(f)-o(g)} g_1^{-1} f_1 \in K[[x]]$ y $r = 0$. Entonces:

$$\begin{aligned}qg + r &= (x^{o(f)-o(g)}) g_1^{-1} f_1 x^{o(g)} g_1 + 0 \\ &= x^{o(f)} f_1 (g_1^{-1} g_1)\end{aligned}$$

$$= x^{\circ(f)} f_1 \\ = f$$

□

Obs) Así pues, tenemos que $K[[x]]$ es DE \Rightarrow DIP \Rightarrow DFU. Recordemos que en un DIP:

p es primo $\Leftrightarrow \langle p \rangle$ es maximal $\Leftrightarrow \langle p \rangle$ es primo

y ademáis, los elementos primos e irreducibles. Luego, como $K[[x]]$ es anillo local con único ideal maximal $\langle x \rangle$, entonces $p \in K[[x]]$ no cero y no unidad es irreducible (p primo, por ser DIP) si y sólo si $\langle p \rangle = \langle x \rangle$ si $p = fx$, con $f \in K[[x]]^*$ si $f(0) \in K \setminus \{0\}$.

Así, si $y \in K[[x]]$ no cero y no unidad, y se expresa de manera única como:

$$y = x^n f$$

(con $f \in K[[x]]^*$ y $n = \circ(y)$. (esta es la cond. de que $K[[x]]$ es DFU).

Teorema.

Sea A un anillo noetheriano. Entonces, el anillo de series de potencias $A[[x]]$ es noetheriano. (A comunitativo con 1).

Dem:

Sea \tilde{I} un ideal de $A[[x]]$ arbitrario no trivial. Probaremos que \tilde{I} es finitamente generado. Definimos para cada $n \geq 0$, el conjunto

$$I_n = \{acA \mid \exists f \in \tilde{I} \text{ s.t. } f = ax^n + \dots\}$$

$I_n \neq \emptyset$ pues $g = 0 \in \tilde{I}$. Afirmamos que $\forall n \geq 0$, I_n es ideal de A . En efecto: sea $a, b \in I_n$ y $r \in A$ arbitrarios.

Como $a, b \in I_n$, $\exists f, g \in A[[x]]$ tales que $f = ax^n + \dots$ y $g = bx^n + \dots$. Como \tilde{I} es ideal de $A[[x]]$, entonces $f - g = (a-b)x^n + \dots \in \tilde{I}$. Luego $a-b \in I_n$.

Además $rf \in \tilde{I}$, donde $rf = ra x^n + \dots$. Luego $ra \in I_n$.

Así, \bar{I}_n es ideal de A , $\forall n \geq 0$.

Además, $\forall n \geq 0$, $I_n \subseteq \bar{I}_{n+1}$, pues si $a \in I_n$:

$$\Rightarrow \exists f \in \tilde{I} \text{ s.t. } f = ax^n + \dots$$

$$\Rightarrow xf \in \tilde{I} \text{ s.t. } xf = ax^{n+1} + \dots$$

$$\Rightarrow a \in \bar{I}_{n+1}.$$

$$\therefore I_n \subseteq \bar{I}_{n+1}$$

Luego $\{\bar{I}_n\}_{n=0}^{\infty}$ es una cadena numerable ascendente de ideales de A . Como A es noetheriano, $\exists m \in \mathbb{N} \cup \{0\}$ mínimo tal que $\bar{I}_n = I_m, \forall n \geq m$. Es decir:

$$I_0 \subseteq I_1 \subseteq \dots \subseteq I_m = \bar{I}_{m+1} = \dots$$

De nuevo, como A es noetheriano, cada I_i con $0 \leq i \leq m$ son finitamente generados y los expresamos como:

$$I_i = \langle a_{i1}, a_{i2}, \dots, a_{ik_i} \rangle, k_i \in \mathbb{N}, \forall i \in [0, m].$$

y elegimos $f_{i1}, f_{i2}, \dots, f_{ik_i} \in \tilde{I}_i, \forall i \in [0, m]$ como:

$$f_{ij} = a_{ij}x^j + \dots$$

$\forall j = 1, \dots, k_i$ y $i = 0, \dots, m$. Afirmamos que:

$$\tilde{I} = \langle f_{ij} \mid j \in [1, k_i] \text{ y } i \in [0, m] \rangle = J$$

En efecto, es claro que $J \subseteq \tilde{I}$. Probemos la recíproca. Sea $f \in \tilde{I}$ con $f \neq 0$. Entonces:

$$f = ax^d + \dots, \text{ con } d = o(f).$$

$$\Rightarrow a \in I_d.$$

Suponemos que $0 \leq d < m$. Como $I_d = \langle a_{d1}, \dots, a_{dk_d} \rangle$, $\exists r_{d1}, \dots, r_{dk_d} \in A$ s.t.

$$a = r_{d1}a_{d1} + \dots + r_{dk_d}a_{dk_d}$$

$$\Rightarrow f - r_{d1}f_{d1} - \dots - r_{dk_d}f_{dk_d} = a, x^{d+1} + \dots \in \tilde{I} \dots (1)$$

Si (1) es cero en el lado derecho, entonces $f = r_{d1}f_{d1} + \dots + r_{dk_d}f_{dk_d}$, por lo cual $f \in \langle f_{ij} \mid \dots \rangle$. Si no, tendremos que la ecuación (1) tendrá a orden $d_1 \geq d+1$. Sea $b_j \in A$

el coef. de x^{l_1} en (1). Luego, supóngase que $0 \leq d < l_1 < m$, repetimos el procedimiento anterior $\Rightarrow b_1 \in I_{l_1} = \langle a_{l_1,1}, \dots, a_{l_1,K_{l_1}} \rangle$. Entonces $\exists r_{l_1,1}, \dots, r_{l_1,K_{l_1}} \in A$ tales que:

$$b_1 = r_{l_1,1} a_{l_1,1} + \dots + r_{l_1,K_{l_1}} a_{l_1,K_{l_1}}$$

Luego

$$f - r_{l_1,1} f_{l_1,1} - \dots - r_{l_1,K_{l_1}} f_{l_1,K_{l_1}} = a_2 x^{l_1+1} + \dots \in \tilde{I} \dots (2)$$

Si la derecha es cero, entonces $f \in \langle f_{i,j} | \dots \rangle$. En caso contrario, seguimos con el proceso y denotamos por l_2 el orden de la serie de la ec. (2), donde $l_2 \geq l_1 + 1$.

Sea b_2 el coef. de la pot. x^{l_2} en (2). Por tanto, $b_2 \in I_{l_2}$, i.e.

$$b_2 = r_{l_2,1} a_{l_2,1} + \dots + r_{l_2,K_{l_2}} a_{l_2,K_{l_2}}$$

Si $0 \leq d < l_1 < l_2 < m$, seguimos con el proceso. Supóngase que $l_2 \geq m$, y hacemos lo siguiente: consideramos el elemento de \tilde{I}

$$f - r_{l_1,1} f_{l_1,1} - \dots - r_{l_1,K_{l_1}} f_{l_1,K_{l_1}} - x^{l_2-m} (r_{m,1} f_{m,1} - \dots - r_{m,K_m} f_{m,K_m}) = a_3 x^{l_2+1} \in \tilde{I} \dots (3)$$

Donde

Sea K campo. Sabemos que $K[[x]]$ es un D.E, luego DIF y DFU. Además, $K[[x]]$ tiene un único elemento irreducible (salvo asociados) el cual es x .

Así que, cada serie f no cero y no unidad de $K[[x]]$ se expresa de manera única de la fo. fmu:

$$f = f_n x^n$$

donde $n =_0(f)$ & $f_n \in K[[x]]^*$. Por ser $K[[x]]$ dominio entero, denotamos por $K((x))$ al Campo de corrientes de $K[[x]]$, i.e:

$$\begin{aligned} K((x)) &= \text{coc}(K[[x]]). \\ &= K[[x]](K[[x]] \setminus \{0\})^\sim \\ &= \left\{ \frac{f}{g} \mid f, g \in K[[x]], g \neq 0 \right\} \end{aligned}$$

Sea $\alpha \in K((x))$, es decir $\alpha = \frac{f}{g}$ donde $f, g \in K[[x]]$, $g \neq 0$. Si $g \in K[[x]]^*$, entonces:

$$\alpha = \frac{f}{g} = fg^{-1} \in K[[x]]$$

Si $g \notin K[[x]]^*$, expresamos $g = g_m x^m$ con $g_m \in K[[x]]^*$ y $m =_0(g) \in \mathbb{N}$. Luego:

$$\alpha = \frac{f}{g} = \frac{f}{g_m x^m} = \frac{fg_m^{-1}}{x^m} \text{ donde } fg_m^{-1} \in K[[x]]$$

Supóngase que: $fg_m^{-1} = \sum_{n=0}^{\infty} c_n x^n = c_0 + c_1 x + c_2 x^2 + \dots$. Por tanto:

$$\alpha = \frac{fg_m^{-1}}{x^m} = \frac{\sum_{n=0}^{\infty} c_n x^n}{x^m} = \frac{c_0 + c_1 x + \dots}{x^m} \stackrel{(1)}{=} \frac{c_0}{x^m} + \frac{c_1}{x^{m-1}} + \dots + c_m + c_{m+1} x + c_{m+2} x^2 + \dots$$

Así, tendremos que:

$$K((x)) = \left\{ \sum_{n=-m}^{\infty} a_n x^n \mid a_n \in K \ \forall n \geq m, m \in \mathbb{N} \right\}$$

Los elementos de $K((x))$ son las llamadas series de Laurent.

Polinomios.

Def. Sea A un anillo. Se define el conjunto de polinomios en la indeterminada x con coeficientes en A como:

$$A[x] = \{ f \in A[[x]] \mid f = \sum_{m=0}^{\infty} a_m x^m \text{ & } \exists m_0 \in \mathbb{N} \cup \{0\} \text{ m } a_m = 0, \forall m > m_0 \}.$$

Así pues, tenemos que si $f \in A[x]$, entonces:

$$f = a_0 + a_1 x + \dots + a_n x^n.$$

Para distinguir a los elementos de $A[[x]]$ y $A[x]$, cada elemento lo denotamos por $f(x)$.

Si $f(x), g(x) \in A[x]$, entonces:

$$\begin{aligned} f(x) = g(x) \Leftrightarrow a_i = b_i, \forall i \text{ donde } f(x) = a_0 + a_1 x + \dots + a_n x^n, \text{ y} \\ g(x) = b_0 + b_1 x + \dots + b_m x^m \end{aligned}$$

Además, $A[x]$ es un subanillo de $A[[x]]$, donde el cero de $A[x]$ es llamado el **polinomio cero**.

Si $f(x) = a_0 + a_1 x + \dots + a_n x^n$, entonces $f(x) = -a_0 - a_1 x - \dots - a_n x^n$.

Obs) Si A es comunitativo, $A[x]$ también lo es.

Si A tiene 1, $A[x]$ también la tiene.

Si A es dominio entero, $A[x]$ también lo es.

Si $f(x) = a_0 + a_1 x + \dots + a_n x^n \neq 0$, siempre supondremos que $a_n \neq 0$ y este es llamado el **coeficiente líder o principal o dominante** y n es llamado el **grado de $f(x)$** denotado por:

$$\text{grad}(f) = \text{gr}(f) = \deg(f) = n.$$

Proposición.

Sea A un anillo y $f(x), g(x) \in A[x]$. Entonces,

- i) $f(x) + g(x) = 0$ ó $\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$.
- ii) $f(x)g(x) = 0$ ó $\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x))$.

Dem:

De (i): Supongamos que $f(x) + g(x) \neq 0$. Entonces $f(x) = a_0 + a_1 x + \dots + a_n x^n \neq 0$ & $g(x) = b_0 + b_1 x + \dots + b_m x^m \neq 0$. Entonces si $\ell = \max\{n, m\}$:

$$f(x) + g(x) = \sum_{k=0}^{\ell} (a_k + b_k) x^k \neq 0$$

Por tanto, $\text{grad}(f(x) + g(x)) \leq \ell = \max\{\text{grad}(f(x)), \text{grad}(g(x))\}$.

De (ii): Supondremos que $f(x)g(x) \neq 0$. Entonces:

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots + (a_n b_{m-1} + a_{n-1} b_m) x^{m+n-1} + \underbrace{a_n b_m}_{= C_{n+m}} x^{m+n}$$

Donde $C_{n+m} = \underbrace{a_0 b_{m+n} + a_1 b_{m+n-1} + \dots + a_{n-1} b_{m+1}}_{= 0} + \underbrace{a_n b_m}_{\text{posiblemente } \neq 0} + \underbrace{a_{n+1} b_{m-1} + \dots + a_{n+m} b_0}_{= 0}$

Luego $\text{grad}(f(x)g(x)) \leq n+m = \text{grad}(f(x)) + \text{grad}(g(x))$.

□

Corolario.

Si $f(x), g(x) \in A[x]$ y $g(x) \neq 0$ con coeficiente líder una unidad de A , entonces: $\text{grad}(f(x)g(x)) = \text{grad}(f(x)) + \text{grad}(g(x))$ si $f(x) \neq 0$.

Dem: es inmediato.

□

Corolario.

Si A es dominio entero, entonces $A[x]$ también lo es.

Dem: es inmediato.

□

Si A y B anillos con A subanillo (también se dice que B es una extensión de A). Y sea $r \in B$ arbitrario. Si $f(x) \in A[x]$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$, entonces el elemento

$$f(r) := a_0 + a_1 r + \dots + a_n r^n \in B$$

se le llama la **valuación** de $f(x)$ en r . Si $r \in \text{Cent}(B) = \{w \in B \mid bw = wb, \forall b \in B\}$ tiene

mos que la función $\phi_r: A[x] \rightarrow B$ dada por:

$$\phi_r(f(x)) = f(r), \quad \forall f(x) \in A[x].$$

es un homomorfismo entre $A[x]$ y B , i.e., se cumple lo siguiente:

$$\phi_r(f(x) + g(x)) = \phi_r(f(x)) + \phi_r(g(x)) \quad y \quad \phi_r(f(x)g(x)) = \phi_r(f(x))\phi_r(g(x))$$

O sea:

$$(f(x) + g(x))|_r = f(x)|_r + g(x)|_r \quad \& \quad (f(x)g(x))|_r = f(x)|_r \cdot g(x)|_r.$$

Luego imagen de ϕ_r es:

$$A[r] = \{a_0 + a_1 r + \dots + a_n r^n \mid a_i \in A, \forall i \in [0, n]; n \in \mathbb{N}\}.$$

y es un subanillo de B ; más aún, $A[r]$ es el mínimo subanillo de B que contiene a A y a r .

$$\Rightarrow \frac{A[x]}{\text{Ker}(\phi_r)} \cong A[r]$$

(pues ϕ_r es suprayectivo), donde $\text{Ker}(\phi_r) = \{g(x) \in A[x] \mid g(r) = 0\}$. Si $g(x) \in A[x]$ tal que $g(r) = 0$, entonces decimos que res raíz de $g(x)$.

Teorema (Algoritmo de la div.).

Sea A anillo conmutativo con 1, y sean $f(x), g(x) \in A[x]$ tales que $g(x) \neq 0$ con coeficiente

líder una unidad en A . Entonces existen únicos polinomios $q(x), r(x) \in A[x]$ m

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

donde $r(x) = 0 \Leftrightarrow \text{grad}(r(x)) < \text{grad}(g(x))$.

Def:

Si $f(x) = 0$, basta tomar $q(x) = r(x) = 0$. Por lo cual, suponemos $f(x) \neq 0$. Denotamos $m = \text{grad}(f(x))$ y $n = \text{grad}(g(x))$.

Si $m < n$, basta tomar $q(x) = 0$ y $r(x) = f(x)$. Así que, suponemos que $n \leq m$. Expresamos

a

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0.$$

6)

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0$$

Además, definimos el polinomio $f_1(x) := f(x) - a_m b_n^{-1} x^{m-n} g(x)$. Notemos que $f_1(x) = 0$ ó $\text{grad}(f_1(x)) = m < n$. Por hipótesis de inducción existen polinomios $r_1(x), q_1(x) \in A[x]$ tal que

$$f_1(x) = q_1(x) g(x) + r_1(x), \text{ i.e.}$$

$$f(x) = (a_m b_n^{-1} x^{m-n} + q_1(x)) g(x) + r_1(x)$$

donde $r_1(x) = 0$ ó $\text{grad}(r_1(x)) < \text{grad}(g(x))$. Tomemos así $q(x) = a_m b_n^{-1} x^{m-n} + q_1(x)$ y $r(x) = r_1(x)$. Lo cual demostraría la existencia.

Ahora con la unicidad. Supongamos que $r_1(x), q_1(x) \in A[x]$ tales que:

$$f(x) = q_1(x) g(x) + r_1(x).$$

Se tiene entonces la igualdad:

$$r(x) - r_1(x) = (q_1(x) - q(x)) \cdot g(x)$$

Teorema.

Sea K campo. Entonces, $K[x]$ es un DE. En consecuencia, $K[x]$ es DIP y DFU.

Dem:

Se sigue de manera inmediata del teorema anterior al considerar a δ como la función grado y aplicando el teorema anterior al dominio entero $K[x]$ sabiendo que todo polinomio de $K[x]$ no cero, su coeficiente líder es una unidad.

□

Teorema.

Sea A un dominio entero y $f(x) \in A[x]$ con $\text{grad}(f(x)) \geq 1$ (i.e $f(x) \neq 0$, $f(x)$ no es una constante). Entonces o bien $f(x)$ no tiene raíces en A ó en caso de tenerlas, a lo más tiene n -raíces distintas en A , con $n = \text{grad}(f(x))$.

Dem:

La demostración será por inducción sobre el grado de $f(x)$ (n). Suponemos que $n=1$, luego $f(x) = ax+b$, donde $a, b \in A$ con $a \neq 0$. Sean $c_1, c_2 \in A$ tales que

$$f(c_1) = f(c_2) = 0$$

$$\Rightarrow ac_1 + b = ac_2 + b = 0$$

$$\Rightarrow a(c_1 - c_2) = 0$$

Como A es dominio entero, $c_1 - c_2 = 0 \Rightarrow c_1 = c_2$. As: $f(x)$ sólo puede tener una raíz.

Supongamos el resultado cierto para cualquier polinomio de grado $< n$. Sea $c \in A$ raíz de $f(x)$, i.e $f(c) = 0$.

Por el algoritmo de la división, existen únicos polinomios $q(x), r(x) \in A[x]$ m

$$f(x) = (x-c)q(x) + r(x)$$

donde $r(x) = 0$ ó $\text{grad}(r(x)) < \text{grad}(x-c) = 1$. Por tanto $\text{grad}(r(x)) = 0 \Rightarrow r(x) = 0$, pero:

$$r(c) = 0$$

Por tanto $r(x) = 0$. Así:

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

donde $\text{grad}(q(x)) = n-1$, pues $A[x]$ es dominio entero. Por hipótesis de inducción, $q(x)$ tiene a lo más $n-1$ raíces distintas en A , donde cada una de ellas es raíz de $f(x)$. Luego entonces, $f(x)$ tiene a lo más n raíces distintas en A (contando multiplicidades). □

Teorema (del residuo).

Sea A un anillo comunitativo con 1, $f(x) \in A[x]$ y $c \in A$. Entonces existe un único polinomio $q(x) \in A[x]$ en

$$f(x) = (x - c)q(x) + f(c)$$

Dem:

Por el algoritmo de la div, $\exists! q(x), r(x) \in A[x]$ en

$$f(x) = (x - c)q(x) + r(x)$$

con $r(x) = 0$ ó $\text{grad}(r(x)) < 1$ (pues $x - c$ tiene coeficiente líder a 1), y:

$$f(c) = r(c)$$

Por tanto $f(x) = (x - c)q(x) + f(c)$. □

Corolario.

En las condiciones del teorema anterior, c es raíz de $f(x) \Leftrightarrow (x - c)$ divide a $f(x)$.

Dem:

Es inmediato. □

Corolario.

Sea A dominio entero y $f(x), g(x) \in A[x] \setminus \{0\}$. Si $a_1, \dots, a_n \in A$ son elementos distintos

entre si con $n > \max\{\text{grad}(f(x)), \text{grad}(g(x))\}$, tales que $f(a_i) = g(a_i)$, $\forall i \in [1, n]$, entonces, $f(x) = g(x)$.

Dem:

Si $f(x) - g(x) \neq 0$, entonces $\text{grad}(f(x) - g(x)) \leq \max\{\text{grad}(f(x)), \text{grad}(g(x))\} < m$, donde $f(x) - g(x)$ tendrá por lo menos m raíces distintas en A , lo cuál es absurdo.

As: $f(x) = g(x)$. □

Corolario.

Si A es dominio entero y $f(x) \in A[x]$ tal que $f(c) = 0$, $\forall c \in S$, donde $S \subseteq A$ es infinito, entonces $f(x) = 0$.

Dem:

Es inmediata. □

Teorema (Fórmula de interpolación de Lagrange).

Sea K un campo, $a_1, \dots, a_n \in K$ distintos entre sí y $b_1, \dots, b_n \in K$ arbitrarios ($n \in \mathbb{N}$). Entonces $\exists!$ polinomio $f(x) \in K[x]$ de grado al más $n-1$ en $f(a_i) = b_i$, $\forall i \in [1, n]$.

Dem:

Basta tomar:

$$f(x) = \sum_{j=1}^n b_j \left(\prod_{\substack{i=1 \\ i \neq j}}^n (a_j - a_i) \right)^{-1} \cdot \left(\prod_{\substack{i=1 \\ i \neq j}}^n (x - a_i) \right)$$

La unicidad se sigue de un corolario anterior. □

Def. Sea A un anillo y $f(x) \in A[x] \setminus A$. Decimos que $f(x)$ es **polinomio irreducible** si no existen dos polinomios $g(x)$ y $h(x) \in A[x]$, con $\text{grad}(g(x)) \geq 1$ y $\text{grad}(h(x)) \geq 1$, y

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

Dicho de otra manera, $f(x)$ es irreducible si, y sólo si dados dos polinomios $g(x), h(x) \in A[x]$, la relación $f(x) = g(x)h(x)$ implica que $g(x) \in A$ o $h(x) \in A$.

En algunas ocasiones, se dice **reducible** en vez de no irreducible.

Recordemos que $f(x) \in A[x]$ **elemento irreducible**, si $\forall g(x), h(x) \in A[x]$ tales que $f(x) = h(x)g(x)$ entonces $g(x)$ o $h(x)$ es una unidad de $A[x]$. Por supuesto, requerimos que A tenga identidad.

Por lo tanto, suponemos que A es dominio entero. En este caso, $A[x]^* = A^*$. En efecto, es claro que $A^* \subseteq A[x]^*$. Recíprocamente, sea $f(x) \in A[x]^* \Rightarrow \exists g(x) \in A[x] \setminus \{0\}$ m

$$\begin{aligned} f(x)g(x) &= 1 \\ \Rightarrow \text{grad}(f(x)) + \text{grad}(g(x)) &= \text{grad}(f(x)g(x)) \\ &= \text{grad}(1) \\ &= 0 \end{aligned}$$

$\Rightarrow \text{grad}(f(x)) = \text{grad}(g(x)) = 0$. Luego: $f(x) = a$ y $g(x) = b$, $a, b \in A$. Así:

$$ab = 1$$

$$\Rightarrow a \in A^* \Rightarrow f(x) \in A^*$$

Por tanto, se cumple la igualdad.

En part. si K es campo, $K[x]^* = K \setminus \{0\}$.

Obs) En un dominio entero A se tiene que elemento irreducible de $A[x] \Rightarrow$ polinomio irreducible de $A(x)$. La recíproca no nec. se cumple. Por ejemplo en $\mathbb{Z}[x]$, todo polinomio de grado 1 es un polinomio irreducible, pero $f(x) = 2x+4 = 2(x+2)$ no es elemento irreducible.

Teorema.

Si K es un campo, entonces todo polinomio no constante de $K[x]$ es polinomio irreducible \Leftrightarrow es elemento irreducible.

Dem:

Se sigue de que $K[x]^* = K \setminus \{0\} = K^*$.



Como $K[x]$ es DE y por tanto, DIP y DFU. Se tiene lo siguiente:

Teorema.

Si K es campo y $f(x) \in K[x]$ de grado ≥ 1 , las sig. son equivalentes:

i) $f(x)$ es polinomio irreducible.

ii) $f(x)$ es elemento irreducible.

iii) $\langle f(x) \rangle$ es ideal primo.

iv) $\langle f(x) \rangle$ es ideal maximal.

v) $K[x]/\langle f(x) \rangle$ es dominio entero.

vi) $K[x]/\langle f(x) \rangle$ es campo.

Dem: ya se tiene.



Teorema.

Si K es campo, entonces todo polinomio no constante se expresa de manera única salvo constantes y orden como un producto finito de polinomios irreducibles de $K[x]$.

Dem:

Y se tiene.



EJEMPLOS.

- 1) Sea K campo, $f(x) \in K[x] \setminus \{0\}$ m $\text{grad}(f(x)) = 3$. Entonces $f(x)$ es pol. irreducible $\Leftrightarrow f(x)$ no tiene raíces en K .
- 2) El polinomio $f(x) = x^3 + x + 1$ es irreducible en $\mathbb{Z}/2\mathbb{Z}[x]$.
- 3) Si p es número primo, entonces el polinomio $f(x) = p$ es elemento irreducible en $\mathbb{Z}[x]$.
- 4) Si p es número primo, entonces el polinomio $f(x) = x^2 - p$ es irreducible en $\mathbb{Q}(x)$ pero no en $\mathbb{R}(x)$.

Recordemos la def. de m.c.d. Un anillo que no admite (para todos sus elementos) el m.c.d. es $\mathbb{Z}[\sqrt{5}]$ ⁷⁾

Def. Sea A D.F.U y $f(x) \in A[x]$ de grado ≥ 1 . Se define el **contenido** de $f(x)$, denotado $c(f)$, como el máximo común divisor de los coef. de $f(x)$, i.e: Si $f(x) = a_0 + a_1 x + \dots + a_n x^n$, donde $a_n \neq 0$ y $n \geq 1$, entonces:

$$c(f) = \text{mcd}\{a_n, \dots, a_1, a_0\} = (a_n, \dots, a_0)$$

Obs) Bajo la notación anterior, tenemos que $a_i = b_i c(f)$, $\forall i \in [0, n]$. Luego,

$$c(f) = (b_0 \cdot c(f), \dots, b_n \cdot c(f))$$

$$= c(f) (b_0, \dots, b_n)$$

$\Rightarrow (b_0, \dots, b_n) \in A^*$. Además, notemos que $c(f) \in A^* \Leftrightarrow \forall p \in A$ elemento irreducible $\exists j \in [0, n]$ m $p \nmid a_j$. Equivalentemente, $c(f)$ no es una unidad ($c(f) \neq 0$) $\Leftrightarrow \exists p \in A$ elemento irreducible de A m $p \mid a_i$, $\forall i \in [0, n]$.

Def. Sea A D.F.U y $f(x) \in A[x]$, con $\text{gr}(f(x)) \geq 1$. Decimos que $f(x)$ es **polinomio primitivo**, si $c(f) \in A^*$.

Proposición.

Sea A D.F.U, $f(x) \in A[x]$, con $\text{gr}(f(x)) \geq 1$. Entonces $\exists!$ (salvo asociadas) $u \in A$ & $g(x) \in A[x]$ tales que $f(x) = u g(x)$, donde $g(x)$ es pol. primitivo.

Dem:

Expresamos $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $n = \text{gr}(f(x)) \geq 1$. Sean $b_0, \dots, b_n \in A$ m $a_i = c(f) b_i$, $\forall i \in [0, n]$ $\Rightarrow f(x) = c(f)(b_0 + b_1 x + \dots + b_n x^n)$, donde $b_0 + b_1 x + \dots + b_n x^n$ es pol. primitivo, pues $(b_0, \dots, b_n) \in A^*$.

Tome $a = c(f)$ y $g(x) = b_0 + \dots + b_n x^n$. As: $f(x) = a g(x)$.

Probemos la unicidad. Sean $b \in A$ y $h(x) \in A[x]$ pol. primitivo m

$$f(x) = b h(x)$$

$$\Rightarrow a g(x) = b h(x)$$

$$\Rightarrow c(g(x)) = c(b h(x))$$

$$\Rightarrow a c(g(x)) = b c(h(x))$$

Donde $c(g(x)), c(h(x)) \in A^*$ $\Rightarrow a$ y b son asociados, i.e $\exists u \in A^*$ m $b = ua$.

$$\Rightarrow a g(x) = ua h(x), \text{ con } a \neq 0.$$

Como $A[x]$ es dominio entero:

$$\Rightarrow g(x) = u h(x)$$

Por tanto, a & b y $g(x)$ & $h(x)$ son asociados.

□

Proposición.

Sea A DFU y $K = \text{coc}(A)$, y $f(x) \in K[x]$ con $\text{grad}(f(x)) \geq 1$. Entonces $\exists!$ (salvo asociados)

$a, b \in A$ y $g(x) \in A[x]$ m

$$f(x) = \frac{a}{b} g(x), \text{ donde } b \neq 0.$$

y $(a, b) = 1$ y $g(x)$ es primitivo.

Dem:

Expresamos:

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \dots + \frac{a_n}{b_n} x^n; b_i \neq 0, \forall i \in [0, n].$$

$$\begin{aligned}
 &= \frac{1}{b_0 b_1 \cdots b_n} \left(a_0 b_1 \cdots b_n + a_1 b_0 b_2 \cdots b_n x + \dots + a_n b_0 \cdots b_{n-1} x^n \right) \\
 &= \frac{1}{b_0 b_1 \cdots b_n} f(x)
 \end{aligned}$$

donde $f(x) = a_0 b_1 \cdots b_n + a_1 b_0 b_2 \cdots b_n x + \dots + a_n b_0 \cdots b_{n-1} x^n$ y su último coef. no es cero. (Si algún $a_i = 0, b_i = 1$). Y:

$$f(x) = c(f(x)) g(x)$$

donde $g(x) \in A[x]$ es primitivo, luego:

$$\begin{aligned}
 f(x) &= \frac{c(f)}{b_0 b_1 \cdots b_n} g(x) \\
 &= \frac{a}{b} g(x)
 \end{aligned}$$

con $a, b \in A$ y $(a, b) = 1$. Probemos la unicidad, suponemos que

$$\frac{a}{b} g(x) = \frac{c}{d} h(x)$$

donde $c, d \in A$, $d \neq 0$ y $h(x) \in A[x]$ es primitivo y $(c, d) = 1$.

$$\Rightarrow ad g(x) = bc h(x)$$

Por la prop. ant. $\exists u \in A^*$ y $g(x) = uh(x)$ y $ad = ubc$. Se tiene que $a/b/c$ con $(a, b) = 1$
 $\Rightarrow a/u/c \Rightarrow \exists r \in A$ y $uc = ur \Rightarrow ad = ubc = arb \Rightarrow d = rb \Rightarrow b \mid d$.

De manera análoga se tiene ahora que $d \mid b \Rightarrow b \mid d$ y d son asociados, i.e $\exists v \in A^*$ y $d = bv$

$$\Rightarrow abv = ubc \Rightarrow a = v^{-1}uc, \text{ con } v^{-1}u \in A^*$$

$\Rightarrow a \mid c$ y c son asociados.

□

Teorema (Lema de Gauss).

Sea A DFLU, $g(x), f(x) \in A[x]$ primitivos, ent. $f(x)g(x)$ es primitivo.

Dem.

Expresamos $f(x) = a_0 + a_1 x + \dots + a_n x^n$ y $g(x) = b_0 + b_1 x + \dots + b_m x^m$, donde $a_n \neq 0 \neq b_m$ & $c(f), c(g) \in A^*$.

Supóngase que $f(x)g(x)$ no es primitivo de $A[x]$, i.e $c(fg) \notin A^*$. Sea $p \in A$ elemento irreducible

$\Rightarrow p \mid c(fg)$. Como $c(f), c(g) \in A^*$ $\Rightarrow p$ no divide a todos los a_i 's ni a todos los b_j 's.

Sea $0 \leq r \leq n$ y $0 \leq s \leq m$ tales que son el primer índice para el cual $p \nmid a_r$ y $p \nmid b_s$. Expresamos:

$$f(x)g(x) = c_0 + c_1 x + \dots + c_{r+s} x^{r+s} + \dots + c_{m+n} x^{m+n}$$

Notemos que $p \nmid c_{r+s}$, ya:

$$c_{r+s} = \underbrace{a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-s} b_{s+1}}_a + \underbrace{a_r b_s + a_{r+1} b_{s-1} + \dots + a_{r+s} b_0}_b + \underbrace{a_{r+s+1} b_1 + \dots + a_{m+n} b_m}_c$$

Por elección de los r y s , $p \nmid a$ y $p \nmid c$. Luego $b = c_{r+s} - a - c \Rightarrow p \mid b = a_r b_s \Rightarrow p \nmid a_r \circ p \nmid b_s$

*c. Por tanto, $f(x)g(x)$ es primitivo. □

Corolario.

Seu A DFU, $f(x)g(x) \in A[x] \setminus A$, entonces $c(f) = r(f)c(g)$ salvo asociados.

Dem:

Expresamos de manera única a:

$$f(x) = a f_1(x) \quad y \quad g(x) = b g_1(x)$$

donde $a, b \in A \setminus \{0\}$ y tanto $f_1(x)$ como $g_1(x)$ son pol. primitivos de $A[x]$. Entonces

$$f(x)g(x) = ab f_1(x)g_1(x)$$

donde $f_1(x)g_1(x)$ es pol. primitivo. Y $a = c(f)$, $b = c(g)$. Por tanto, por unicidad en la descomposición se tiene que $c(fg) = r(f)c(g)$, salvo unidades. □

Corolario.

Seu A DFU, y seu $f(x), g(x) \in A \setminus A$. Entonces $f(x)$ y $g(x)$ son pol. primitivos $\Leftrightarrow fg$ lo es también.

Teorema.

Sea A un DFLU. Y sea $f(x) \in A[x] \setminus A$. Entonces, $f(x)$ es elemento irreducible de $A(x) \Leftrightarrow f(x)$ es polinomio irreducible y primitivo de $A[x]$.

Dem:

\Rightarrow) Suponemos que $f(x)$ es elemento irreducible de $A(x)$. Sean $g(x), h(x) \in A(x)$ m $f(x) = g(x)h(x)$. Puesto que $f(x)$ es elemento irreducible, entonces $g(x) \in A(x)^*$ o $h(x) \in A(x)^* \Rightarrow g(x) = cte.$ o $h(x) = cte.$ Por tanto $f(x)$ es pol. irreducible de $A(x)$.

Por otro lado expresamos al pol. de manera única como $f(x) = af_1(x)$, donde $a = c(f)$ y $f_1(x)$ es pol. primitivo. Como $f(x)$ es elemento irreducible, $c(f) \in A(x)^*$ o $f_1(x) \in A(x)^*$, pero $\text{grad}(f_1(x)) \geq 1$, luego $f_1(x) \notin A(x)^* \Rightarrow c(f) \in A^* = A(x)^*$.

Así, $f(x)$ es pol. primitivo.

\Leftarrow) Sean $g(x), h(x) \in A(x)$ m $f(x) = g(x)h(x)$. Como $f(x)$ es pol. irreducible $\Rightarrow g(x) = cte$ o $h(x) = cte$.

Suponemos $h(x) = c \in A \Rightarrow f(x) = c g(x) = c c(g) g_1(x)$, $g_1(x)$ pol. prim. de $A(x) \Rightarrow c(f) = c \cdot c(g) \Rightarrow$ como $c(f) \in A^* \Rightarrow c \in A^*$, i.e $h(x) \in A(x)^*$. Luego $f(x)$ es elemento irreducible.

□

Obs) Sea A DFLU y $f(x) = a \in A \setminus \{0\}$. Entonces $f(x)$ es elemento irreducible de $A(x) \Leftrightarrow a$ es elemento irreducible de A .

Corolario.

Sea A un DFLU y $f(x) \in A[x] \setminus \{0\}$ y no unidad. Entonces, $f(x)$ es elemento irreducible de $A(x) \Leftrightarrow f(x)$ es cte. con valor a , elemento irreducible de A ó $f(x)$ es pol. primitivo y pol. irreducible.

Teorema.

Sea A DFL y $K = \text{coc}(A)$, y $f(x) \in A[x] \setminus A$. Entonces, si $f(x)$ es pol. irreducible en $K[x]$ $\Rightarrow f(x)$ es pol. irreducible en $A[x]$.

Recíprocamente, si $f(x)$ es pol. prim. y pol. irreducible en $A[x]$, ent. $f(x)$ es polinomio irreducible en $K[x]$.

Dem:

\Rightarrow Es inmediata.

\Leftarrow Sean $g(x), h(x) \in K[x]$ m $f(x) = g(x)h(x)$ con $\text{gr}(g(x)), \text{gr}(h(x)) \geq 1$. Por una prop. exp-
resumos de manera única $g(x) = \frac{a}{b}g_1(x)$ y $h(x) = \frac{c}{d}h_1(x)$ donde $a, b, c, d \in A$, $b, d \neq 0$,
 $(a, b) = 1 = (c, d)$, $g_1(x), h_1(x) \in A[x]$ son pol. primitivos. As: que:

$$bd f(x) = ac g_1(x)h_1(x)$$

$$\Rightarrow bd c(f) = ac c(g_1)c(h_1)$$

donde $c(f), c(g_1), c(h_1) \in A^*$ $\Rightarrow \exists u \in A^*$ m $f(x) = ug_1(x)h_1(x)$, donde $\text{gr}(g_1) = \text{gr}(g)$ y
 $\text{gr}(h_1) = \text{gr}(h)$. Por tanto $f(x)$ no es pol. irreducible de $A[x]$ \square .

\square

Teorema.

Sea A un DFL. Entonces, $A[x]$ es un DFL.

Dem:

Por ser A DFL, $A[x]$ es conmutativo con 1 y es dominio entero. Probaremos que $A[x]$ es DFL.

Sea $K = \text{coc}(A)$ y $H(x) \in A[x]$ no cero y no unidad. Tenemos 2 casos:

1) $\text{grud}(f(x)) = 0 \Rightarrow f(x) = a$, $a \neq 0$ y $a \in A \setminus A^*$. As: que, como A es DFL, $\exists p_1, \dots, p_s \in A$ elementos irreducibles de A tal que $a = p_1 \cdots p_s$. As:;

$$f(x) = P_1(x) \cdots P_s(x)$$

donde $P_i(x) = p_i$, $\forall i \in [1, s]$ son elementos irreducibles de $A[x]$.

2) $\text{grad}(f(x)) \geq 1$. Expresamos a $f(x)$ de manera única como $f(x) = af_1(x)$ donde $a \in A \setminus \{0\}$ y $f_1(x) \in A[x]$ es polinomio primitivo, i.e $a = c(f)$.

Si a es no unidad, expresamos a a como un producto de polinomios (es. de elementos irreducibles de A) (como en la primera parte).

Anulicemos $f_1(x)$. Puesto que $f_1(x) \in A[x] \subseteq K[x]$, enl. $f_1(x)$ se expresa como un producto de polinomios irreducibles de $K[x]$. pues $K[x]$ es DIP. Sea esta descomposición:

$$f_1(x) = h_1(x) \cdot \dots \cdot h_s(x)$$

donde $h_i(x) \in K[x]$ son polinomios irreducibles, $\forall i \in [1, s]$. Cada $h_i(x)$ lo expresamos de manera única como:

$$h_i(x) = \frac{c_i}{d_i} q_i(x), \quad \forall i \in [1, s]$$

donde $c_i, d_i \in A$, $(c_i, d_i) = 1$, $q_i(x) \in A[x]$ es primitivo, $\forall i \in [1, s]$. (Además. q_i es pol. irreducible en $K[x]$). Luego $q_i(x)$ es pol. primitivo y pol. irreducible en $A[x]$, q.s: $q_i(x)$ es elemento irreducible de $A[x]$.

Pero:

$$\begin{aligned} f_1(x) &= \frac{c_1 \cdot c_2 \cdot \dots \cdot c_s}{d_1 \cdot d_2 \cdot \dots \cdot d_s} q_1(x) \cdot \dots \cdot q_s(x) \\ &= \frac{u}{v} q_1(x) \cdot \dots \cdot q_s(x) \end{aligned}$$

donde $u, v \in A \setminus \{0\}$ y $(u, v) = 1$. Por tanto:

$$\begin{aligned} v f_1(x) &= u q_1(x) \cdot \dots \cdot q_s(x) \\ \therefore v c(f_1) &= u c(q_1) \cdot \dots \cdot c(q_s) \end{aligned}$$

$\therefore a = bu$ para algún $u \in A^*$. $\therefore f_1(x) = u q_1(x) \cdot \dots \cdot q_s(x)$. Por ende:

$$\begin{aligned} f(x) &= a f_1(x) \\ &= u p_1(x) \cdot \dots \cdot p_t(x) \cdot q_1(x) \cdot \dots \cdot q_s(x) \end{aligned}$$

donde $u \in A[x]^*$ y $p_1(x), \dots, p_t(x), q_1(x), \dots, q_s(x)$ son elementos irreducibles de $A[x]$.

Así pues, (1) y (2) prueban la existencia de la descomposición. Probaremos la unicidad.

Suponemos que $\text{grad}(f(x)) \geq 1$ ($s; \text{grad}(f(x)) = 0$, estuimos trabajando en A , que es DFLU) y que tenemos las descomposiciones:

$$p_1 \cdot \dots \cdot p_s \cdot q_1(x) \cdot \dots \cdot q_s(x) = f(x) = r_1 \cdot \dots \cdot r_\lambda \cdot m_1(x) \cdot \dots \cdot m_n(x) \dots (1)$$

donde $p_1, \dots, p_s, r_1, \dots, r_\lambda \in A$ y $q_1(x), \dots, q_s(x), m_1(x), \dots, m_n(x) \in A(x)$ son todos elementos irreducibles de $A(x)$. Aplicando contenidas en (1), tenemos que $\exists v \in A^*$ tal que

$$p_1 \cdot \dots \cdot p_s = vr_1 \cdot \dots \cdot r_\lambda \dots (2)$$

y que, por el lema de Gauss, los productos $q_1(x) \cdot \dots \cdot q_s(x)$ y $m_1(x) \cdot \dots \cdot m_n(x)$ son pol. prim. (salvo unidades). Como A es DFLU, entonces $f = l$ y todo p_i es un r_j y viceversa (salvo unidades).

$$\Rightarrow \exists w \in A^*$$

$$q_1(x) \cdot \dots \cdot q_s(x) = w m_1(x) \cdot \dots \cdot m_n(x) \dots (3)$$

Usando (3) y el 2º Lema de Gauss y al saber que $K(x)$ es DFLU, ent. $s = n$ & todo $q_i(x)$ es un $m_i(x)$ y viceversa. Por tanto, la descomposición en (1) es única salvo orden y asociados.

□

Lema (de Gauss 2)

Si A es DFLU y $f(x) \in A(x)$, $\text{gr}(f) \geq 1$, ent. si $f(x)$ es primitivo, $f(x)$ es pol. irreducible en $A(x) \Leftrightarrow$ es pol. irreducible en $K(x)$.

Dom:

Es inmediato del teorema ante. anterior.

□

Teorema (Criterio de Eisenstein).

Sea A un DFLU, $K = \text{coc}(A)$ y $f(x) \in A[x]$ de grado $n \geq 1$ con $f(x) = a_0 + a_1x + \dots + a_nx^n$.

Si existe un elemento irreducible $p \in A$ tal que

i) $p | a_i$, $\forall i \in \{1, \dots, n-1\}$.

ii) $p \nmid a_n$.

iii) $p \nmid a_0$.

entonces $f(x)$ es un pol. irreducible en $K[x]$.

Dem:

Expresamos a $f(x)$ de manera única como $f(x) = a f_1(x)$ donde $a = c(f) \in A$ & $f_1(x) \in A[x]$ es primitivo. Notemos que $p \nmid c(f)$ pues $p \nmid a_n$ y $c(f) \mid a_n$. Además, $f_1(x)$ cumple las mismas cond. (i), (ii) y (iii) con respecto al elemento irreducible p para sus coeficientes (de $f_1(x)$).

Supóngase que $f_1(x)$ fuera pol. irreducible en $K[x]$, ent. el pol. $f(x)$ también lo será, pues si $f(x) = r(x)s(x)$ donde $\text{grad}(r), \text{grad}(s) \geq 1$ con $r(x), s(x) \in K[x]$, entonces:

$$\frac{1}{a} r(x)s(x) = f_1(x)$$

donde $\frac{1}{a} r(x), s(x) \in K[x]$ con grados $\geq 1 \Rightarrow f_1(x)$ es reducible en $K[x] \neq c$. Luego basta suponer que $f_1(x) = f(x)$ o que $f(x)$ es pol. primitivo en $A[x]$. Luego, para probar que $f(x)$ es pol. irreducible en $K[x]$, basta probarlo en $A[x]$.

Supóngase que $f(x)$ es reducible en $A[x]$, seun $g(x), h(x) \in A[x]$ con sus grados ≥ 1 y tal que

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

Expresamos $g(x) = b_0 + b_1x + \dots + b_k x^k$ y $h(x) = c_0 + c_1x + \dots + c_l x^l$ $\pi k+l=n$, $b_k \neq 0 \neq c_l$.

Puesto que $p \mid a_0 \Rightarrow p \mid b_0 \circ p \mid c_0$. Supongamos que $p \mid b_0 \Rightarrow p \nmid c_0$ pues $p^2 \nmid a_0 = b_0 c_0$.

Sea $1 \leq j \leq k$ el primer índice de los b_j $\pi p \nmid b_j$ (este existe, pues si $p \mid b_i, \forall i \in [0, k]$ ent. $p \mid a_n \neq c$). i.e $p \nmid b_i, \forall i \in [0, j-1]$. Entonces:

$$a_j = b_0 c_j + b_1 c_{j-1} + \dots + b_{j-1} c_1 + b_j c_0$$

$$\Rightarrow b_j c_0 = a_j - (b_0 c_j + \dots + b_{j-1} c_1)$$

Como $p \mid a_j \Rightarrow p \mid b_j c_0$ (pues $j < n$), luego $p \mid b_j \circ p \mid c_0 \neq c$ pues $p \nmid b_j$ y $p \nmid c_0$.

As: pues, $f(x)$ es irreducible en $A[x]$.



EJEMPLOS.

1) $f(x) = 6 + 3x^2 + 15x^5 + 7x^7$ es pol. de Eisenstein y pol irreducible en $\mathbb{Q}[x]$ (al tomar el primo $p=3$).

2) $f(x) = x + 4$ no es de Eisenstein pero si es irreducible en $\mathbb{Q}[x]$.

3) Sea A un DFL. Sabemos que $A[x]$ es DFL. Tomemos y una nueva indeterminada algebraicamente independiente a x . Luego, el anillo

$$A[x, y] = A[x][y] \text{ es DFL}$$

Notemos que x es un elemento irreducible en $A[x]$. Luego $f(x, y) = y^3 + x^2y^2 + x^3y + x$ es un pol. irreducible por ser de Eisenstein en $K(x)[y]$ donde $K(x)$ es el coc($A[x]$).

Notas.

1) De ahora en adelante, todos los anillos son commutativos con identidad. (No siempre).

2) De (i): Considere las dos series de potencias

$$f = \sum_{n=0}^{\infty} a_n x^n \quad g = \sum_{n=0}^{\infty} b_n x^n$$

$$\Rightarrow f+g = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

Por def. de orden, $a_n = 0 \quad \forall n < o(f)$ y $b_m = 0, \quad \forall m < o(g)$. Supongu sin pérdida de generalidad que $o(g) \leq o(f)$.

Entonces $a_n + b_n = c_n = 0, \quad \forall n < o(g)$. Si $f+g \neq 0$ (es decir, $f = -g$), entonces $c_{o(f)+g} = a_{o(f)+g} + b_{o(f)+g} \neq 0$ (por def. de orden). Por lo ant. $o(f+g) \geq o(g) = \min\{o(f), o(g)\}$.

De (ii): Supongu $f_g \neq 0$. Probaremos que

$$c_K = \sum_{i=0}^K a_i b_{K-i}$$

es cero $\forall K < o(f) + o(g)$. Supongu $o(g) \leq o(f) \leq o(f) + o(g)$. Si $K < o(f)$, entonces:

$$c_K = \sum_{i=0}^K a_i b_{K-i} = \sum_{i=0}^K 0 \cdot b_{K-i} = 0$$

Pues $a_i = 0 \quad \forall i \leq K < o(f)$. Si $o(f) \leq K < o(f) + o(g)$, tenemos:

$$c_K = \sum_{i=0}^K a_i b_{K-i} = \sum_{i=o(f)}^{o(f)-1} a_i b_{K-i} + \sum_{i=o(f)}^{K} a_i b_{K-i}$$

Donde $a_i = 0 \quad \forall i \in [0, o(f)-1]$ y $b_{K-i} = 0, \quad \forall i \in [o(f), K]$, pues $K-i \leq K-o(f) < o(g)$, $\forall i \in [o(f), K]$. Luego ambas sumas son cero y por ende, $c_K = 0$.

Asi, $o(fg) \geq o(f) + o(g)$.

□

3)

Supongu que A es dominio entero. Por lo anterior $o(fg) \geq o(f) + o(g)$. Notemos que:

$$c_{o(f)+o(g)} = \sum_{i=0}^{o(f)+o(g)} a_i b_{(o(f)+o(g))-i}$$

$$= \sum_{i=0}^{o(f)-1} a_i b_{(o(f)+o(g))-i} + a_{o(f)} b_{o(g)} + \sum_{i=o(f)+1}^{o(f)+o(g)} a_i b_{(o(f)+o(g))-i}$$

Por la part. anterior, las dos sumas son cero, pero $a_{o(f)} b_{o(g)} \neq 0$, pues A es dominio entero

Asi, $o(fg) = o(f) + o(g)$.

Luego, si $f, g \neq 0 \Rightarrow fg \neq 0$, i.e $A[[x]]$ no tiene div. de cero, i.e es dominio entero. □

4) $K_0 \in \mathbb{N}$. Si $K_0 = 0 \Rightarrow I = K[[x]]$.

5) Para probar la igualdad, definimos

$$K' = \left\{ \sum_{n=-m}^{\infty} a_n x^n \mid \dots \right\}$$

el cuál lo hacemos campo con las dos operaciones de la serie de pot. modificadas:

$$\sum_{n=-m}^{\infty} a_n x^n + \sum_{n=-1}^{\infty} b_n x^n = \sum_{n=-\max\{m, 1\}}^{\infty} (a_n + b_n) x^n$$

$$\sum_{n=-m}^{\infty} a_n x^n \cdot \sum_{n=-1}^{\infty} b_n x^n = \sum_{n=(-m+1)}^{\infty} c_n x^n, \text{ con } c_n = \sum_{\substack{i+j=n \\ -m \leq i \\ -1 \leq j}} a_i b_j$$

y damos un isomorfismo entre K' y $K((x))$ (el natural xd).

$$\frac{f}{g} = \frac{f g^{-1}}{x^m} \mapsto x^{-m} \cdot f \cdot g^{-1}$$

6) Podemos proceder por inducción sobre m.

Para $m=1$: Por argumentos anteriores, $f(x) \neq 0$ y $n \leq 1$, digamos $g(x) = b_0 + b_1 x$ y

$$f(x) = a_0 + a_1 x.$$

7) En $\mathbb{Z}[\sqrt{-5}]$:

8) En $K(x)$, los polinomios irreducibles son también elementos irreducibles (cuando el grado del polinomio es ≥ 1).