TEMA 13: POLINOMIOS. OPERACIONES. FÓRMULA DE NEWTON. DIVISIBILIDAD DE POLINOMIOS. FRACCIONES ALGEBRAICAS.

TIEMPO: 91 — 88

Esquema

1) Introducción
   - 1.1) Antigüedad: Mesopotamia y Egipto
   - 1.2) Antigüedad: China
   - 1.3) Árabes
   - 1.4) ss.XVIII - XIX
   - 1.5) Gauss
   - 1.6) Posteriormente

2 Polinomios
   - 2.1) Construcción
   - 2.2) Def: pol. ctes., coeficientes, variable, monomio
   - 2.3) Def: grado + propiedades
   - 2.4) Teorema (división)
   - 2.5) Def: anillo euclídeo
   - 2.6) Fórmula de Newton

3) Divisibilidad
   - 3.1) Def 1 + propiedades
     - 3.1.1) Teorema (anillo $\mathbb{K}[x]$ principal)
   - 3.2) Def 2
     - 3.2.1) Proposición
   - 3.3) MCD
     - 3.3.1) Def + propiedades
     - 3.3.2) Teorema de Euclides
   - 3.4) MCM
     - 3.4.1) Def + propiedades
   - 3.5) Cálculo del MCD y el MCM
   - 3.6) Más propiedades

4) Más propiedades
   - 4.1) Def: raíz
   - 4.2) Principio de identidad
   - 4.3) Teorema de descomposición factorial
   - 4.4) Cuerpo de fracciones
     - 4.4.1) Teorema $\times$ 2

1) Introducción:

▷ Antigüedad (Mesopotamia y Egipto): ya hacia el año 2.000 a.C. tenemos tablillas de resolución de ecuaciones cuadráticas de manera equivalente al método actual general. El álgebra egipcia se centró casi exclusivamente en la resolución de ecuaciones lineales pero en Mesopotamia fueron más allá y resolvieron "satisfactoriamente" la ecuación de segundo grado normalizada: $x^2 + p \cdot x + q = 0$. Por "satisfactoriamente" queremos decir que aunque su nivel de abstracción y flexibilidad de los conceptos a los problemas era muy alto, ellos no tenían alfabeto (con lo que "$a \cdot x = b$" no significaba nada), tampoco tenían reparo en sumar un área y un volumen, necesitaban distinguir casos como $x^2 + p \cdot x = q$ y $x^2 + q = p \cdot x$ pues la fórmula general requiere del alfabeto y también resulta claro que todos los problemas eran situaciones reales que requerían una solución real (así pues "$x^2 + 1 = 0$" no les valía como ecuación).
Aparte de las ecuaciones de segundo grado resolvieron algunas ecuaciones cúbicas y del estilo "$x^4 + b \cdot x^2 + c = 0$" pues era de segundo grado "camufladas". Obsérvese que estamos hablando de personas que no tenían nuestro sistema de notación (aunque sí el principio posicional) y que vivieron hace más de 3.000 años.

▷ Antigüedad (China): la base práctica del último libro de la "La Matemática en Nueve Libros" (hacia el s.II a.C., es una recopilación de los logros de la matemática china hasta comienzos de nuestra era) la constituyen los problemas de determinación de distancias y alturas no accesibles con ayuda del Teorema de Pitágoras y las propiedades de los triángulos semejantes. Algunos problemas conducen a una ecuación cuadrática completa y su regla de resolución es equivalente a la actual. Para ecuaciones más complejas utilizaban un sistema llamado "método del elemento celeste" que es equivalente al método de Ruffini-Horner (s.XIX).

▷ Árabes: los matemáticos árabes acumularon muchos procedimientos de cálculo y algoritmos especiales. Por ejemplo:

a) Obtención de 17 cifras decimales exactas del número π mediante polígonos inscritos.

b) Cálculo del raíces por el método de Ruffini-Horner (técnica que aprendieron de los chinos) y cálculo de distintas raíces del tipo $\sqrt[n]{q}$.

c) Se dieron cuenta de que: $(a+b)^n = a^n + C_1^n a^{n-1} b + \ldots + C_{n-1}^n a b^{n-1} + C_n^n b^n$ y la relación $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$

▷ En Europa la tabla de coeficientes binomiales ($n \leq 17$) fue publicada en el siglo XVI (por Stiefel) y el método para calcular raíces sería superado en el s.XIX.

▷ ss.XVIII - XIX: durante estos siglos el problema fundamental del Álgebra lo constituía la resolución de ecuaciones algebraicas. Se descubrieron multitud de métodos y, a finales del s.XVIII, se vieron obligados a la introducción de nuevos conceptos como el de grupo o el de campo que terminarían revolucionando el Álgebra.
Los resultados correspondientes a polinomios son la Teorema de Abel-Galois que viene a decir que "dado un polinomio no tiene por qué ser resoluble (= fórmula explícita o algoritmo usando raíces y operaciones racionales) si su grado es mayor de 4" y el Teorema Fundamental del Álgebra: "todo polinomio con coeficientes complejos y de grado n tiene exactamente n raíces complejas (contando sus multiplicidades)".

▷ Gauss (1.777 - 1.855): hizo innumerables aportaciones a la Matemáticas pero relacionadas con el Álgebra podemos destacar:

a) Advirtió la relación entre la resolución de $x^n - 1 = 0$ y la división de la circunferencia en partes iguales con regla y compás. El resultado dice que la ecuación es resoluble para p primo si, y sólo si, $p = 2^{2^n} + 1$. Es decir, para $p = 3, 5, 17, 257, \ldots$ pero no para $p = 7, 11, 13, \ldots$.

b) Considerando la ecuación $\mathbb{X} = \frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \ldots + x + 1$, estableció que si $m = n - 1$ con n primo, $\mathbb{X} = 0$ es irreducible en el campo de los racionales y sus raíces tienen la forma $\alpha, \alpha^\beta, (\alpha^\beta)^\beta \ldots$ (es decir, un grupo cíclico).

c) Demostración del Teorema Fundamental del Álgebra: para ello parte de antemano que existe $\mathbb{C}$ y que toda ecuación con coeficientes reales tiene raíces en $\mathbb{C}$.

▷ Posteriormente: como la premisa sobre $\mathbb{C}$ no estaba muy clara (más el uso de herramientas del Análisis), no se admitió la prueba mundialmente hasta que el desarrollo de la teoría de campos fue lo suficiente como para dar validez a las suposiciones. Este hecho fue demostrado por Kronecker y el teorema dice: "el campo de cualquier polinomio es un subcampo de los números complejos o es isomorfo a este campo".
Galois, usando los resultados de Gauss y Lagrange, formuló su teoría sobre grupos, teoría que sería terminada por Abel en basándose en los trabajos de Galois. Como consecuencia de ellos se demuestra la imposibilidad de resolución algebraica de las ecuaciones de grado mayor de cuatro.

2) Polinomios:

▷ Empezaremos definiendo los polinomios para un anillo y después los extenderemos a un cuerpo.

▷ Sea $(A, +, \cdot)$ un anillo y consideremos $A^{\mathbb{N}} = \{(a_0, a_1, \ldots)\}$ el conjunto de todas las sucesiones de elementos de A. Se comprueba fácilmente que tiene estructura de A-módulo. Quedémonos con $A^{(N)}$, el conjunto de sucesiones que son nulas salvo un número finito de términos (a veces este espacio es denotado por C_{00}). Con la restricción de las operaciones de $A^{\mathbb{N}}$, se comprueba fácilmente que $(A^{(N)}, +, \text{operación externa})$ es un submódulo. Además tenemos una base formada por los vectores $\{e_j = (0, \ldots, \overbrace{1}^{j}, 0 \ldots)\}$ de $A^{(N)}$.
En $A^{(N)}$ podemos definir un producto interior, $a \cdot b = c \leftrightarrow c_k = \sum_{i+j=k} a_i \cdot b_j$ que le otorga a $(A^{(N)}, +, \cdot)$ estructura de anillo conmutativo y unitario.
Como la operación externa es $\alpha \times a = (\alpha \cdot a_0, \alpha \cdot a_1, \ldots)$, $\alpha \in A$, $a \in A^{(N)}$ y es compatible con el producto, tenemos que $(A^{(N)}, +, \cdot, \text{operación externa})$ es una A-álgebra unitaria y conmutativa.

▷ **Definición**: al conjunto $A^{(N)}$ se le conoce con el nombre de A-álgebra de los polinomios con una indeterminada con coeficientes en el anillo A. Lo notaremos por $A(x)$.

▷ $f : A \mapsto A(x)$, $\alpha \mapsto f(\alpha) = \times \cdot e_0 = (\alpha, \ldots)$ es un homomorfismo de A-álgebras. Entonces, a los elementos $\alpha \in A$ los vemos como polinomios constantes en $A(x)$.

▷ Llamando $e_0 \equiv 1$, $e_1 \equiv x, \ldots, e_n \equiv x^n$ podemos identificar $A^{(N)} \equiv A(x)$ y los elementos de $A^{(N)}$ los escribiremos de forma única como combinaciones lineales finitas de potencias de "x".

$$\forall a \in A(x), a = a_0 + a_1 \cdot x + \ldots + a_n \cdot x^n$$

▷ **Definición**: a los elementos $a_j \in A$ los llamamos coeficientes del polinomio.

▷ **Definición**: a la letra "x" la llamamos indeterminada o variable.

▷ **Definición**: llamamos monomio a los elementos de $A(x)$ donde $a_j = 0$, $\forall j$ menos para uno.

▷ **Definición**: llamaremos grado de un polinomio $a \in A(x)$ a la mayor potencia de la variable con coeficiente distinto de cero. Lo notaremos por "deg". En el caso de elemento neutro "**0**", por convenio tiene grado "$-\infty$" o no tiene (depende del texto).

▷ En nuestro caso, $deg : A(x) - \{0\} \mapsto \mathbb{N}$ es un homomorfismo de semigrupos donde se verifica que $deg(a \cdot b) = deg(a) + deg(b)$ (lo que nos demuestra que $A(x)$ no tiene divisores de cero. Además, siempre se cumple que $deg(a + b) \leq \text{máx}\{deg(a), deg(b)\}$.

▷ **Proposición**: $A(x)$ es un Dominio de Integridad.

▷ Vamos a pasar a tener $(\mathbb{K}, +, \cdot)$ un cuerpo conmutativo. Construyamos $\mathbb{K}(x)$ de la misma forma que se ha hecho con $A(x)$.

▷ **Teorema**: $\forall P(x), Q(x) \in \mathbb{K}(x)$ tal que $Q(x) \neq 0$, $\exists C(x), R(x)$ polinomios únicos en $\mathbb{K}(x)$ tales que $P(x) = Q(x) \cdot C(x) + R(x)$ con $deg(R(x)) < deg(Q(x))$ o $R(x) = 0$.

Proof. El algoritmo es el mismo que la para división de enteros y no ganamos nada demostrándolo. Nos detendremos en la unicidad:
Supongamos $P(x) = Q(x) \cdot C(x) + R(x) = Q(x) \cdot \hat{C}(x) + \hat{R}(x) \longrightarrow Q(x)(C(x) - \hat{C}(x)) = \hat{R}(x) - R(x)$.
Si $C(x) \neq \hat{C}(x) \longrightarrow \otimes = deg(Q(x) \cdot (C(x) - \hat{C}(x))) \geq deg(Q(x)) > deg(\hat{R}(x) - R(x)) = \odot$, lo que es un contradicción pues $\otimes = \odot \longrightarrow \hat{C}(x) = C(x) \longrightarrow \hat{R}(x) = R(x)$.

□

▷ **Definición**: decimos que un anillo unitario es euclídeo si existe una aplicación $g : A - \{0\} \mapsto \mathbb{N}$ cumpliendo:

a) Si $p|q \longrightarrow g(p) \leq g(p)$, $\forall p, q \in A - \{0\}$.

b) $\forall p, q \in A - \{0\}$, $\exists c, r \in A$ tales que $p = q \cdot c + r$ con $g(r) < g(q)$.

▷ **Corolario**: $\mathbb{K}(x)$ con la aplicación grado es un anillo euclídeo.

▷ **Fórmula de Newton**: dados $a, b \in \mathbb{K}$ (cuerpo), $1 \leq n \in \mathbb{N}$, entonces:

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j, \text{ donde } \binom{n}{m} = \frac{n!}{m!(n-m)!}$$

▷ Para polinomios no es más que cambiar una de las letras por la variable.

3) Divisibilidad:

▷ **Definición**: decimos que $P(x)$ divide a $Q(x)$ y lo notaremos por $P(x)|Q(x)$ cuando exista un polinomio $C(x)$ tal que $P(x) \cdot C(x) = Q(x)$.

▷ Esta es una relación de preorden (x^2 y $2x^2$ se dividen y son distintos), así que para hacerla de orden vamos a definir una relación de equivalencia.

▷ **Definición**: llamamos unidades de $(\mathbb{K}, +, \cdot)$ a todo elemento $a \in \mathbb{K} - \{0\}$.

▷ **Definición**: diremos que $P(x)$ y $Q(x)$ están asociados si $\exists a \in \mathbb{K} - \{0\}$ tal que $a \cdot P(x) = Q(x)$.

▷ **Definición**: tomando clases en los polinomios, diremos que $\overline{P(x)}$ divide a $\overline{Q(x)}$ y lo notaremos por $\overline{P(x)}|\overline{Q(x)}$ cuando existe un polinomio $\overline{C(x)}$ tal que $\overline{P(x)} \cdot \overline{C(X)} = \overline{Q(x)}$. Para no abusar de notación, no emplearemos las barras aunque se sobreentenderán.

▷ **Proposición**: la relación "|" ahora es una relación de orden.

▷ **Propiedades**:

1) $\forall a \in \mathbb{K}$, $a \neq 0$, $\forall P(x) \in \mathbb{K}(x) \longrightarrow a|P(x)$.

2) Si $P(x)|Q(x)$, $Q(x) \neq 0 \longrightarrow deg(P(x)) \leq deg(Q(x))$.

3) Si $P(x)|Q(x)$, $Q(x) \neq 0$ y $deg(P(x)) = deg(Q(x)) \longrightarrow P(x)$ está asociado con $Q(x)$.

4) Si $P(x)|Q(x)$ y $P(x)|\hat{Q}(x) \longrightarrow P(x)|(Q(x) \pm \hat{Q}(x))$.

5) Si $P(x)|Q(x) \longrightarrow P(x)|Q(x) \cdot \hat{Q}(x)$, $\forall \hat{Q}(x) \in \mathbb{K}(x)$.

6) Si $P(x)|Q(x) \longrightarrow P(x)|Q^n(x)$, $\forall n \in \mathbb{N}$.

▷ **Teorema**: todo ideal del anillo $\mathbb{K}(x)$ es un ideal principal. Esto es: $I =< P(x) >=< P >= (P)$.

Proof. Sea $I \neq 0$ un ideal de $\mathbb{K}(x)$. Veamos que está engendrado por un sólo elemento. Sea $P(x) \in I$ con el menor grado posible. Sea $P(x) \in I$ otro polinomio.
Entonces $Q(x) = C(x) \cdot P(x) + R(x)$ con $deg(R(x)) < deg(P(x))$ o bien $R(x) = 0$. Como I es ideal, $R(x) \in I \longrightarrow R(x) = 0$ (si no, contradeciría que $P(x)$ tiene grado mínimo) $\longrightarrow \forall Q(x) \in I$, $Q(x) = C(x) \cdot P(x) \longrightarrow I =< P(x) >=< P >= (P)$. □

▷ **Proposición**: $P(x)$, $Q(x) \in \mathbb{K}(x)$ son asociados $\longleftrightarrow (P) = (Q)$.

Proof. $\Longrightarrow$: si P y Q son asociados $\longrightarrow \exists a \in \mathbb{K}$ tq $P(x) = a \cdot Q(x) \longrightarrow (P) = (a \cdot Q) \longrightarrow (P) = (Q)$.
$\Longleftarrow$: si tenemos que $(P) = (Q) \longrightarrow P \in (Q)$, $Q \in (P) \longrightarrow P(x) = C(x)Q(x)$, $Q(x) = \hat{C}(x)P(x) \longrightarrow P(x) = P(x)C(x)\hat{C}(x) \longrightarrow C(x)\hat{C}(x) = 1 \longrightarrow$ son unidades de $\mathbb{K} \longrightarrow P$ y Q son asociados.

□

▷ **Definición**: dados $P(x)$, $Q(x) \in \mathbb{K}(x)$ no nulos, decimos que $P(x)$ divide a $Q(x)$ cuando tenemos que $(Q) \subset (P)$.

▷ **Proposición**: ambas definiciones son equivalentes.

Proof. Si $P(x)|Q(x) \longrightarrow \exists C(x) \in \mathbb{K}(x)$ tq $Q(x) = C(x) \cdot P(x) \longrightarrow Q(x) \in (P) \longrightarrow (Q) \subset (P)$.
Si $(Q) \subset (P) \longrightarrow Q(x) \in (P) \longrightarrow Q(x) = P(x) \cdot C(x) \longrightarrow P(x)|Q(x)$.

□

▷ **Definición**: dados $A(x)$, $B(x) \in \mathbb{K}(x)$ llamamos ideal máximo común divisor de $A(x)$ y $B(x)$ al ideal $(D) = (A) + (B)$.

▷ **Definición**: llamamos máximo común divisor de los polinomios $A(x)$ y $B(x)$ a la base del ideal $(A) + (B)$. Lo notaremos por m.c.d$(A(x), B(x)) = D(x)$.

▷ **Proposición**: el m.c.d. de $A(x)$ y $B(x)$ cumple que es divisor de $A(x)$ y $B(x)$.

Proof. Como $(D) = (A) + (B) \longrightarrow (A) \subset (D)$, $(B) \subset (D) \longrightarrow D(x)|A(x)$ y $D(x)|B(x)$

□

▷ **Proposición**: cualquier divisor de $A(x)$ y $B(x)$ es divisor del m.c.d. de ambos.

Proof. Sea $\hat{D}(x)$ tq $\hat{D}(x)|A(x)$, $B(x) \longrightarrow (A) \subset (\hat{D})$, $(B) \subset (\hat{D}) \longrightarrow (D) = (A) + (B) \subset (\hat{D}) \longrightarrow \hat{D}(x)|D(x)$

□

▷ **Definición**: de la relación $(D) = (A) + (B)$ se sigue que $\exists \lambda(x)$, $\mu(x) \in \mathbb{K}(x)$ tales que se cumple:
$D(x) = \lambda(x) \cdot A(x) + \mu(x) \cdot B(x)$. Es es la llamada relación de Bezout.

▷ **Propiedades**:

1) Si $A(x), B(x) \neq 0$ y $\hat{D}(x)$ los divide $\longrightarrow deg(\hat{D}(x)) \leq deg(D(x))$.

2) Si $D(x) =$ m.c.d.$(A(x), B(x)) \longrightarrow D(x) \cdot C(x) =$ m.c.d.$(A(x) \cdot C(x), B(x) \cdot C(x))$

3) Si $D(x) =$ m.c.d.$(A(x), B(x)) \longrightarrow 1 =$ m.c.d.$(A(x)/D(x), B(x)/D(x))$

4) Si $A(x)|B(x) \longrightarrow A(x) =$ m.c.d.$(A(x), B(x))$

▷ **Definición**: diremos que dos polinomios son primos entre sí si m.c.d.$(A(x), B(x)) = a \in \mathbb{K}$. En este caso, $(D) = (1)$ y tenemos que $1 = \lambda(x) \cdot A(x) + \mu(x) \cdot B(x)$

▷ **Proposición**: $A(x), B(x)$ primos entre sí $\longleftrightarrow \exists \lambda(x), \mu(x)$ tq $1 = \lambda(x) \cdot A(x) + \mu(x) \cdot B(x)$.

▷ **Teorema de Euclides**: si $A(x)|B(x) \cdot C(x)$ y m.c.d.$(A(x), B(x)) = 1 \longrightarrow A(x)|C(x)$

Proof. Por la identidad de Bezout: $1 = \lambda(x)A(x)+\mu(x)B(x) \longrightarrow C(x) = \lambda(x)A(x)C(x)+\mu(x)B(x)C(x)$ y $A(x)$ divide a cada sumando $\longrightarrow A(x)|C(x)$.

□

▷ **Definición**: dados $A(x)$, $B(x) \in \mathbb{K}(x)$ llamamos ideal mínimo común múltiplo de $A(x)$ y $B(x)$ al ideal $(M) = (A) \cap (B)$

▷ **Definición**: llamamos mínimo común múltiplo de los polinomios $A(x)$ y $B(x)$ a la base del ideal $(A) \cap (B)$. Lo notaremos por m.c.m$(A(x), B(x)) = M(x)$

▷ **Proposición**: m.c.m.$(A(x), B(x)) = M(x)$ es múltiplo de $A(x)$ y $B(x)$.

Proof. $(M) = (A) \cap (B) \longrightarrow (M) \subset (A)$, $(M) \subset (B) \longrightarrow A(x)|M(x)$ y $B(x)|M(x)$

□

▷ **Proposición**: cualquier múltiplo de $A(x)$ y $B(x)$ es múltiplo de $M(x)$.

Proof. Sea $\hat{M}(x)$ tq $A(x)|\hat{M}(x)$ y $B(x)|\hat{M}(x) \longrightarrow (\hat{M}) \subset (A)$, $(B) \longrightarrow (\hat{M}) \subset (A) \cap (B) = (M) \longrightarrow M(x)|\hat{M}(x)$

□

▷ **Propiedades**:

1) Si $A(x)$, $B(x) \neq 0$ y $\hat{M}(x)$ es múltiplo común $\longrightarrow deg(M(x)) \leq deg(\hat{M}(x))$.
2) Si m.c.m.$(A(x), B(x)) = M(x) \longrightarrow$ m.c.m.$(A(x)C(x), B(x)C(x)) = M(x)C(x)$.
3) Si m.c.m.$(A(x), B(x)) = M(x) \longrightarrow$ m.c.d.$(M(x)/A(x), M(x)/B(x)) = 1$.
4) Si $A(x)|B(x) \longleftrightarrow$ m.c.m.$(A(x), B(x)) = B(x)$.
5) Si m.c.m.$(A(x), B(x)) = M(x)$ y $C(x)|A(x), B(x) \longrightarrow$ m.c.m.$(A(x)/C(x), B(x)/C(x)) = M(x)/C(x)$

▷ Como $(\mathbb{K}(x), \cup, \cap)$ es un retículo distribuido $\longrightarrow (\mathbb{K}(x)$, n.c.d., m.c.m.) también lo es.

▷ Cómo hallar el m.c.d. de dos polinomios y, a partir de él, su m.c.m. Empecemos con el máximo común divisor:
m.c.d.$(A(x), B(x)) =$ m.c.d.$(B(x), R_1(x)) =$ m.c.d.$(R_1(x), R_2(x)) = \ldots =$ m.c.d.$(R_n(x), 0) = R_n(x)$, que es el algoritmo de Euclides para polinomios.

Proof. $A(x) = B(x)C_1(x) + R_1(x)$ con $deg(R_1(x)) < deg(B(x)) \longrightarrow B(x) = R_1(x)C_2(x) + R_2(x)$ con $deg(R_2(x)) < deg(R_1(x)) \longrightarrow \ldots$ y como tenemos grado finito $\longrightarrow$ lo podemos realizar en un número finito de pasos. La igualdad final viene de que $R(x) = A(x) - B(x)C(x)$, con lo que el m.c.d. dividirá también a $R(x)$ y, por lo tanto, m.c.d.$(A(x), B(x))$ = m.c.d.$(B(x), R(x))$.

□

▷ **Teorema**: $A(x) \cdot B(x)$ = m.c.d.$(A(x), B(x))\cdot$ m.c.m.$(A(x), B(x))$.

▷ **Corolario**: dos polinomios serán primos entre sí $\longleftrightarrow$ su m.c.m. vale el producto de ambos.

▷ **Definición**: sea $A(x) \in \mathbb{K}(x)$ con $deg(A(x)) > 0$. Decimos que es primo o irreducible si no es divisible por otro $B(x) \in \mathbb{K}(x)$ tal que $0 < deg(B(x)) < deg(A(x))$.

▷ *Nota*: la coincidencia entre primo e irreducible no es cierta siempre.

▷ **Proposición**: en un anillo principal (como $\mathbb{Z}$ o el anillo de los polinomios) se cumple que P es primo e irreducible $\longleftrightarrow$ (P) es un ideal maximal. En nuestro caso: $A(x)$ es primo $\longleftrightarrow$ (A) es maximal.

4) Más propiedades:

▷ Sea un polinomio $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ construido sobre un anillo A o un cuerpo $\mathbb{K}$. Entonces:

▷ **Definición**: llamamos valor numérico de $P(x)$ para $X = \alpha$ ($\alpha \in A$, $\alpha \in \mathbb{K}$) al valor:

$$P(\alpha) = a_0 + a_1\alpha + \ldots a_n\alpha^n$$

▷ **Definición**: decimos que "α" es una raíz del polinomio si $P(\alpha) = 0$.

▷ **Teorema**: sea $(\mathbb{K}, +, \cdot)$ un cuerpo conmutativo y $P(x) = a_0 + \ldots a_nx^n$ un elemento de $\mathbb{K}(x)$. Si $P(x)$ se anula para más de "n" valores $\longrightarrow P(x)$ es el polinomio nulo.

Proof. Sean $\alpha_j.j = 1, \ldots, n+1$ tales que $a_0 + \ldots + \alpha_j^n a_n$, $\forall j = 1, \ldots, n+1$. Supongamos que no todos los a_j son nulos.
Llamemos $H = \begin{pmatrix} 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_{n+1} \\ \alpha_1^2 & \ldots & \alpha_{n+1}^2 \\ \vdots & \vdots & \vdots \\ \alpha_1^n & \ldots & \alpha_{n+1}^n \end{pmatrix}$ que es una matriz cuadrada de orden $(n+1)$.
Podemos escribir $(a_0, \ldots, a_n)H = (0, \ldots, 0)$ (por definición de α_j)$\longrightarrow \det(H) = 0$, pero es sabido que $\det(H) = \prod_{i<j}(\alpha_j - \alpha_j) \neq 0 \longrightarrow j < n+1 \longrightarrow$ si $deg(P(x)) = n$ hay, a lo sumo, "n" raíces.

□

▷ **Corolario** (principio de identidad para polinomios): sean $P(x), Q(x) \in \mathbb{K}(x)$ no nulos y con grados "p" y "q" respectivamente. Si $P(x) = Q(x)$ en máx$\{p, q\}+1$ puntos distintos $\longrightarrow P(x) = Q(x)$.

Proof. Consideramos $R(x) = P(x) - Q(x)$ y aplicamos el teorema anterior.

□

▷ Dado $P(x) \in \mathbb{K}(x)$, el resto de la división de $P(x)$ entre $(x - \alpha)$ es el valor numérico de dicho polinomio en $x = \alpha$. Se demuestra mediante la división euclídea que:
$P(x) = (x - \alpha)C(x) + R(x)$ con $deg(R(x))) = 0$ o bien con $R(x) = 0$.

▷ **Teorema**: dado $P(x) \in \mathbb{K}(x)$ con una raíz $\alpha \in \mathbb{K}$. Eso es equivalente a que $(x - \alpha)|P(x)$.

Proof. $\Longrightarrow$: si "α" es raíz $\longrightarrow P(\alpha) = 0 \longrightarrow$ {Teorema del Resto} $\longrightarrow P(x) = (x - \alpha)C(x) \longrightarrow (x - \alpha)|P(x)$
$\Longleftarrow$: si $(x - \alpha)|P(x) \longrightarrow P(x) = (x - \alpha)C(x)$ con $C(x) \in \mathbb{K}(x)$; $P(\alpha) = 0 \cdot C(x) \longrightarrow \alpha$ es raíz. □

▷ **Teorema (de descomposición factorial)**: sea $P(x) \in \mathbb{K}(x)$, $P(x) = a_0 + \ldots + a_n x^n$ teniendo $\alpha_1, \ldots, \alpha_m (m \leq n)$ raíces. Entonces $P(x) = (x - \alpha_1) \cdots (x - \alpha_m) \cdot Q(x)$ con $deg(Q(x)) = n - m$.

Proof. Aplicar "m" veces el teorema anterior.

□

▷ Lo anterior nos dice que podemos descomponer cualquier polinomio en producto de polinomios irreducibles o primos de manera única. Es decir, $\mathbb{K}(x)$ es un anillo factorial.

▷ Podemos construir el cuerpo de fracciones de $\mathbb{K}(x)$, $[\mathbb{K}(x)]$ como hacemos con los números. Usando que $\mathbb{K}(x)$ es un anillo factorial y, además, euclídeo, obtenemos que:

▷ **Teorema**: sean $P(x), Q(x) \in \mathbb{K}(x)$ no nulos y primos entre sí. Entonces podemos escribir $\dfrac{\lambda(x)}{Q(x)} + \dfrac{\mu(x)}{P(x)} = \dfrac{1}{P(x)Q(x)}$

Proof. Como es un anillo euclídeo y m.c.d.$(P(x), Q(x)) = 1$, aplicamos la relación de Bezout para obtener $\lambda(x), \mu(x)$ / $\lambda(x)P(x) + \mu(x)Q(x) = 1$. De ahí obtenemos que $\dfrac{\lambda(x)}{Q(x)} + \dfrac{\mu(x)}{P(x)} = \dfrac{1}{P(x)Q(x)}$

□

▷ **Teorema**: dado $\dfrac{P(x)}{Q(x)} \in [\mathbb{K}(x)]$, e puede descomponer de forma única como $C(x) + \dfrac{R(x)}{Q(x)}$ con $deg(R(x)) < deg(Q(x))$ o $R(x) = 0$

Proof. Existencia: por el algoritmo de Euclides: $\dfrac{P(x)}{Q(x)} = C(x) + \dfrac{R(x)}{Q(x)}$ con $deg(R(x)) < deg(Q(x))$.

Unicidad: $C(x) + \dfrac{R(x)}{Q(x)} = \hat{C}(x) + \dfrac{\hat{R}(x)}{Q(x)} \longleftrightarrow (C(x) - \hat{C}(x))Q(x) = \hat{R}(x) - R(x)$, pero tenemos que $deg(\hat{R}(x) - R(x)) < deg(Q(x)) \longrightarrow \hat{C}(x) = C(x)$ y $\hat{R}(x) = R(x)$. □