UNA INTRODUCCIÓN AL ÁLGEBRA DE POLINOMIOS

Dr. Jean Carlos Liendo (UCV)

¿Qué significa la palabra álgebra?

La etimología de la palabra álgebra se conoce como el arte que consiste en armar huesos que estaban dislocados o quebrados.

Un algebrista es un armador de estructuras óseas.

En la actualidad el álgebra es el área de la matemática que se centra en el estudio de las estructuras.

Estructura

Es igual a

Un conjunto con operaciones:
suma, producto, división, composición,
Substitución, unión, intersección,…

Que satisfacen propiedades

Asociatividad, conmutatividad,
Distributividad,…

Formuladas usando

Variables: a, b, c, f, g,…

El estudio de las expresiones formadas por <u>*sumas finitas de productos finitos de variables*</u> es el origen de lo que se conoce como álgebra.

$$3x^2 + 4x^3 + \boxed{7x^5} + 6x + 3$$

Monomio

Polinomios

Muchos **Regla, distribución**

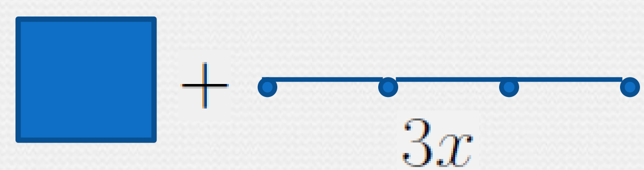
¿Porqué estas expresiones?

¿Cuál es el número que multiplicado por a es b?

$$ax = b$$

¿Cuál es el área del cuadrado tal que sumado a tres veces la longitud de su lado es igual a ocho?

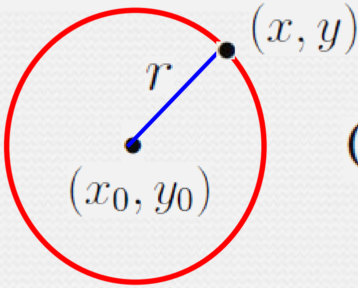
$$x^2 + 3x = 8$$

x^2  $= 8$

En general $ax^2 + bx + c = 0$

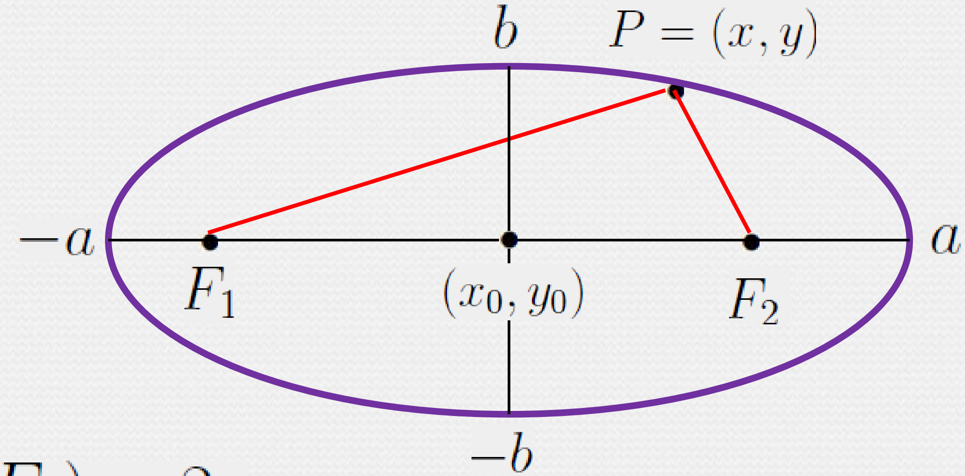
parábolas, movimientos parabólicos

$$(x - x_0)^2 + (y - y_0)^2 = r^2$$



Circunferencia

$$\frac{(x - x_0)^2}{a^2} + \frac{(y - y_0)^2}{b^2} = 1$$

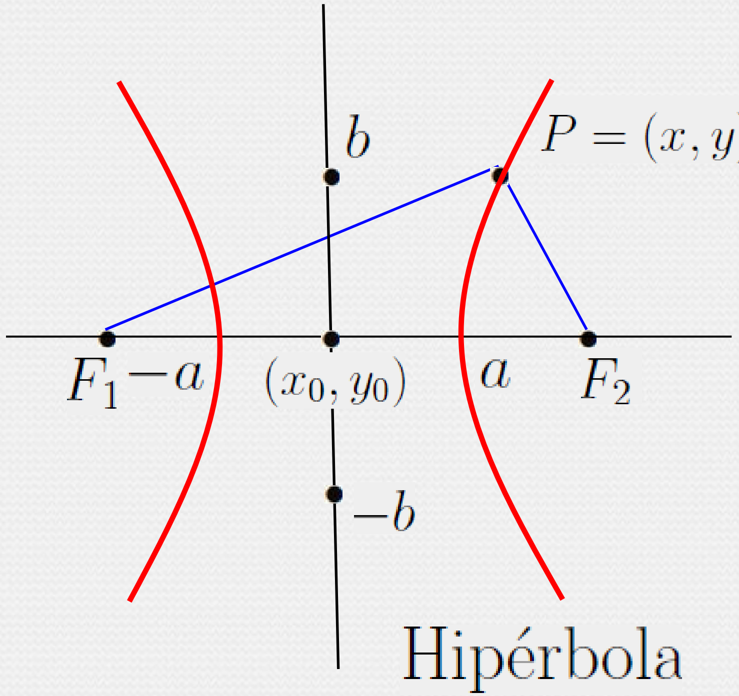


$$d(P, F_1) + d(P, F_2) = 2a$$

Elipse

$$\frac{(x-x_0)^2}{a^2} - \frac{(y-y_0)^2}{b^2} = 1$$

$$|d(P,F_1) - d(P,F_2)| = 2a$$



En la construcción de números tenemos

- $\mathbb{Z}$ es una extensión de $\mathbb{N}$

$$x+n=0, \forall n \in \mathbb{N}$$

$$x=-n, \text{ opuesto aditivo}$$

- $\mathbb{Q}$ es una extensión de $\mathbb{Z}$

$$bx - a = 0, \forall b \in \mathbb{Z} - \{0\}, a \in \mathbb{Z}$$
$$x = \frac{a}{b}, \text{ fracción}$$

- Al resolver la ecuación $x^n = q$ para cada número natural $n \geq 2$, $q \in \mathbb{Q}^+$, tenemos extensiones de $\mathbb{Q}$ por adjunción de radicales $(\sqrt{2}, \sqrt[3]{5}, \sqrt[5]{\frac{7}{3}}, \ldots)$,

$$\vdots$$

$$\boxed{\text{AXIOMA DE COMPLETITUD}}$$

$\mathbb{R}$ Números reales

- Al resolver la ecuación $x^2 + 1 = 0$

$$x = i,\ i^2 = -1 \quad \mathbb{C} = \{a + ib/a, b \in \mathbb{R}\}$$

TEOREMA FUNDAMENTAL DEL ÁLGEBRA

Las soluciones de cualquier ecuación polinomial, son números complejos

$\mathbb{C}$ es el conjunto de números más usado por sus aplicaciones en: Mecánica cuántica, Ingeniería, Electrónica y las telecomunicaciones.

$$\boxed{e^{i\theta} = cos(\theta) + isen(\theta), \text{ Formula de Euler}}$$

Álgebra de Polinomios en una Variable

$\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, Un *polinomio* con coeficientes en $\mathbb{K}$ es una función $P : \mathbb{N} \longrightarrow \mathbb{K}$ que cumple con la condición

$$\{n \in \mathbb{N}/P(n) \neq 0\} \text{ es finito.}$$

$P(n) = p_n$, entonces $P = (p_0, p_1, p_2, p_3, ...)$

p_n es el *coeficiente n-ésimo* de P.

x variable o incógnita

$k = max\{n \in \mathbb{N} / p_n \neq 0\}$, entonces escribimos

$$P(x) := p_0 + p_1 x + p_2 x^2 + \cdots + p_k x^k \quad \sim (p_0, p_1, ...)$$

$P(x) = Q(x)$ si son iguales como funciones, $p_n = q_n, \forall n \in \mathbb{N}$,

k se denomina el *grado* de $P(x)$, se denota por $grad(P)$

$\mathbb{K}[x]$ denotará al conjunto formado por todos los polinomios con coeficientes sobre $\mathbb{K}$.

Operaciones

Suma

La suma en $\mathbb{K}[x]$ es la suma punto a punto de funciones:

$$(P+Q)_n = p_n + q_n$$

suma coeficiente a coeficiente

$$(3x^2 + 8x^5 + 3) + (2x + 5x^2 + 4x^5 + 2) = 12x^5 + 8x^2 + 2x + 5$$

Producto

$$x^n . x^m = x^{n+m}$$

$$(P.Q)_n = \sum_{k=0}^{n} p_k q_{n-k}$$

Producto de Cauchy

$$(3x^2+1-4x)(x^2+2) = 3x^4+6x^2+x^2+2-4x^3-8x$$
$$= 3x^4-4x^3+7x^2-8x+2$$

Propiedades

1. $P(x)+Q(x)=Q(x)+P(x)$
2. $(P(x)+Q(x))+R(x)=P(x)+(P(x)+Q(x))$
3. $P(x)+0=P(x)$
4. $(P(x)+(-P(x))=0$
5. $P(x).Q(x)=Q(x).P(x)$

$(\mathbb{K}[x],+)$ es un grupo abeliano

6. $(P(x).Q(x)).R(x)=P(x).(Q(x).R(x))$
7. $P(x)\cdot 1=P(x)$
8. $(\lambda P(x).Q(x))=P(x).(\lambda Q(x))=\lambda(P(x).Q(x)), \forall\lambda\in\mathbb{K}$
9. $P(x).(Q(x))+R(x))=P(x).Q(x)+P(x).R(x)$

$\boxed{(\mathbb{K}[x],\ +,\ .)\text{ es un álgebra conmutativa.}}$

Si $P(x)Q(x) = 0$, entonces $P(x) = 0$ o $Q(x) = 0$.

La función grado $grad : \mathbb{K} - \{0\} \longrightarrow \mathbb{N}$ satisface

$$grad(P(x)Q(x)) = grad(P(x)) + grad(Q(x))$$

Haciendo inducción sobre esta función tenemos

$\boxed{\text{Teorema de la División}}$

Sean $P(x)$ y $D(x) \neq 0$ polinomios, existen polinomios $Q(x)$ y $R(x)$ tales que

$$P(x) = D(x)Q(x) + R(x)$$

$R(x) = 0$ *o* $grad(R(x)) < grad(Q(x))$

cuando $R(x) = 0$, *decimos que* $D(x)/P(x)$

$P(x)$ Dividendo

$$
\begin{array}{l|l}
\cancel{3x^4} + 8x^3 - \frac{1}{2}x^2 + 3x - 2 & x^2 + x - 1 \\
\cline{2-2}
-(\cancel{3x^4} + 3x^3 - 3x^2) & 3x^2 + 5x - \frac{5}{2} \\
\cline{1-1}
\cancel{5x^3} + \frac{5}{2}x^2 + 3x - 2 & \\
-(\cancel{5x^3} + 5x^2 - 5x) & \\
\hline
\cancel{-\frac{5}{2}x^2} + 8x - 2 & \\
-(\cancel{-\frac{5}{2}x^2} - \frac{5}{2}x + \frac{5}{2}) & \\
\hline
\frac{21}{2}x - \frac{9}{2} &
\end{array}
$$

$D(x)$ Divisor

$Q(x)$ Cociente

$$P(x) = D(x)Q(x) + R(x)$$

$R(x)$ Resto o residuo

$(\mathbb{K}[x], +, .)$ junto a TEOREMA DE LA DIVISIÓN = *Anillo Euclidiano*

IDEALES

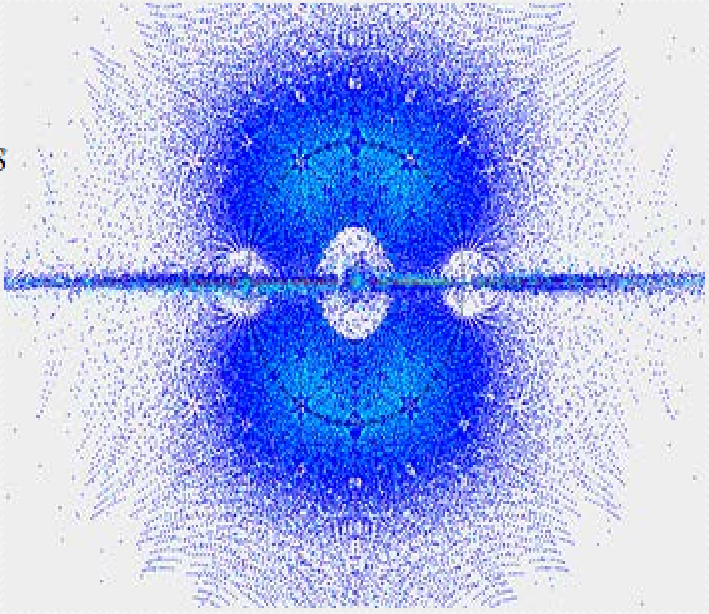
La teoría de ideales es reciente, fue creada por el matemático aleman Richard Dedekind, a fines del siglo XIX, en la época la comunidad matemática estaba interesada en

LOS NÚMEROS ALGEBRAICOS = solución de una ecuación polinomial con coeficientes enteros

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

Generalización de la divisibilidad en $\mathbb{Z}$

- Descomposición en factores primos
- Determinación de raíces



Ideal se refiere a los números ideales que factorizan a otros números.

$$i.i = -1 \qquad \begin{cases} 2 = a.b \quad 3 = c.d \quad 1 + i\sqrt{5} = a.c \\ 1 - \sqrt{5}i = b.d \quad 6 = a.b.c.d \end{cases}$$

En Geometría el concepto de ideal permitió el estudio de las curvas como soluciones de sistemas de ecuaciones polinomiales. $\boxed{Variedad\ afín}$

Teorema de los ceros de Hilbert establece un puente de conexión entre

Variedades (Curvas)
objeto geométrico
ceros del conjunto
de polinomios

ideales
objeto algebraico
conjunto de polinomios

$\boxed{\text{Geometría algebraica.}}$

Emmy Noether mujer alemana nacida en 1882 de origen judio
Conocida por sus grandes contribuciones en la física teórica,
álgebra abstracta, pionera en lo que hoy se conoce como
álgebra moderna.

Según David Hilbert y Albert Eintein:

La mujer más importante de la historia de la matemática

No fue reconocida en los inicios de su carrera y su fama llega de la mano del propio Hilbert, fue muy generosa en contribuciones académicas con muchos de sus colegas, entre ellos el propio Hilbert y el matemático B.L. Van der Waerden.

Entre (1920-1926) Noether realizó los trabajos que cambiaron la dinámica de estudio en el álgebra abstracta en su articulo *La teoría de ideales en anillos*.

el concepto de ideal se convierte en una herramienta importante con numerosas aplicaciones. Noether efectuó el uso de cadena ascendente y los objetos que las satisfacen se denominan Noetherianos en su honor.

En el álgebra moderna el concepto de *ideal* se entiende como el núcleo o kernel de funciones que preservan operaciones (Suma, Producto, ...) *Homomorfismos* y miden que tan inyectiva es una función.

Ideal

soluciones de sistemas de ecuaciones — contexto antiguo

ceros de homomorfismos nivel de inyectividad — contexto moderno

Los ideales permiten la creación de estructuras mas reducidas a través de cocientes (*Relaciones de equivalencia*), estas estructuras reducidas se entienden a través de *generadores y relaciones* definidas por un ideal. La construcción es universal.

En $\mathbb{K}[x]$ un ideal I, es un subconjunto no vacío de polinomios que satisface

1. $P(x) + Q(x) \in I, \forall P(x), Q(x) \in I$

2. $P(x)Q(x) \in I, \forall P(x) \in \mathbb{K}[x], \forall Q(x) \in I$

ideales en $\mathbb{K}[x]$:

$\{0\}, \mathbb{K}[x], \{(x^3+1)Q(x) \,:\, Q(x) \in \mathbb{K}[x]\} = (x^3+1)$

A una matriz cuadrada, $\{P(x) \in \mathbb{K}[x] : P(A) = 0\}$

Teorema

$\mathbb{K}[x]$ es un dominio de ideales principales. Es decir, para todo ideal I de $\mathbb{K}[x]$, existe un polinomio $P(x)$ tal que

$$I = (P(x)) = \{P(x)Q(x) : Q(x) \in \mathbb{K}[x]\}$$

Además $P(x)$ es único salvo múltiplo escalar.

La demostración se sigue del hecho de que $\{grad(H(x)) : H(x) \in I\}$ tiene un elemento mínimo.

$P(x)$ es uno de los polinomios de I con grado mínimo.

Aplicaciones del Concepto Ideal

1. Máximo Común Divisor. Si P y G son polinomios no ambos nulos, el máximo común divisor de P y Q es el polinomio D tal que

- $D \mid P$ y $D \mid G$
- Si $H \mid P$ y $H \mid G$, entonces $H \mid D$

Más aún $\langle P, Q \rangle = \{W_1 P + W_2 G : W_1, W_2 \in \mathbb{K}[x]\} = (D)$

Generalización
Lema de Bezout
ecuaciones Diofánticas

Existen polinomios W_1 *y* W_2 *tales que* $W_1 P + W_2 G = D$

Se pueden encontrar W_1 *y* W_2 usando

el *Algoritmo de la División de Euclides*

Despeje de restos para obtener $W_1 \quad W_2$

$$P = Q_0 G + R_1 \quad grad(R_1) < grad(G)$$

$$G = Q_1 R_1 + R_2 \quad grad(R_2) < grad(R_1)$$

$$R_1 = Q_2 R_2 + R_3 \quad grad(R_3) < grad(R_2)$$

$$\vdots$$

$$R_{n-2} = Q_{n-1} R_{n-1} + R_n \quad grad(R_n) < grad(R_{n-1})$$

$$R_{n-1} = Q_n R_n$$

División sucesiva de restos

máximo común divisor de P y Q

$$W_1 P + W_2 G = R_n = D$$

2. Álgebra Residual de Polinomios.

Útil para construir otras estructuras. similar a $\mathbb{Z}_n$

$$(P) = I = \{PQ : Q \in \mathbb{K}[x]\} \text{ ideal de } \mathbb{K}[x].$$

$$G_1 \sim G_2 \Longleftrightarrow G_1 - G_2 \in I \Longleftrightarrow G_1 - G_2 = PQ \Longleftrightarrow G_1 = G_2 + PQ$$

es una relación de equivalencia.

$$\overline{G_2} = \{G_1 \in \mathbb{K}[x] : G_1 \sim G_2\} = \{G_2 + PQ : Q \in \mathbb{K}[x]\} = G_2 + I$$

$$\mathbb{K}[x]/\!\sim\; = \mathbb{K}[x]/(P) = \{G + I : G \in \mathbb{K}[x]\}$$

$\boxed{\text{Operaciones:}}$

Suma: $(G_1 + I) + (G_2 + I) = (G_1 + G_2) + I$

Producto: $(G_1 + I).(G_2 + I) = (G_1 G_2) + I$

$\forall \lambda \in \mathbb{K},\ \lambda(G + I) = (\lambda + I)(G + I) = \lambda G + I$

Están bien definidas debido al concepto de ideal

I es el neutro de la suma

$1 + I$ es el neutro del producto

¿Por qué Residual?

$$G(x) = P(x)Q(x) + R(x)$$

$$\begin{aligned} G(x) + I &= (P(x)Q(x) + R(x)) + I \\ &= (P(x)Q(x) + I) + (R(x) + I) \\ &= I + (R(x) + I) \\ &= R(x) + I \end{aligned}$$

$grad(R(x)) < grad(P(x)) = n$, entonces $R(x) = a_0 + a_1 x + a_2 x^3 + \cdots a_{n-1} x^{n-1}$

$$\begin{aligned} R(x) + I &= (a_0 + a_1 x + a_2 x^2 + \cdots a_{n-1} x^{n-1}) + I \\ &= a_0(1 + I) + a_1(x + I) + a_2(x + I)^2 + \cdots + a_{n-1}(x + I)^{n-1} \\ &= R(x + I) = R(t) \end{aligned}$$

$$\boxed{t = x + I}$$

Finalmente

$$G(x) + I = R(x) + I = R(t)$$

$$\mathbb{K}[x]/(P) = \{a_0 + a_1 t + \cdots a_{n-1} t^{n-1} : a_i \in \mathbb{K}, P(t) = 0\} = \langle 1, t, t^2, \ldots, t^{n-1} : P(t) = 0 \rangle$$

Generadores

Relación

Ejemplos

Números Complejos

$$\mathbb{R}[x]/(x^2+1) = \{a_0 + a_1 t : a_0, a_1 \in \mathbb{R}, t^2+1=0\}$$

$$\boxed{\overline{x} = x + (x^2+1) = t = i}$$

$$= \{a_0 + a_1 t : a_0, a_1 \in \mathbb{R}, t^2 = -1\}$$

$$= \{a_0 + a_1 i : a_0, a_1 \in \mathbb{R}, i^2 = -1\} = \mathbb{C}$$

La adjunción de $\sqrt{2}$ a $\mathbb{Q}$

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2) = \{a_0 + a_1 t : a_0, a_1 \in \mathbb{Q}, t^2 - 2 = 0\}$$

$$= \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\} \quad \boxed{\overline{x} = x + (x^2-2) = t = \sqrt{2}}$$

$$(a_0 + a_1\sqrt{2})(a_0 - a_1\sqrt{2}) = a_0^2 - 2a_1^2, \quad a_0, a_1 \neq 0$$

$\boxed{\text{conjugado}}$

$$(a_0 + a_1\sqrt{2})\underbrace{\left(\frac{a_0}{a_0^2 - 2a_1^2} - \frac{a_1}{a_0^2 - 2a_1^2}\sqrt{2}\right)}_{(a_0 + a_1\sqrt{2})^{-1}} = 1$$

CUERPOS FINITOS

$$\mathbb{Z}_5[x]/(x^4+2) = \{a_0 + a_1 t + a_2 t^2 + a_3 t^3 : a_0, a_1, a_2, a_3 \in \mathbb{Z}_5, t^4 + 2 = 0\}$$

$$= \{\underset{\substack{\uparrow \\ 5}}{a_0} + \underset{\substack{\uparrow \\ 5}}{a_1} t + \underset{\substack{\uparrow \\ 5}}{a_2} t^2 + \underset{\substack{\uparrow \\ 5}}{a_3} t^3 : a_0, a_1, a_2, a_3 \in \mathbb{Z}_5, t^4 = -2 = 3\}$$

5^4 elementos.

PRIMALIDAD

Un polinomio $P(x)$ con grado positivo es irreducible o primo, si para toda factorización:

$$P(x) = Q(x)G(x)$$

se tiene que $grad(Q(x)) = 0$ o $grad(G(x)) = 0$

x^2+1 es irreducible en $\mathbb{R}[x]$, pero es reducible en $\mathbb{C}[x]$, $(x-i)(x+i) = x^2+1$.

Se puede demostrar que

$\mathbb{K}[x]/(P(x))$ es un cuerpo,
$a_0 + a_1 t + a_2 t^2 + \cdots a_{n-1} t^{n-1} \neq 0$
tiene inverso

$\iff$

$P(x)$ es primo

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$ $\quad \mathbb{Z}_5[x]/(x^4+2)$

son cuerpos

Teorema de descomposición en factores primos

$\mathbb{K}[x]$ es un dominio de factorización. Todo polinomio $Q(x)$ con grado positivo se factoriza como un producto finito de polinomios primos.

$$Q(x) = P_1(x)P_2(x)\cdots P_k(x)$$

y cada $P_i(x)$ es un polinomio primo.

Álgebra de Polinomios en las variables $x_1, x_2, ..., x_n$

$$\mathbb{A} = \{x_1, x_2, ..., x_n\}$$

¿Qué es un monomio en las variables $x_1, x_2, ..., x_n$?

Caso No Conmutativo

Un *monomio rígido* de grado k es una k-tupla $\omega = (x_{i_1}, x_{i_2}, x_{i_3}, ..., x_{i_k}) \in \mathbb{A}^k$

$i_j \in \{1, 2, 3, ..., n\}$ $\quad \omega := x_{i_1}x_{i_2}x_{i_3}...x_{i_k}$ $\quad x_2x_3 = (x_2, x_3) \neq (x_3, x_2) = x_3x_2$

$\omega = \emptyset$ es el monomio vacío

$$\mathbb{A}^* = \{\emptyset\} \cup \mathbb{A} \cup \mathbb{A}^2 \cup \mathbb{A}^3 \cdots = \bigcup_{k \geq 0} \mathbb{A}^k$$

es el conjunto formado por todos los monomios rígidos de grado finito.

Un polinomio en las variables $x_1, x_2, ..., x_n$ es una función $P : \mathbb{A}^* \longrightarrow \mathbb{K}$ tal que $\{\omega \in \mathbb{A}^* : P(\omega) \neq 0\}$ es finito.

$$\boxed{P(\omega) = p_\omega}$$

$$\boxed{P(x_1, x_2, ..., x_n) := \sum_{\omega \in \mathbb{A}^*} p_\omega \, \omega}$$

$$P(x_1, x_2, x_3) = 3x_1x_2 - \frac{1}{2}x_2x_3x_2 + 8x_2x_1 - \frac{1}{3}x_2x_1x_2x_1 + 3$$

$$p_\emptyset = 3, \quad p_{x_1x_2} = 3, \quad p_{x_2x_3x_2} = -\frac{1}{2}, \quad p_{x_2x_1} = 8, \quad p_{x_2x_1x_2x_1} = -\frac{1}{3}$$

$$P = Q \Longleftrightarrow p_\omega = q_\omega, \quad \forall \omega \in \mathbb{A}^*$$

Operaciones

Suma: suma punto a punto de funciones

$$(P+Q)(\omega) = P(\omega) + Q(\omega) = p_\omega + q_\omega$$

$$\sum_{\omega\in\mathbb{A}^*} p_\omega\,\omega \;+\; \sum_{\omega\in\mathbb{A}^*} q_\omega\,\omega = \sum_{\omega\in\mathbb{A}^*} (p_\omega + q_\omega)\,\omega$$

Propiedades: $\begin{cases} \text{Asociativa, Conmutativa, } P=0 \text{ es el neutro,} \\ -P \text{ es opuesto de } P \end{cases}$

Producto: Concatenación de Monomios

$$\cdot : \mathbb{A}^k \times \mathbb{A}^r \longrightarrow \mathbb{A}^{r+k}$$

$$\underline{x_{i_1}x_{i_2}x_{i_3}\ldots x_{i_k}} \cdot \underline{x_{j_1}x_{j_2}x_{j_3}\ldots x_{j_r}} = \underline{x_{i_1}x_{i_2}x_{i_3}\ldots x_{i_k}x_{j_1}x_{j_2}x_{j_3}\ldots x_{j_r}}$$

$$x_2x_3x_1 \cdot x_3x_1x_2 = \underline{x_2x_3x_1x_3x_1x_2}$$

$$\left.\begin{array}{r}(\omega_1 \cdot \omega_2) \cdot \omega_3 = \omega_1 \cdot (\omega_2 \cdot \omega_3) = \omega_1\omega_2\omega_3 \quad \text{Asociativo} \\ \omega \cdot \emptyset = \omega = \emptyset \cdot \omega \quad \text{Neutro}\end{array}\right\} \text{Monoide}$$

$$(P \cdot Q)(\omega) = \boxed{(p \cdot q)_\omega = \sum_{\omega_1 \cdot \omega_2 = \omega} p_{\omega_1} q_{\omega_2}}$$

$$\left(\sum_{\omega \in \mathbb{A}^*} p_\omega\, \omega\right)\left(\sum_{\omega \in \mathbb{A}^*} p_\omega\, \omega\right) = \sum_{\omega \in \mathbb{A}^*} (p \cdot q)_\omega\, \omega = \sum_{\omega \in \mathbb{A}^*} \left(\sum_{\omega_1 \cdot \omega_2 = \omega} p_{\omega_1} q_{\omega_2}\right) \omega$$

$$\begin{aligned}(3x_1x_2 + 5x_1x_2x_3 - x_2x_3)(x_1 - x_2x_3) \quad = \quad & 3x_1x_2x_1 - 3x_1x_2x_2x_3 \\ & + 5x_1x_2x_3x_1 - 5x_1x_2x_3x_2x_3 \\ & - x_2x_3x_1 + x_2x_3x_2x_3\end{aligned}$$

Propiedades: Asociatividad, $\delta_{\emptyset,\omega} = 1$ es la unidad, No es conmutativo,
Leyes distributivas, $\lambda \in \mathbb{K}$, $(\lambda P)Q = P(\lambda Q) = \lambda(PQ)$

$\mathbb{K}\langle x_1, x_2, ..., x_n\rangle$ es la $\mathbb{K}$-álgebra de polinomios no conmutativa en las variables $x_1, x_2, ..., x_n$

IDEALES

Un ideal de $\mathbb{K}\langle x_1, x_2, ..., x_n\rangle$ *es un subconjunto no vacío* I *de polinomios tales que:*

1. $P + Q \in I \quad \forall P, Q \in I$

2. $PQ \in I$
   - $\forall P \in \mathbb{K}\langle x_1, x_2, ..., x_n\rangle,\ \forall Q \in I$ *Lateral izquierdo*
   - $\forall P \in I,\ \forall Q \in \mathbb{K}\langle x_1, x_2, ..., x_n\rangle$ *Lateral derecho*

   Bilateral

Si I es un ideal bilateral en $\mathbb{K}\langle x_1, x_2, ..., x_n\rangle$

$P \sim Q \iff P - Q \in I$ es una relación de equivalencia

$$\overline{P} = P + I = \{P + Q : Q \in I\}$$

$$\mathbb{K}\langle x_1, x_2, ..., x_n\rangle / I = \{P + I : P \in \mathbb{K}\langle x_1, x_2, ..., x_n\rangle\}$$

$\mathbb{K}\langle x_1, x_2, ..., x_n\rangle / I$ con las operaciones

es una $\mathbb{K}$-álgebra no conmutativa de polinomios y reducida por el ideal bilateral I.

$$(P+I)+(Q+I)=(P+Q)+I$$

$$(P+I)(Q+I)=PQ+I$$

Ejemplos:

CUATERNIONES Fueron creados por William Rowan Hamilton en 1843 que buscaba extender a los números complejos a un número mayor de dimensiones. Tienen varias aplicaciones:

Teoría de Números: Sirve para probar el Teorema de Lagrange, que dice:

Todo número natural $n > 0$ *se escribe como* $n = a^2 + b^2 + c^2 + d^2$, a, b, c, d *son enteros no negativos*

$$5 = 2^2 + 1^2 + 0^2 + 0^2, \qquad 31 = 5^2 + 2^2 + 1^2 + 1^2.$$

Física: Los cuaterniones representan rotaciones del espacio que son útiles para interpretar ecuaciones provenientes del electromagnetismo y la mecánica cuántica

También son utilizados para la interpretación de gráficos asistidos por el computador.

Construcción: $\mathbb{R}\langle x_1, x_2, x_3\rangle$ $P_1(x_1, x_2, x_3) = x_1^2 + 1$, $P_2(x_1, x_2, x_3) = x_2^2 + 1$, $P_3(x_1, x_2, x_3) = x_3^2 + 1$, $P_4(x_1, x_2, x_3) = x_1 x_2 x_3 + 1$

Sea I el ideal bilateral generado por P_1, P_2, P_3, P_4.

Un elemento de I es una suma finita: $\sum_{i=1}^{k} Q_i P_{j_i} Q_i'$ $\quad Q_i, Q_i' \in \mathbb{R}\langle x_1, x_2, x_3\rangle$, $j_i \in \{1, 2, 3, 4\}$

$\mathbb{H} = \mathbb{R}\langle x_1, x_2, x_3\rangle / I \quad x_1 + I = i, \quad x_2 + I = j, \quad x_3 + I = k$

$$i^2 = (x_1 + I)(x_1 + I) = x_1^2 + I = -1 + I, \quad \boxed{i^2 = -1}$$
$$j^2 = (x_2 + I)(x_2 + I) = x_2^2 + I = -1 + I, \quad \boxed{j^2 = -1}$$

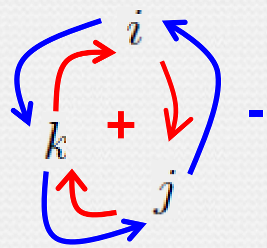
$$k^2 = (x_3 + I)(x_3 + I) = x_3^2 + I = -1 + I, \quad \boxed{k^2 = -1}$$

$$ijk = (x_1 + I)(x_2 + I)(x_3 + I) = x_1x_2x_3 + I = -1 + I, \quad \boxed{ijk = -1}$$

$$i^2 = j^2 = k^2 = ijk = -1$$

Ecuaciones que inspiraron a Hamilton mientras cruzaba el puente de Brougham con su esposa.

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1



Si ω es un monomio de grado mayor o igual a 2, entonces

$$\omega + I \in \{i, j, k, -i, -j, -k, 1, -1\}$$

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$$
$$= \mathbb{R}\langle 1, i, j, k : i^2 = j^2 = k^2 = ijk = -1\rangle$$

Generadores

Relaciones

De forma similar que en los números complejos

$$\overline{q} = \overline{a + bi + cj + dk} = a - bi - cj - dk \qquad | q | = \sqrt{a^2 + b^2 + c^2 + d^2}$$

$$q\overline{q} = | q |^2 \qquad q\frac{\overline{q}}{| q |^2} = 1, \qquad q^{-1} = \frac{\overline{q}}{| q |^2}$$

Polinomios conmutativos en varias variables

Sea I el ideal bilateral de $\mathbb{K}\langle x_1, x_2, ..., x_n\rangle$ generado por todos los binomios de la forma $\omega - \omega'$ en donde ω' es el resultado de haber cambiado de posición las variables de ω. $\boxed{x_1x_2x_3x_1 - x_2x_1x_3x_1}$ $\boxed{x_1x_2x_3 - x_2x_3x_1}$

Un elemento de I es una suma finita de polinomios que tienen la forma $Q(\omega - \omega')R, \quad Q, R \in \mathbb{K}\langle x_1, x_2, ..., x_n\rangle$,

$$\mathbb{K}\langle x_1, x_2, ..., x_n\rangle / I = \mathbb{K}[x_1, x_2, ..., x_n]$$

$$x_1x_2x_3x_1 + I = x_1x_1x_2x_3 + I = x_2x_1x_3x_1 + I := x_1^2x_2x_3$$

$$\omega + I := x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$$

i_j es el número de repeticiones que tiene la variable x_j en ω.

Un polinomio en las variables $x_1, x_2, ..., x_n$ es:

$$\boxed{P(x_1, x_2, ..., x_n) = \sum_{(i_1,i_2,...,i_n)\in\mathbb{N}^n} a_{i_1,i_2,...,i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}}$$

$\mathbb{K}[x_1, x_2, ..., x_n]$ es similar a $\mathbb{K}\langle x_1, x_2, ..., x_n\rangle$ excepto que el producto es conmutativo.

Otros resultados importantes sobre $\mathbb{K}[x_1, x_2, ..., x_n]$

Teorema de la base de Hilbert **(1888)**

Todo ideal I de $\mathbb{K}[x_1, x_2, ..., x_n]$ está finitamente generado.

$$I = \langle P_1, P_2, ..., P_k\rangle = \left\{\sum_{i=1}^{k} Q_iP_i : Q_i \in \mathbb{K}[x_1, x_2, ..., x_n]\right\}$$

Si $PQ = 0$, entonces $P = 0$ o $Q = 0$

$\mathbb{K}[x_1, x_2, ..., x_n]$ admite descomposición en factores primos

Funciones polinómicas

Una función $f : \mathbb{K} \longrightarrow \mathbb{K}$, es polinómica, si existen $a_0, a_1, ..., a_n \in \mathbb{K}$ tales que

$$f(s) = a_0 + a_1 s + a_2 s^2 + \cdots a_n s^n \text{ para cada } s \in \mathbb{K}.$$

$\mathbb{K}[x]$ no es igual al conjunto formado por todas las funciones polinómicas de $\mathbb{K}$ en $\mathbb{K}$

$P(x) = x^2 + x \neq 0$ en $\mathbb{Z}_2[x]$, pero P como función de $\mathbb{Z}_2$ en $\mathbb{Z}_2$ es la función cero.

$$P(\overline{0}) = \overline{0}^2 + \overline{0} = \overline{0},\ P(\overline{1}) = \overline{1}^2 + \overline{1} = \overline{2} = \overline{0}$$

Aplicaciones

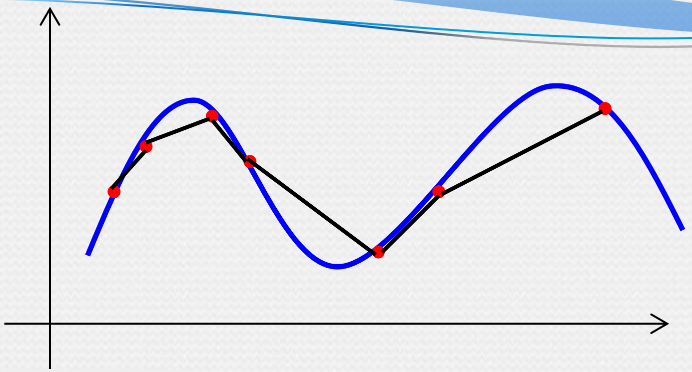
Análisis

1. Interpolación

la interpolación polinomial consiste en aproximarse a valores reales de una curva o función f, mediante

$$(x_k, P_m(x_k)) \text{ y } P_m(x_k) = f(x_k)$$

P_m polinomio interpolador de grado m.



Interpolación de Lagrange

f, $x_0, x_1, ..., x_m$, $f(x_j) = f_j$, el polinomio de grado $n \leq m$ a interpolar es

$$\sum_{j=0}^{n} f_j L_j(x)$$

$$L_j(x) = \prod_{j \neq i} \frac{x - x_i}{x_j - x_i} = \frac{(x-x_0)(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_j-x_0)(x_j-x_1)\cdots(x_j-x_{j-1})(x_j-x_{j+1})\cdots(x_j-x_n)}$$

$L_j(x)$ se denomina polinomio de Lagrange.

Teorema de Taylor Si f es derivable n-veces en el abierto $(a-\epsilon, a+\epsilon)$, $\epsilon > 0$, entonces:

$$f(x) = \boxed{f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots \frac{f^{(n)}(a)}{n!}(x-a)^n} + R_n(f)$$

Polinomio de Taylor de grado n

$$R_n(f) = \frac{f^{(n+1)}(\xi)}{(n+1)!}(x-a)^{n+1} \quad , a < \xi < x < a + \epsilon$$

$$R_n(f) = \int_a^x \frac{f^{(n+1)}(t)}{n!}(x-t)^n \, dt$$

TEOREMA DE APROXIMACIÓN DE WEIERSTRASS (1885)

Todas las funciones continuas definidas en un intervalo cerrado $[a, b]$ *se pueden aproximar por un polinomio*

Posteriormente Marshall Stone en (1937) simplificó la demostración y también demostró que la aproximación era uniforme.

$f \in C[a, b]$, Para todo $\epsilon > 0$ existe un polinomio P tal que

$$Sup\{| f(x) - P(x) |: x \in [a, b]\} < \epsilon$$

Los polinomios de Berntein funcionan para aproximarse a f.

$$B_n(f)(x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k} \qquad \lim_{x \longrightarrow \infty} B_n(f)(x) = f(x)$$

Combinatoria (*Principios de Conteo*)

El factorial de un número k es $\quad k! = k(k-1)(k-2)\cdots 2\cdot 1, \quad 3! = 3\cdot 2\cdot 1$

Binomio de Newton

$$(1+x)^n = \underbrace{(1+x)(1+x)\cdots(1+x)}_{n\text{-veces}} = 1 + a_1x + a_2x^2 + a_3x^3 + \cdots a_nx^n$$

El monomio x^k se construye eligiendo de los n-factores la letra x una cantidad k de veces.

$$\begin{array}{rccccc}
\text{elección} & 1 & 2 & 3 & & k \\
x^k = & \boxed{x} & \boxed{x} & \boxed{x} & \boxed{\cdots} & \boxed{x} \\
 & \uparrow & \uparrow & \uparrow & & \uparrow \\
\text{posibilidades} & \multicolumn{5}{c}{\dfrac{n \;\cdot\; (n-1) \cdot (n-2) \quad \cdots \quad (n-k+1)}{k!}}
\end{array}$$

$$a_k = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Diferentes subconjuntos de tamaño k que tiene $\{1,2,3,\ldots,n\}$

$$(1+1)^n = 2^n = \sum_{k=0}^{n} \binom{n}{k} = \mid \mathbb{P}(\{1,2,3,\ldots,n\}) \mid$$

$$\left(1+\frac{x}{y}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \left(\frac{x}{y}\right)^k$$

$$\frac{(y+x)^n}{y^n} = \left(\frac{y+x}{y}\right)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{-k}$$

$$\boxed{(y+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

Descomposición Fuerte de un número

Sea n un número entero positivo. Una k-descomposición fuerte de n es una k-tupla de enteros positivos $(n_1, n_2, ..., n_k)$ tales que

$$n_1 + n_2 + n_3 + \cdots n_k = n$$

Las 3-descomposiciones fuertes de 5 son

$$3+1+1 \qquad 1+3+1 \qquad 1+1+3 \qquad 2+2+1 \qquad 2+1+2 \qquad 1+2+2$$

una k-descomposición fuerte de n es una descomposición del monomio x^n

$$x^n = x^{n_1} \cdot x^{n_2} \cdot x^{n_3} \cdots x^{n_k} \quad n_i > 0$$

$$x^n = \boxed{x \bullet_1 x \bullet_2 x \cdots x \bullet_{m_1} \,|\, x \cdots x \bullet_{m_2} \,|\, \cdots \bullet_{m_{k-1}} \,|\, x \cdots \bullet_{n-1} x}$$

$$x^{n_1} \qquad x^{n_2} \qquad \cdots \qquad x^{n_k}$$

Lo que estamos haciendo es elegir del conjunto de espacios $\{\bullet_1, \bullet_2, ... \bullet_{n-1}\}$

el subconjunto $\{\bullet_{m_1}, \bullet_{m_2}, ..., \bullet_{m_{k-1}}\}$

$$\binom{n-1}{k-1}$$ número de diferentes k-descomposiciones fuertes de n.