TEMAS DE MATEMÁTICAS
(Oposiciones de Secundaria)

TEMA 13

<u>POLINOMIOS. OPERACIONES. FÓRMULAS DE NEWTON. DIVISIBILIDAD DE POLINOMIOS. FRACCIONES ALGEBRAICAS.</u>

TEMA 13

POLINOMIOS. OPERACIONES. FÓRMULAS DE NEWTON. DIVISIBILIDAD DE POLINOMIOS. FRACCIONES ALGEBRAICAS.

1. EL ANILLO DE LOS POLINOMIOS DE UNA VARIABLE.

Vamos a considerar por la letra A un anillo conmutativo con elemento unidad, $(A, +, \cdot)$. Representaremos por 0 al elemento neutro de $(A, +)$ y por 1 al neutro de $(A, \cdot)$. Es evidente que todo lo que digamos sobre A, serán válidas para un cuerpo K (siendo habitualmente $\mathbb{R}$ ó $\mathbb{C}$).

DEF Llamaremos Polinomio de una indeterminada con coeficientes en A a toda sucesión $(a_m)_{m\in\mathbb{N}}$ de elementos de A verificando que existe un cierto $n\in\mathbb{N}$ tal que $a_m = 0 \;\; \forall m > n$.

NOTACIÓN El conjunto de los polinomios de una indeterminada con coef. en A se denota por A[x].

Ejemplos.

(2, 3, -1, 0, 0,….) y (0, -1, 0, 1, 2, 0, 0,…) son dos polinomios con coeficientes en el anillo de los números enteros, $\mathbb{Z}$.

DEF Los elementos $a_m\in A$ de un polinomio reciben el nombre de coeficientes. El elemento a_o se llama término independiente y el elemento a_n tal que $a_m = 0 \;\; \forall m > n$ recibe el nombre de coeficiente principal.

DEF Llamaremos grado de un polinomio al nº n, siempre que a_n sea el coeficiente principal del mismo.

1.1. Suma de Polinomios.

DEF Dados $P, Q\in A[x]$ polinomios con $P = (a_m)_{m\in\mathbb{N}}$ y $Q = (b_m)_{m\in\mathbb{N}}$ definimos la suma $+: A[x] \times A[x] \rightarrow A[x]$ como

$$P + Q = (a_o + b_o, a_1 + b_1, a_2 + b_2,\ldots..) = (a_m + b_m)_{m\in\mathbb{N}}$$

La suma está bien definida ya que

$$\exists n\in \mathbb{N} \,/\, a_m = 0 \quad \forall m > n$$

$$\exists n' \in \mathbb{N} \,/\, b_m = 0 \quad \forall m > n'$$

Entonces $a_m + b_m = 0 \;\; \forall m > \max (n, n') \Rightarrow P + Q \in A[x]$

PROP La suma de polinomios de A[x] verifica las siguientes propiedades, siendo P, Q y R elementos de A[x]:

1) Conmutativa: P + Q = Q + P

2) Asociativa: (P + Q) + R = P + (Q + R)

3) Existencia de Elemento neutro: P + 0 = P

4) Existencia de Elemento Simétrico: P + (-P) = 0

Dem.

Sean $P = (a_m)_{m\in\mathbb{N}}$, $Q = (b_m)_{m\in\mathbb{N}}$ y $R = (c_m)_{m\in\mathbb{N}}$

1) $P + Q = (a_m + b_m)_{m\in\mathbb{N}} = (b_m + a_m)_{m\in\mathbb{N}} = Q + P$

2) Análogo

3) Sea 0 = (0, 0, 0,….) el polinomio con todos sus coeficientes nulos.

Así definido, el polinomio 0 verifica que es el polinomio neutro para la suma.

4) Sea $-P = (-a_m)_{m\in\mathbb{N}}$ el polinomio con todos sus coeficientes con signo contrario a los de P.

Trivialmente verifica que P + (- P) = 0

El conjunto A[x] con la ley de composición interna así definida (A[x], +) tiene estructura de grupo conmutativo.

1.2. Producto de polinomios.

DEF Dados P, Q∈A[x] polinomios con $P = (a_m)_{m\in\mathbb{N}}$ y $Q = (b_m)_{m\in\mathbb{N}}$ definimos el producto ·: A[x] x A[x] → A[x] como

$$P \cdot Q = (a_o \cdot b_o,\ a_o \cdot b_1 + a_1 \cdot b_o, \ldots, \sum_{i=0}^{P} a_i \cdot b_{p-i}, \ldots) = (\sum_{i=0}^{m} a_i b_{m-i})_{m\in\mathbb{N}}$$

El producto está bien definido ya que

$$\exists n\in\mathbb{N} \,/\, a_m = 0 \quad \forall m>n$$

$$\exists n' \in\mathbb{N} \,/\, a_m = 0 \quad \forall m>n'$$

Entonces $\sum_{i=0}^{P} a_i b_{p-i} = 0 \quad \forall p > n + n' \Rightarrow \left(\sum_{i=0}^{m} a_i b_{m-i} \right)_{m\in\mathbb{N}} \in A[x]$

PROP El producto de polinomios definido en A[x] verifica las siguientes propiedades, con P, Q, R∈A[x].

1) Conmutativa P · Q = Q · P

2) Asociativa (PQ)R = P(QR)

3) Existencia de elemento neutro P · 1 = P

Dem.

En la demostración tendremos en cuenta que

$$\sum_{i=0}^{m} a_i b_{m-i} = \sum_{i+j} a_i b_j$$

1) $P \cdot Q = \left(\sum_{i+j} a_i b_j \right)_{m\in\mathbb{N}} = \left(\sum_{i+j} b_j a_i \right)_{m\in\mathbb{N}} = \left(\sum_{i+j=m} b_i a_j \right)_{m\in\mathbb{N}} = P \cdot Q$

2) $(PQ)R = \left(\sum_{K+p=m} \left(\sum_{i+j=p} a_i b_j \right) \cdot c_K \right)_{m\in\mathbb{N}} = \left(\sum_{K+p=m} \sum_{i+j=p} a_i b_j c_K \right)_{m\in\mathbb{N}} = \left(\sum_{i+j+K=m} a_i b_j c_K \right)_{m\in\mathbb{N}} =$

$= \sum_{q+i=m} \left(a_i \cdot \sum_{j+K=q} b_j c_K \right) = P \cdot (QR)$

3) Sea $1 \in K[x]$ definido como $1 = (1, 0, 0, 0, \ldots.)$

Entonces verifica que $P \cdot 1 = P \quad \forall P \in A[x]$.

El conjunto A[x] con la ley de composición interna así definida (A[x], ·) tiene estructura de semigrupo conmutativo.

1.3. El Anillo de Polinomios.

PROP Dado A[x] con la suma y el producto definidos, se verifica la propiedad distributiva del producto respecto de la suma.

Dem.

$\forall$P, Q, R$\in$ A[x], hemos de comprobar P · (Q + R) = PQ + PR y (P + Q)R = PR + QR.

Al verificarse la propiedad conmutativa tanto para la suma como para el producto, solo es necesario comprobar una de ellas.

$$P(Q+R) = \sum_{i\in\mathrm{N}} a_i \cdot \left(\sum_{j\in N} b_j + \sum_{k\in\mathrm{N}} c_K \right) = \sum a_i \cdot \sum \left(b_j + c_j \right) = \sum_{i+j=m} a_i (b_j + c_j) =$$

$$= \sum_{i+j=m} a_i b_j + \sum_{i+j=m} a_i c_j = PQ + PR$$

Como conclusión podemos afirmar que (A[x], +, ·) tiene estructura del Anillo conmutativo con elemento unidad.

A[x] recibe el nombre del anillo de los polinomios en una indeterminada.

PROP Si A es un dominio de Integridad $\Rightarrow$ A[x] es un dominio de Integridad.

Dem.

Sean P, Q $\in$ A[x] dos polinomios no nulos.

$P = (a_m)_{m\in\mathbb{N}} = (a_o, a_1, \ldots, a_n, 0, \ldots)$ con $a_m = 0 \quad \forall m > n$ y $a_n \neq 0$

$Q = (b_m)_{m\in\mathbb{N}} = (b_o, b_1, \ldots, b_p, 0, \ldots)$ con $b_m = 0 \quad \forall m > p$ y $b_p \neq 0$

$$P \cdot Q = \left(\sum_{i+j=m} a_i b_j \right)_{m\in\mathbb{N}} = (\ldots, a_n \cdot b_p, \ldots) \text{ y } a_n \cdot b_p \neq 0 \Rightarrow PQ \neq 0$$

OBS Si A[x] es un dominio de integridad, podemos afirmar que

grad (P · Q) = grad (P) + grad (Q) $\forall$P, Q $\in$ A[x] no nulos.

1.3. Otras Estructuras de A[x].

Comprobemos que el anillo A se puede identificar con un subconjunto de A[x].

PROP Sea f: A $\to$ A[x] mediante f(a) = (a, 0, 0,….). Entonces f es un monomorfismo.

Dem.

- f(a + b) = (a + b, 0, 0,….) = (a, 0, 0, 0,….) + (b, 0, 0,…) = f(a) + f(b)
- f(a · b) = (ab, 0, 0,….) = (a, 0, 0,….) · (b, 0, 0,…) = f(a) · f(b)
- f(1) = 1 siendo 1 = (1, 0, 0,….., 0)
- f es inyectiva.

$$f(a) = f(b) \Rightarrow (a, 0, 0, \ldots) = (b, 0, 0, \ldots) \Rightarrow a = b$$

OBS Si identificamos el elemento a con el polinomio (a, 0, 0,….) podemos considerar que A$\subset$A[x]. Los llamaremos polinomios constantes.

Según lo anterior, los elementos de A son polinomios de grado cero, excepto el 0 = (0, 0, 0,….) que no tiene grado.

DEF Definimos la operación externa $\bullet_A$: $A x A[x] \rightarrow A[x]$ como $\forall a \in A$ $\forall (b_m)_{m\in\mathbb{N}} \in A[x]$ $a\cdot (b_1, b_2, b_3,\ldots.) = (a, 0, 0, 0,\ldots) (b_1, b_2, b_3,\ldots.) = (ab_1, ab_2, ab_3,\ldots)$.

PROP La operación externa definida anteriormente verifica las siguientes propiedades; dados $\forall\lambda, \mu\in A$ y $\forall P, Q\in A[x]$.

1) Distributiva respecto de las Escalares: $(\lambda+\mu)\cdot P = \lambda P+\mu P$

2) Distributiva respecto de los polinomios: $\lambda(P+Q) = \lambda P+ \lambda Q$

3) PseudoAsociativa: $\lambda\cdot(\mu P) = (\lambda\mu)\cdot P$

4) Elemento Unidad: $1\cdot P = P$

Dem.

Inmediata.

Como A es un anillo y $(A[x], +)$ es un grupo conmutativo, entonces $(A[x], +, \bullet_A)$ tiene estructura de A-módulo.

Si A tuviese estructura de cuerpo (habitualmente utilizaremos como dominio de operadores el cuerpo $\mathbb{R}$ o el cuerpo $\mathbb{C}$) lo denotaremos por K, y entonces $(A[x], +, \bullet_K)$ es un espacio vectorial sobre K.

Y aun podemos definir otra nueva estructura algebraica sobre A[x]. Como es un anillo conmutativo y unitario que verifica

$$\lambda(PQ) = (\lambda P)Q = P(\lambda Q) \quad \forall \lambda\in A \quad y \quad \forall P,Q\in A[x]$$

entonces A[x] es un A-álgebra, o álgebra de los polinomios con una indeterminada sobre el anillo A.

1.4. Notación Clásica de los Polinomios.

DEF Sea X el polinomio de A[x] que tiene todos sus coeficientes nulos menos el segundo, cuyo valor es 1 (Neutro del producto en A). Es decir, $X = (0, 1, 0, 0,\ldots.)$.

PROP $X^n = (0, 0,\ldots,0, \overset{n+1}{\smile}{1}, 0,\ldots)$ $\forall n\in\mathbb{N}$

Dem.

Inmediata.

Dado $P\in A[x]$ con $P = (a_m)_{m\in\mathbb{N}}$ podemos escribirlo como $P = (a_0, a_1, a_2,\ldots) =$

$(a_0, 0, 0,\ldots) + (0, a_1, 0,\ldots) + (0, 0, a_2,\ldots) + \ldots.= a_0 + a_1(0, 1, 0,\ldots) + a_2(0, 0, 1,\ldots) +\ldots =$

$= a_0 + a_1x + a_2x^2 + \dots + a_nx^n$

sabiendo que $a_m = 0 \ \forall m > n$

PROP Se verifica:

1) $a_Kx^K + b_Kx^K = (a_K + b_K)x^K \quad \forall k \in \mathbb{N}$

2) $(a_Kx^K) \cdot (b_px^p) = a_K \cdot b_p \cdot x^{K+p} \quad \forall k, p \in \mathbb{N}$

Dem.

Inmediata.

Si tomamos $X^0 = 1$ por convenio, junto con la proposición anterior, obtenemos una forma cómoda de realizar la suma y el producto de polinomios.

DEF Un polinomio $P \in A[x]$ recibe el nombre de Monomio si todos sus coeficientes son nulos menos uno.

DEF Llamaremos Polinomio a una suma finita de monomios.

Ejemplo.

1) a_ix_i es un monomio y $a_0 + a_1x + \dots + a_nx^n$ un polinomio.

2. FORMULA DE NEWTON.

Antes de llegar a obtener la fórmula de Newton para el desarrollo, la potencia de un binomio, o su generalización a la potencia de un polinomio mediante la fórmula de Leibniz, veamos unos resultados previos.

2.1. Números Combinatorios.

Debido a que en la fórmula de Newton aparecen los números combinatorios, comenzaremos el repaso por éstos, remitiendo al lector al tema 3 del temario específico si desea encontrar las demostraciones de las propiedades que enumeremos.

Sabemos que los números combinatorios se definen como

$$\binom{n}{K} = \frac{n!}{K!(n-K)!}$$

siendo sus propiedades más importantes:

1) $\binom{n}{0} = 1 \quad y \quad \binom{n}{n} = 1$

2) $\binom{n}{K} = \binom{n}{n-K}$

3) $\binom{n}{K} = \binom{n-1}{K-1} + \binom{n-1}{K}$ Llamada fórmula de Stiefel.

4) $\binom{n}{K} = \binom{n-1}{K-1} + \binom{n-2}{K-1} + \ldots\ldots + \binom{K}{K-1} + \binom{K-1}{K-1}$

Si escribimos los números combinatorios en forma de triángulo

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

………….

Y aplicando la fórmula de Stieffel, obtenemos que cada número combinatorio es suma de los dos que tiene encima, quedando

1 1
1 2 1
1 3 3 1
1 4 6 4 1
……..

que se conoce como triángulo de Tartaglia (Nicola de Fontana) o triángulo de Pascal.

2.2. Fórmula de Newton.

Vamos ahora a obtener el desarrollo del binomio de Newton, para lo cual utilizaremos las propiedades de los números combinatorios.

PROP Se verifica $(a+b)^n = \sum_{K=0}^{n} \binom{n}{K} a^{n-K} \cdot b^K$

Dem.

Realizaremos la demostración por inducción en el exponente, n.

Para n = 1 $\quad (a+b)^1 = a+b = 1\cdot a + 1\cdot b = \binom{1}{0}a + \binom{1}{1}b = \sum_{K=0}^{1}\binom{1}{K}a^{1-K}\cdot b^K$

Para n = 2 $\quad (a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}ab + \binom{2}{2}b^2 = \sum_{K=0}^{2}\binom{2}{K}a^{2-K}\cdot b^K$

Supongamos que

$$(a+b)^{n-1} = \binom{n-1}{n}a^{n-1} + \binom{n-1}{1}a^{n-2}\cdot b + \ldots + \binom{n-1}{n-2}ab^{n-2} + \binom{n-1}{n-1}b^{n-1} = \sum_{K=0}^{n-1}\binom{n-1}{K}^{n-1-K}\cdot b^K$$

Veamos para n $\quad (a+b)^n = (a+b)^{n-1}\cdot(a+b) = (a+b)^{n-1}\cdot a + (a+b)^{n-1}\cdot b =$

$$= \sum_{K=0}^{n-1}\binom{n-1}{K}a^{n-K}\cdot b^K + \sum_{K=0}^{n-1}\binom{n-1}{K}a^{n-1-K}\cdot b^{K+1} =$$

$$= \binom{n-1}{0}a^n + \sum_{K=1}^{n-1}\binom{n-1}{K}a^{n-K}\cdot b^K + \sum_{K=0}^{n-2}\binom{n-1}{K}a^{n-(K+1)}\cdot b^{k+1} + \binom{n-1}{n-1}b^n =$$

$$= \binom{n-1}{0}a^n + \sum_{K=1}^{n-1}\binom{n-1}{K}a^{n-K}\cdot b^K + \sum_{K=1}^{n-1}\binom{n-1}{K-1}a^{n-K}\cdot b^K + \binom{n-1}{n-1}b^n =$$

$$= \binom{n-1}{0}a^n + \sum_{K01}^{n-1}\left[\binom{n-1}{K} + \binom{n-1}{K-1}\right]a^{n-K}\cdot b^K + \binom{n-1}{n-1}b^n =$$

Aplicando la fórmula de Stiefel.

$$= \binom{n-1}{0}a^n + \sum_{K=1}^{n-1}\binom{n}{K}a^{n-K}b^K + \binom{n-1}{n-1}b^n =$$

Y teniendo en cuenta que $\binom{n-1}{0} = \binom{n}{0}$ $\;y\;$ $\binom{n-1}{n-1} = \binom{n}{n}$ queda

$$= \binom{n}{0}a^n + \sum_{K=1}^{n-1}\binom{n}{K}a^{n-K}\cdot b^K + \binom{n}{n}b^n = \sum_{K=0}^{n}\binom{n}{K}a^{n-K}\cdot b^K.$$

El resultado anterior lo podemos particularizar a los binomios de A[x].

$$(1+x)^n = \sum_{K=0}^{n} \binom{n}{K} x^K = 1 + nx + \frac{n\cdot(n-1)}{2} x^2 + \ldots + nx^{n-1} + x^n$$

$$(a+x)^n = \sum_{K=0}^{n} \binom{n}{K} a^{n-K} \cdot x^K = a^n + na^{n-1} \cdot x + \frac{n(n-1)}{2} a^{n-2} \cdot x^2 + \ldots + nax^{n-1} + x^n$$

$$(a+bx)^n = \sum_{K=0}^{n} \binom{n}{K} a^{n-K} \cdot (bx)^K = a^n + na^{n-1} \cdot b \cdot x + \ldots + nab^{n-1} \cdot x^{n-1} + b^n x^n$$

Y en general:

$$\left(ax^i + bx^j\right)^n = \sum_{K=0}^{n} \binom{n}{K} \left(ax^i\right)^{n-K} \cdot \left(bx^j\right)^K = a^n \cdot x^{ni} + na^{n-1} \cdot b \cdot x^{ni-i+j} + \ldots + nab^{n-1} x^{nj+i-j} + b^n x^{nj}$$

2.3. Fórmula de Leibniz.

La fórmula de Newton se puede generalizar a un polinomio cualquiera.

Vamos a explicar como se obtiene el desarrollo de la potencia n-ésima de un polinomio formado por m términos, sin entrar en demostraciones farrangosas.

Sea el polinomio ($a_1 + a_2 + \ldots + a_m$) que lo expresaremos por $\sum_{i=1}^{m} a_i$. Queremos calcular su potencia n-ésima.

$$\left(\sum_{i=1}^{m} a_i\right)^n = (a_1 + \ldots + a_m) \cdot (a_1 + \ldots + a_m) \cdot \ldots \cdot (a_1 + \ldots + a_m)$$

siendo un producto de n factores.

Si aplicamos de forma reiterada la propiedad distributiva obtenemos que cualquier sumando del desarrollo es de la forma:

$$a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_m^{\alpha_m} = \prod_{i=1}^{m} a_i^{\alpha_i} \qquad (1)$$

verificándose que la suma de exponentes es n

$$\sum_{i=1}^{m} \alpha_i = n$$

Para ver el coeficiente que antecede a cada sumando, hemos de contar las veces que aparece repetido. Para ello, tengamos en cuenta que el término (1) proviene de una permutación de los $(a_i)_{i:1,...,m}$ en los que cada a_i aparece repetido α_i veces. Ese número de permutaciones es

$$P_n^{a_1,a_2,...,a_m} = \frac{n!}{a_1!a_2!\cdot....\cdot a_m!}$$

3. DIVISIBILIDAD DE POLINOMIOS.

A lo largo de este punto, trabajaremos con el cuerpo K en lugar del anillo conmutativo A. Por tanto, llamaremos K[x] al anillo de los polinomios en una indeterminada (sobre el cuerpo K).

3.1. División Enclíde.

PROP Sean A y B polinomios de K[x] con $B \neq 0$. Existen y son únicos dos polinomios C y R de K[x] verificando

$$A = B\cdot C + R \qquad \text{y} \qquad \text{grad}(R) < \text{grad}(B) \text{ si } R \neq 0$$

Dem.

• Existencia.

Consideremos el conjunto de los polinomios de la forma $A - BQ$ donde Q recorre k[x]. Se pueden dar dos casos:

a) Existe $C \in K[x]$ tal que $A - BC = 0$

Entonces A = BC y tenemos demostrada la existencia. En este caso R = 0.

b) $\forall\ Q \in K[x]\quad A - BQ \neq 0 \Rightarrow \exists c \in K[x]$ /grad $(A - BC) \leq$ grad $(A - BQ)\quad \forall Q \in K[x]$

Escribamos $A = BC + R$. Comprobemos que grad (R) < grad (B).

Supongamos que grad (R) $\geq$ grad (B).

Si grad (B) = m $\Rightarrow$ grad (R) = m + K con $K \geq 0$. Entonces

$$B = b_o + b_1 x + ... + b_m x^m \quad con\ b_m \neq 0$$

$$R = r_o + r_1 x + ... + r_{m+K} \cdot x^{m+K} \quad con\ r_{m+K} \neq 0 \quad (K \geq 0)$$

Si multiplicamos el polinomio B por el monomio $r_{m+K}\cdot(b_m)^{-1}x^K$ (llamaremos $c_K = r_{m+K}\cdot b_m^{-1}$), obtenemos que $R' = R - c_K x^K \cdot B$ es un polinomio tal que grad (R´) < grad (R), de donde

$$A = BC + R = BC + R' + C_K x^K \cdot B = B(C + C_K x^K) + R' = BC' + R'$$

que puede escribirse como

$$A - BC' = R'$$

Siendo, por hipótesis, $R' \neq 0$

Pero grad $(R') <$ grad (R) con lo que

$$\text{Grad } (A - BC') < \text{grad } (A - BC)$$

lo que es una contradicción con la elección que hemos de C.

Por tanto $\exists C \in K[x]$ / $A = BC + R$ con grad $(R) <$ grad (B)

- Unicidad.

Supongamos que $\exists C_1\ R_1 \in K[x]$ /$A = BC_1 + R_1$ con grad $(R_1) <$ grad (B)

Entonces $R - R_1 = B(C_1 - C)$

Si $C_1 \neq C \Rightarrow$ grad $(R - R_1) \geq$ grad (B)

Y llegamos a una contradicción.

Entonces $C_1 = C$ y por tanto $R_1 = R$, siendo únicos.

Si realizamos la división euclidea de A entre B, llamamos cociente al polinomio C y Resto al polinomio R, tal que $A = BC + R$.

3.2. Relaciones en K[x].

DEF Diremos que dos polinomios P, $Q \in K[x]$ son Asociados cuando sólo se diferencian en el producto de constantes. Es decir, $P = a \cdot Q$ con a **Î K.**

Podemos definir en K[x] la relación siguiente:

DEF Dados P, $Q \in K[x]$, $P \sim Q$ si y solo si $\exists a \in K$ / $P = a \cdot Q$. La relación recibe el nombre de " ser asociado".

PROP La relación definida anteriormente es una relación de equivalencia.

<u>Dem.</u>

Inmediata.

DEF Sean P y Q dos polinomios de K[x]. Diremos que Q divide a P si existe $C \in K[x]$ tal que $P = QC$. Lo denotaremos por Q/P.

PROP La relación “divide a” es una relación de orden en K[x].

Dem.

Inmediata.

3.3. Máximo Común Divisor y Mínimo Común Múltiplo de Polinomios.

Como K[x] es un anillo, definiremos los términos de MCD y mcm en función de los ideales de K[x].

PROP Sea I un ideal de K[x]. Entonces existe un polinomio $P \in K[x]$ tal que I es el conjunto de todos los múltiplos de P.

Dem.

- Si $I = \{0\} \Rightarrow P = 0$
- Si $I \neq \{0\} \Rightarrow$ Sea $P \in I$ un polinomio tal que grad (P) $\leq$ grad (Q) $\forall Q \in I$.

Entonces P es un polinomio de grado mínimo en I.

$\forall Q \in P$, al realizar la división euclidea.

$\exists C, R \in K[x]$ tal que $Q = P \cdot C + R$ con grad (R) < grad (P)

Si $R \neq 0$ sea $R = Q - P \cdot C$

$P \in I, Q \in I, C \in K[x] \Rightarrow$ Como I es ideal $P \cdot C \in I \Rightarrow R \in I$

Contradicción: Hemos llegado a la conclusión de que $R \in I$ con grado menor que el de P.

Entonces $R = 0$ y $Q = P \cdot C \Rightarrow Q \in (P) \Rightarrow I \subset (P)$

Como trivialmente $P \in I \Rightarrow (P) \subset I$.

Obtenemos que $I = (P)$.

El polinomio P es único, salvo asociados.

DEF Llamamos Base de ideal I (con $I \neq \{0\}$) al polinomio normalizado P tal que $I = (P)$. (Polinomio Normalizado es el polinomio de coeficiente principal 1). En caso de que $I = \{0\}$, el polinomio base de I será $P = 0$.

DEF Sean P y Q polinomios de K[x]. Llamamos máximo común divisor de P y Q y se representa por MCD (P, Q), al polinomio base del ideal (P) + (Q).

PROP Sea $D = MCD(P, Q)$ siendo $P, Q \in K[x]$ dos polinomios. El polinomio D verifica:

1) $\exists A, B \in K[x]$ dos polinomios tales que $D = PA + QB$

2) D/P y D/Q.

3) Si $\exists D' \in K[x] \,/\, D'/P$ y $D'/Q \Rightarrow D'/D$ (D es el mayor de los divisores comunes).

<u>Dem.</u>

1) Sabemos que $(P) + (Q)$ es un ideal de $K[x]$, por lo que existirá $D \in K[x]$ tal que $(P) + (Q) = (D)$.

Como $D \in (D)$ ya que $D = D \cdot 1 \Rightarrow D \in (P) + (Q)$

Si $D \in (P) + (Q) \Rightarrow \exists A, B \in K[x] \,/\, D = P \cdot A + Q \cdot B$

D se expresa como un polinomio de (P) más otro de (Q).

2) $P \in (P) + (Q) \Rightarrow P \in (D) \Rightarrow D/P$

$Q \in (P) + (Q) \Rightarrow Q \in (D) \Rightarrow D/Q$

3) Sea $D' \in K[x]$ tal que D'/P y D'/Q.

Entonces $\exists G, H \in K[x]$ tales que $P = D'G$ y $Q = D'H$

Siendo $D = P \cdot A + Q \cdot B = (D'G)A + (D'H)B = D'(GA + HB)$

Y como $GA + HB \in K[x] \Rightarrow D'/D$

DEF Diremos que dos polinomios $P, Q \in K[x]$ son primos entre si $MCD(P, Q) = 1$.

PROP Sean P y Q dos polinomios de $K[x]$ y $D = MCD(P, Q)$. Si $D \neq 0$ y escribimos $P = P'D$ y $Q = Q'D$ entonces P' y Q' son primos entres si.

<u>Dem.</u>

Dados P y Q $\exists A, B \in K[x] \,/\, D = P \cdot A + Q \cdot B$

$D = P'DA + Q'DB \Rightarrow 1 = P'A + Q'B \Rightarrow MCD(P', Q') = 1$

PROP Sean $A, P, Q \in K[x]$

A/PQ y $MCD(A, P) = A/Q$

<u>Dem.</u>

Como MCD (A, P) = 1 $\Rightarrow \exists G, H \in K[x] / 1 = A \cdot G + PH$

Al multiplicar por Q resulta $Q = AQG + PQH$

Como A/PQ $\Rightarrow \exists C \in K[x] / PQ = AC$

Luego $Q = AQG + ACH \Rightarrow A = A \cdot (QG + CH)$

Y como $(QG + CH) \in K[x] \Rightarrow A/Q$

COROLARIO Si $A \in K[x]$ es primo con $P, Q \in K[x]$ entonces A es primo con $P \cdot Q$.

DEF Sea P y Q dos polinomios de K[x]. Llamamos mínimo común múltiplo de P y Q, y se re presenta por mcm (P, Q), al polinomio base del ideal $(P) \cap (Q)$.

PROP Sean P y Q dos polinomios de K[x] y M = mcm (P, Q). El polinomio M verifica:

1) P/M y Q/M (M es múltiplo de P y Q).

2) Si $\exists M' \in K[x]$ / P/M´ y Q/M´ $\Rightarrow$ M/M´

Dem.

1) Por definición de M se tiene $(P) \cap (Q) = (M)$

$M \in (M) \Rightarrow M \in (P) \cap (Q) \Rightarrow \begin{cases} M \in (P) \Rightarrow P/M \\ M \in (Q) \Rightarrow Q/M \end{cases}$

2) Si $\exists M' \in K[x]$ / P/M´ y Q/M´ $\Rightarrow M' \in (P)$ y $M' \in (Q)$

Entonces $M' \in (P) \cap (Q) \Rightarrow M' \in (M) \Rightarrow$ M/M´

Dados dos polinomios de K[x], vamos a ver un método para calcular su máximo común divisor.

PROP Sean P y Q dos polinomios de K[x]. Si existen $C, R \in K[x]$ tales que $P = QC + R$, entonces mcd (P, Q).

Dem.

Sean D = mcd (P, Q) y D´= mcd (Q, R)

Es claro que D/P y D/Q $\Rightarrow$ D/P y D/QC $\Rightarrow$ D/P-QC $\Rightarrow$ D/R

Entonces D/Q y D/R $\Rightarrow$ D/D´. (1)

De forma Análoga; como D´/Q y D´/R $\Rightarrow$ D´/P

Entonces D'/Q y $D'/P \Rightarrow D'/D$ (2)

Como D y D´ son dos polinomios normalizados, de (1) y (2) se deduce que $D = D'$.

Una vez que sabemos calcular el máximo común divisor, podemos calcular el mínimo común múltiplo de la siguiente forma.

PROP Sean $P, Q \in K[x]$ con $P = \sum_{i=0}^{n} a_i x^i$ y $Q = \sum_{j=0}^{m} b_j x^j$ siendo $a_n \neq 0$ y $b_m \neq 0$. Si $D = MCD(P, Q)$ y $M = mcm(P, Q)$ entonces se verifica la igualdad

$$a_n \cdot b_m \cdot MD = PQ$$

<u>Dem.</u>

Sea $M' = PQ' = P'Q$ ya que $P = P'D$ y $Q = Q'D$

Es claro que el coeficiente principal de M´ es $a_n b_m$ y que $PQ = M' \cdot D$

Por definición de M´ se verifica que M´ es múltiplo de P (P/M') y de Q (Q/M'), por tanto M´ es múltiplo de M (M/M') (1).

Como M es múltiplo de P y Q $\Rightarrow \exists A, B \in K[x] \,/\, M = PA = QB$

$$PA = QB \Rightarrow P'DA = Q'DB \Rightarrow P'A = Q'B$$

Pero como P´ y Q´ son primos entre si F $\Rightarrow \exists G, H \in K[x] \,/\, B = P'G$ y $A = Q'H$

Entonces $M = PA = QB \Rightarrow M = PQ'H = QP'G \Rightarrow M = M'H = M'G$

Luego M es múltiplo de M´ (M'/M) (2)

De (1) y (2) se obtiene que $M' = a_n b_m M$

Como $PQ = M'D \Rightarrow PQ = a_n b_m MD$

<u>3.4. Descomposición Factorial de K[x].</u>

DEF Diremos que un Polinomio $P \in K[x]$ es Irreducible o Primo si $grad(P) \geq 1$ y no es posible escribirlo como producto de dos polinomios $P_1, P_2 \in K[x]$ tales que $grad(P_i) < grad(P)$ i: 1, 2.

En caso contrario diremos que el polinomio es reducible o descomponible en K[x].

PROP Los polinomios de primer grado, $X - a$, con $a \in K$ son primos o irreducibles en K[x] (cualquiera que sea K).

<u>Dem.</u>

Sea $P = X - a$ con grad (P) = 1.

Supongamos que P es reducible: $\exists P_1\ P_2 \in K[x] \,/\, P = P_1 \cdot P_2$ y Grad (Pi) < grad (P) $\forall$i: 1, 2.

Si $P = P_1 \cdot P_2 \Rightarrow$ grad (P) = grad (P_1) + grad (P_2)

Entonces 1 = grad (P_1) + grad (P_2). Caben dos posibilidades:

Si grad (P_1) = 1 y grad (P_2) = 0 $\Rightarrow$ Contradicción: grad (P) = grad (P_1)

Si grad (P_1) = 0 y grad (P_2) = 1 $\Rightarrow$ Contradicción: grad (P) = grad (P_2)

Luego P es irreducible.

DEF Diremos que K[x] es Algebraicamente Cerrado si sus únicos polinomios irreducibles son de grado 1.

El que K[x] sea algebraicamente cerrado depende del cuerpo K. Es decir, el concepto de irreducibilidad de un polinomio depende de K.

Por ejemplo, $x^2 - 5$ es irreducible en Q[x] pero no en $\mathbb{R}[x]$ $\left(x^2 - 5 = \left(x + \sqrt{5}\right)\left(x - \sqrt{5}\right)\right)$

Y también $x^2 + 5$ es irreducible en $\mathbb{R}[x]$ pero no en $\mathbb{C}[x]$ $\left(x^2 + 5 = \left(x + i\sqrt{5}\right)\left(x - i\sqrt{5}\right)\right)$.

$\mathbb{C}[x]$ es algebraicamente cerrado.

PROP Para todo polinomio $P \in K[x]$ tal que grad (P) > 0, existe $\lambda \in K$, $P_1,\ldots,P_m \in K[x]$ polinomios primos normalizados y $\alpha_1, \alpha_2, \ldots, \alpha_m$ enteros mayores de 1 únicos tales que

$$P = \lambda \cdot P_1^{\alpha_1} \cdot \ldots\ldots \cdot P_m^{\alpha_m}$$

<u>Dem.</u>

- Existencia.

Vamos a realizar la demostración por inducción en el grado de P. Si grad (P) = 1 la proposición es trivialmente cierta.

Supongamos cierta la proposición para todos los polinomios de grado $n - 1$.

Si grad (P) = n

En caso de que P sea irreducible, la descomposición es inmediata.

Supongamos pues, que P es descomponible o reducible.

Entonces $\exists Q \in K[x]$ con $0 < \text{grad}(Q) < \text{grad}(P)$ y verificando que el grado de Q es el menor de entre todos los divisores de P que cumplan la condición anterior para los grados.

Con esas condiciones podemos decir que Q es irreducible pudiendo escribir

$$P = Q \cdot P'$$

Pero grad (P´) < grad (P) y aplicando la hipótesis de inducción tenemos

$$P' = \lambda' P_1^{\beta_1} \cdot ..... \cdot P_{m'}^{\beta_{m'}}$$

donde Q puede coincidir con algún P_i o no .

Entonces $P = Q \cdot P' = \lambda P_1^{\alpha_1} \cdot .... \cdot P_m^{\alpha_m}$ siendo P_i polinomios irreducibles normalizados y $0 < \alpha_i$ enteros $\forall$i: 1,…., m.

• Unicidad.

Igualmente realizaremos la demostración por inducción en el grado de P.

Si grad (P) = 1 la proposición se cumple de forma evidente.

Supongamos que es cierto para grad (P) = n – 1.

Si grad (P) = n

Supongamos $P = \lambda P_1^{\alpha_1} \cdot ..... \cdot P_m^{\alpha_m} = \mu Q_1^{\beta_1} \cdot .... \cdot Q_{m'}^{\beta_{m'}}$

Como los polinomios P_i i: 1,…., m y Q_j j: 1,…, m´ están normalizados, debe de ocurrir que $\lambda = \mu$.

Dados dos polinomios A y B que son irreducibles y normalizados, si $A \neq B$ entonces A y B son primos entre si. Teniendo en cuenta esto,

P_1 es primo, normalizado y $P_1 / Q_1^{\beta_1} \cdot .... \cdot Q_{m'}^{\beta_{m'}}$

Entonces, aplicando una proposición anterior, P_1 debe coincidir con algún Q_j $1 \leq j \leq m'$.

Sea $P_1 = Q_1$ (Reordenamos si es necesario).

Entonces queda $P_1^{\alpha_1 - 1} \cdot P_2^{\alpha_2} \cdot .... \cdot P_m^{\alpha_m} = Q_1^{\beta_1 - 1} \cdot .... \cdot Q_{m'}^{\beta_{m'}}$

Como ahora ambos polinomios tienen un grado menos, aplicamos la hipótesis de inducción.

$P_i = Q_i \quad \forall i: 1,\ldots, m, \quad m = m' \quad y \quad \alpha_i = \beta_i \quad \forall i: 1,\ldots, m.$

Siendo la descomposición única.

COROLARIO Sean A y B dos polinomios de K[x] con

$$A = l P_1^{a_1} \cdot \ldots \cdot P_m^{a_m} \quad \text{y} \quad B = m \cdot P_1^{b_1} \cdot \ldots \cdot P_m^{b_m}$$

siendo P_i polinomios irreducibles normalizados, y $\alpha_i, \beta_i \in \mathbb{N} - \{0\}$ para todo i: 1,…, m. Entonces:

$$Q/P \iff \beta_i \le \alpha_i \qquad \forall i: 1,\ldots, m$$

Hasta ahora hemos estado hablando de polinomios en una indeterminada. Para cada polinomio podemos definir una función como sigue:

$\forall P \in K[x]$ definimos $P^*: K \to K$ aplicación tal que si $P = a_o + a_1X + \ldots + a_nX^n$ entonces

$$P^*(x) = a_o + a_1x + \ldots + a_nx^n \quad \forall x \in K$$

DEF La aplicación P^* recibe el nombre de función polinómica asociada al polinomio $P \in K[x]$.

La suma y producto de funciones polinómicas se realiza como sigue:

$$(P^* + Q^*)(x) = P^*(x) + Q^*(x)$$

$$(P^*Q^*)(x) = P^*(x) \cdot Q^*(x)$$

Habitualmente, se escribe P(x) en lugar de $P^*(x)$. Aun así, debemos ser conscientes de la diferencia, P(x) es una función y P(X) es una función del anillo K[x]. Por abuso de notación llamaremos polinomio a ambos, y los denotaremos igual.

DEF Llamaremos valor numérico de un polinomio en una indeterminada, al valor que se obtiene al sustituir la variable por su valor correspondiente.

TEOREMA. Teorema del Resto.

El resto de la división de un polinomio es X por el binomio X – a coincide con el valor numérico del polinomio en x = a.

Dem.

Sea $P \in K[x]$. Al dividir P entre (X – a) tenemos $P = (X - a) \cdot Q + R$ con grad(R) = 0

Tomando ahora $P(a) = (a - a)\, Q(a)$ `R $\Rightarrow$ R = P(a)

DEF Dado un polinomio $P(x)$, llamaremos raíces o ceros del polinomio a los valores de la indeterminada x, para los que el valor numérico de $P(x)$ es cero.

TEOREMA. Teorema del Factor.

Sea $P \in K[x]$. $a \in K$ es raíz de $P(x) \Leftrightarrow (x - a) / P$.

<u>Dem.</u>

"$\Rightarrow$"

Si $a \in K$ es raíz de $P \Rightarrow P(a) = 0$

Como $P = (x - a) Q + R$ y $P(a) = 0 \Rightarrow R = 0$

Luego $P = (X - a) Q \Rightarrow X - a / P$

"$\Leftarrow$"

Si $(X - a) / P \Rightarrow P = (X - a) \cdot Q$

Entonces $P(a) = (a - a) \cdot Q(a) \Rightarrow P(a) = 0 \Rightarrow$ a es raíz de P.

PROP Sea $P \in K[x]$ con $P = a_o + a_1 X + \ldots .. + a_n X^n$ con $a_i \in K$ i: 1,…, n. Si P admite m raíces distintas $x_1, x_2, \ldots ., x_m$ con $m \leq n$, entonces

$$P = (X - x_1)(X - x_2) \cdot \ldots\ldots \cdot (X - x_m) H$$

con $H = a_n \cdot X^{n-m} + \ldots .$

<u>Dem.</u>

Como $x_1 \in K$ es una raíz de $P \Rightarrow X - x_1 / P \Rightarrow$

$\Rightarrow P = (X - x_1) \cdot H_1$ siendo $H_1 = a_n X^{n-1} + \ldots .$

Como $x_2 \in K$ es otra raíz de $P \Rightarrow X - x_2 / P \Rightarrow X - x_2 / (X - x_1) H_1$

Y como $X - x_2$ no divide a $X - x_1 \Rightarrow X - x_2 / H_1$

$\Rightarrow H_1 = (X - x_2) H_2$ con $H_2 = a_n X^{n-2} + \ldots .$

$\Rightarrow P = (X - x_1)(X - x_2) H_2$

Reiterando el proceso m veces obtenemos que

$$P = (X\ x_1) \cdot \ldots . \cdot (X - x_m) \cdot H \quad \text{con} \quad H = a_n X^{n-m} + \ldots .$$

PROP Todo polinomio de grado n de K[x] admite a lo sumo n raíces.

<u>Dem.</u>

Si grad (P) = n $\Rightarrow$ $P = a_n X^n + \ldots + a_1 X + a_o$

Si P admite n raíces $x_1, \ldots, x_n$, por la proposición anterior

$$P = a_n (X - x_1) \cdot \ldots \cdot (X - x_n)$$

Veamos que no puede tener más raíces.

Sea r otra raíz de P. Entonces $r \neq x_i \quad \forall i: 1, \ldots, n$.

$P(R) = 0$ por ser r raíz de P

$P(r) = a_n (r - x_1)(r - x_2) \ldots \ldots (r - x_n) \neq o$

$\Rightarrow$ Contradicción, r no es raíz de P, y por tanto P tiene a lo sumo n raíces.

4. FRACCIONES ALGEBRÁICAS.

DEF Llamaremos fracción algebraica a un par de polinomios N, $D \in K[x]$ con $D \neq 0$. El primero, N, recibe el Nombre de Numerador y el segundo, D, de denominador. Se representa por $\frac{N}{D}$.

DEF Definimos en el conjunto $K[x] \times K[x]^*$ la relación de equivalencia R dada por (siendo $K[x]^* = K[x] - \{0\}$):

$$\frac{N}{D} R \frac{N'}{D'} \Leftrightarrow N \cdot D' = DN'$$

PROP La relación R definida en $K[x] \times K[x]^*$ es una relación de equivalencia.

Dem.

Inmediata.

DEF Cada clase de $K[x] \times K[x]^* / R$ recibe el nombre de razón algebraica, siendo $K[x] \times [x]^* / R$ el conjunto de razones algebraicas.

4.1. El Cuerpo de las Razones Algebraicas.

4.1.1. Suma de razones algebraicas.

DEF Definimos en $K[x] \times K[x]^* / R$ la ley de composición interna que llamaremos suma como

$$\forall \left[\frac{A}{B}\right], \left[\frac{C}{D}\right] \in K[x] x K[x]^* / R \qquad \left[\frac{A}{B}\right] + \left[\frac{C}{D}\right] = \left[\frac{A \cdot D + B \cdot C}{B \cdot D}\right]$$

La operación está bien definida.

• $AD + BC \in K[x]$ y $B \neq 0$, $D \neq 0 \Rightarrow BD \neq 0 \Rightarrow BD \in K[x]^*$

• No depende del representante elegido.

Si

$$\left[\frac{A}{B}\right] R \left[\frac{A'}{B'}\right] \quad y \quad \left[\frac{C}{D}\right] R \left[\frac{C'}{D'}\right] \Rightarrow \left[\frac{A}{B}\right] + \left[\frac{C}{D}\right] = \left[\frac{AD+BC}{BD}\right] \; y \; \left[\frac{A'}{B'}\right] + \left[\frac{C'}{D'}\right] = \left[\frac{A'D'+B'C'}{B'D'}\right]$$

Como $AB' = BA'$ y $CD' = DC'$

Multiplicando la 1ª igualdad por DD' $\qquad ADB'D' = BDA'D'$

Multiplicando la 2ª igualdad por BB' $\qquad BCB'D' = BDB'C'$

Sumando y sacando factor común queda

$B'D' (AD + BC) = BD (A'D' + B'C')$

Y equivale a

$$\left[\frac{AD+BC}{BD}\right] R \left[\frac{A'D'+B'C'}{B'D'}\right]$$

Luego la suma no depende del representante elegido.

PROP La suma definida en $K[x] \times K[x]^* / R$ verifica las propiedades

1) Asociativa
2) Conmutativa
3) Existencia de Elemento Neutro
4) Existencia de Elemento Simétrico.

Dem.

Inmediata.

El conjunto $(K[x] \times K[x]^* / R, +)$ tiene estructura de grupo conmutativo.

4.1.2. Producto de Razones Algebraicas.

DEF Definimos en $K[x] \times K[x]^* / R$ la ley de composición interna que llamaremos producto como

$$\forall \left[\frac{A}{B}\right], \left[\frac{C}{D}\right] \in K[x] x K[x]^* / R \qquad \left[\frac{A}{B}\right] \cdot \left[\frac{C}{D}\right] = \left[\frac{A \cdot C}{BD}\right]$$

La operación está bien definida

- A, C$\in$K[x] $\Rightarrow$ A$\cdot$ C$\in$K[x]

  B, D$\in$K[x]* $\Rightarrow$ B $\neq$ 0, D $\neq$ 0 $\Rightarrow$ BD $\neq$ 0 $\Rightarrow$ BD$\in$K[x]*

- No depende del representante elegido.

  $$\left[\frac{A}{B}\right]R\left[\frac{A'}{B'}\right] y \left[\frac{C}{D}\right]R\left[\frac{C'}{D'}\right] \Rightarrow AB' = A'B \ y\ CD' = C'D \Rightarrow$$

Multiplicando ambas igualdades ACB´D´ = A´C´BD $\Rightarrow$

$$\Rightarrow AC \cdot B'D' = A'C' \cdot BD \Rightarrow \left[\frac{AC}{BD}\right]R\left[\frac{A'C'}{B'D'}\right]$$

PROP El producto definido en K[x] x K[x]* / R verifica las siguientes propiedades:

1) Asociativa.
2) Conmutativa.
3) Existencia de Elemento Neutro.
4) Existencia de Elemento Neutro (si la razón es no nula).

Dem.

Inmediata.

El conjunto (K[x] x K[x]*, $\cdot$) tiene estructura de grupo conmutativo.

4.1.3. El Cuerpo de las Razones Algebraicas.

PROP En el conjunto K[x] x K[x]* / R se verifica la propiedad distributiva del producto respecto de la suma (por ambos lados).

Dem.

Inmediata.

El conjunto (K[x] x K[x]* /R, +, $\cdot$) tiene estructura de cuerpo conmutativo. Recibe el nombre de Cuerpo de las Razones Algebraicas, y se representa por K(x).

4.2. Descomposición en fracciones simples.

PROP Dado $\frac{A}{B} \in K(x)$ y P$\in$K[x] con P $\neq$ 0, se verifica que $\frac{A}{B} = \frac{AP}{BP}$.

Dem.

Inmediata.

COROLARIO Para cada $\frac{A}{B} \in K(x)$, existen dos únicos polinomios A´, b´∈K[x] tales que:

$$\frac{A}{B} = \frac{A´}{B´} \text{ con mcd (A´, B´) = 1 y B´ normalizado}$$

Dem.

• Existencia.

Sea D = mcd (A, B) ⇒ A = A´D y B = B´D con mcd (A´, B´) = 1

Trivialmente $\frac{A}{B} = \frac{A´}{B´}$

• Unicidad.

Si $\frac{A}{B} = \frac{A´´}{B´´}$ con mcd (A´´, B´´) = 1 y B´´ normalizado ⇒ A´B´´ = A´´B´ ⇒

⇒ A´ = A´´ y B´ = B´´

DEF Sea $\frac{A}{B} \in K(x)$ con mcd (A, B) = 1. Dicha razón algebraica recibe el nombre de fracción simple, o forma reducida.

PROP Todo elemento $\frac{A}{B}$ (fracción simple) de K(x) se puede escribir de forma única como

$$\frac{A}{B} = P + R$$

donde P∈K[x] y R es una fracción simple $\frac{A´}{B}$, con grad (A´) < grad (B) si R ≠ 0.

Dem.

• Existencia.

Sea $\frac{A}{B}$ una fracción simple.

Por la división enclidea ∃P, A´∈K[x] / A = B · P + A´ con grad (A´) < grad (B)

Entonces $\frac{A}{B} = P + \frac{A´}{B}$

Y como mcd (A, B) = mcd (B, A´) $\Rightarrow \dfrac{A'}{B}$ es una fracción simple.

- Unicidad.

Sea $\dfrac{A}{B} = P + R = Q + S$ con $Q \in K[x]$ y $S \in K[x]$ siendo $S = \dfrac{C}{D}$ fracción irreducible y grad (C) < grad (D). Si $S \neq 0$.

Entonces $P + \dfrac{A'}{B} = Q + \dfrac{C}{D}$

Y $P - Q = \dfrac{C}{D} - \dfrac{A'}{B} \Rightarrow P - Q = \dfrac{CB - A'D}{DB}$

En caso de que $P \neq Q \Rightarrow$ grad (CB – A´D) = grad ((P – Q) · DB)

Y grad ((P – Q) · DB) = grad (P – Q) + grad (D) + grad (B) ≥ grad (D) + grad (B)

Siendo grad (CB – A´D) ≥ grad (D) + grad (B) (1)

Por otro lado $\dfrac{CB - A'D}{DB}$ verifica grad (CB – A´D) < grad (DB) lo que es lo mismo que grad (CB – A´D) < grad (D) + grad (B) (2)

De (1) y (2) se deduce una contradicción, que viene de suponer $P \neq Q$.

Entonces P = Q y R = S.

DEF El polinomio P que nos da la proposición anterior se llama parte entera de $\dfrac{A}{B}$.

LEMA Sea $\dfrac{A}{B} \in K(x)$ con grad (A) < grad (B) sí $A \neq 0$. Sea $B = B_1 \cdot B_2$ con B_1 y B_2 primos entre sí. Entonces $\dfrac{A}{B}$ se descompone de forma única como

$$\frac{A}{B} = \frac{N_1}{B_1} + \frac{N_2}{B_2}$$

con grad (N_i) < grad (B_i) si $N_i \neq 0$ $\forall$i: 1, 2.

<u>Dem.</u>

- Existencia.

Como B_1 y B_2 son coprimos, $\exists P, Q \in K[x]$ tales que

$$1 = B_1P + B_2Q$$

Y entonces $A = AB_1P + AB_2Q$ (1)

Si dividimos AP entre B_2 (por ser $B_2 \neq 0$) tenemos $\exists C, N \in K[x]$ / $AP = B_2C + N_2$ con grad $(N_2) <$ grad (B_2) (2)

Al sustituir (2) en (1)

$$A = (B_2C + N_2)\, B_1 + AB_2Q$$

$$A = B_1B_2C + N_2B_1 + AB_2Q$$

$$A = (B_1C + AQ)\, B_2 + N_2B_1$$

Llamando $N_1 = B_1C + AQ$ queda $A = N_1B_2 + N_2B_1$ (3)

Si grad $(N_1) \geq$ grad (B_1) $\Rightarrow$ grad $(A) \geq$ grad (B_1) + grad (B_2), pues grad$(N_2) <$ grad (B_2) si $N_2 \neq 0$, lo que contradice la hipótesis.

Por tanto si $N_1 \neq 0$ grad $(N_1) \geq$ grad (B_1)

De la expresión (3) se deduce que $\dfrac{A}{B} = \dfrac{N_1}{B_1} + \dfrac{N_2}{B_2}$

- Unicidad.

Supongamos que $\dfrac{A}{B} = \dfrac{N_1}{B_1} + \dfrac{N_2}{B_2} = \dfrac{N_1´}{B_1} + \dfrac{N_2´}{B_2}$ con grad $(N_i´) <$ grad (B_i) si $N_i´ \neq 0$ $\forall i$:1, 2.

Entonces $\dfrac{N_1 - N_1´}{B_1} = \dfrac{N_2´ - N_2}{B_2}$

verificándose $B_2\, (N_1 - N_1´ = B_1\, (N_2´ - N_2)$

Y como B_1 y B_2 son coprimos, la igualdad sólo puede ser cierta si $N_1 = N_1´$ y $N_2´= N_2$.

LEMA Sea $\dfrac{A}{B} \in K(x)$ con grad (A) < grad (B) si $A \neq 0$. Sea $B = B_1 \cdot B_2 \cdot \ldots \cdot B_p$ con B_i y B_j coprimos $\forall i \neq j$. Entonces $\dfrac{A}{B}$ se descompone de modo único como

$$\frac{A}{B} = \frac{N_1}{B_1} + \ldots\ldots + \frac{N_p}{B_p}$$

con grad (N_i) < grad (B_i) si $N_i \neq 0$ $\forall$i: 1,…., p.

Dem.

Inmediata aplicando inducción.

LEMA Sea $\frac{A}{B^m} \in K(x)$ con grad (A) < grad (B^m) sí A $\neq$ 0. Entonces $\frac{A}{B^m}$ se descompone de forma única como

$$\frac{A}{B^m} = \frac{N_1}{B} + \frac{N_2}{B^2} + \ldots\ldots + \frac{N_m}{B^m}$$

siendo grad (N_i) < grad (B) si $N_i \neq 0$ $\forall$i: 1,…, m.

Dem.

Vamos a demostrar el lema mediante inducción en m. Para m = 1. Es evidente, siendo N_1 = A.

Supongamos cierto el lema cierta para m – 1.

Para m.

- Existencia.

Si realizamos la división enclidea de A entre B

$$\exists C, R \in K[x] \;/\; A = BC + R$$

con grad (R) < grad (B) si R $\neq$ 0.

Entonces $\frac{A}{B^n} = \frac{C}{B^{n-1}} + \frac{R}{B^n}$ (1)

Despejando $\frac{C}{B^{n-1}} = \frac{A-R}{B^n}$ y como grad (A) < grad (B^n) y grad (R) < grad (B^n), entonces grad (C) < grad (B^{n-1}) si C $\neq$ o.

Aplicamos a $\frac{C}{B^{n-1}}$ la hipótesis en inducción y sustituyendo en (1) obtenemos la descomposición pedida.

- Unicidad.

Supongamos que $\frac{A}{B^m} = \frac{N_1}{B} + ... + \frac{N_m}{B^m} = \frac{N_1´}{B} + ... + \frac{N_m´}{B^m}$ con grad ($N_i´$) < grad (B) si $N_i \neq 0$ $\forall$i: 1,…., m

Si multiplicamos por B^m la expresión anterior

$$N_m + BP = N_m´ + BQ$$

con P, Q$\in$K[x], verificándose

$$N_m – N_m´ = B(Q – P)$$

Y teniendo en cuenta las relaciones entre los grados, la igualdad anterior solo es cierta si $N_m - N_m´ = 0 \Rightarrow N_m = N_m´$ y $P = Q$

Aplicando ahora la hipótesis de inducción a $\frac{P}{B^{n-1}} = \frac{Q}{B^{n-1}}$ obtenemos $N_i = N_i´$ $\forall$i:1,…, m – 1.

TEOREMA. Teorema de Descomposición.

Sea $\frac{A}{B} \in K[x]$ fracción simple. Supongamos que E es la parte entera de $\frac{A}{B}$ y que $B = lB_1^{a_1} \cdot ...... \cdot B_s^{a_s}$ es su descomposición en factores primos con $\lambda \in$K. Entonces, la descomposición

$$\frac{A}{B} = E + \frac{N_{11}}{B_1} + ... + \frac{N_{1a_1}}{B^{a_1}} + \frac{N_{21}}{B_2} + ... + \frac{N_{2a_2}}{B_2^{a_2}} + ... + \frac{N_{S1}}{B_S} + ... + \frac{N_{Sa_S}}{B_S^{a_S}}$$

es única donde grad (N_{ij}) < grad (B_i) si $N_{ij} \neq 0$ $\forall$j: 1,…., α_i $\forall$i:1,…., s.

<u>Dem.</u>

Este resultado es una consecuencia inmediata de la última proposición y de los dos últimos lemas.

Bibliografía Recomendada.

Álgebra. Aut. Serge Lang. Ed. Aguilar.

Algèbre. Aut. S. MacLane, G. Birkhoff. Ed. Gauthier Villars.

Curso de Álgebra Moderna. Aut. Peter Hilton. Ed.Reverté.

Álgebra. Aut. Thomas W. Hungerford. Ed. Springer-Verlag.