# Álgebra

Nicolás Margenat

2Q 2020

## Secciones

# 1 Conjuntos

Definición: Colección de objetos llamados *elementos* que tienen la propiedad que dado un objeto cualquiera se puede decidir si el elemento está o no en el conjunto.

- **No** importa el orden de los elementos
- **No** se tienen en cuenta las repeticiones

Hay dos *maneras de definir un conjunto*:

- **Extensión**: A={a,e,i,o,u}
- **Comprensión**: A={x/ x es vocal}

## 1.1 Subconjuntos

Definición: Sea A un conjunto. Se dice que un conjunto B está contenido ó incluido en A si todo elemento de B está incluido en A.

$$B \subseteq A \Leftrightarrow \forall x,\, x \in B \Rightarrow x \in A$$

$$B \nsubseteq A \Leftrightarrow \exists x / \, x \in B \wedge x \notin A$$

**Igualdad de conjuntos**

$$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$$

**Conjunto de Partes**

$$A \; conjunto. \; \mathcal{P}_{(A)} = \{B \; conjunto / \; B \subseteq A\}$$

## 1.2 Operaciones entre conjuntos

Para trabajar con conjuntos se toma un conjunto llamado conjunto universal o conjuntos de referencia

1. **Unión**
$$A \cup B = \{x \in \mathcal{U} / \, x \in A \vee x \in B\}$$
2. **Intersección**
$$A \cap B = \{x \in \mathcal{U} / \, x \in A \wedge x \in B\}$$
3. **Diferencia/Resta**
$$A - B = \{x \in \mathcal{U} / \, x \in A \wedge x \notin B\}$$
4. **Complemento**
$$\overline{A} = A^c = \{x \in \mathcal{U} / \, x \notin A\}$$

5. **Diferencia Simétrica**

$$A \triangle B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

**Propiedades**

1. *Leyes de De Morgan*

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

2. *Leyes Distributivas*

$$A \cap B(B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup B(B \cap C) = (A \cup B) \cap (A \cup C)$$

3. *Ley Conmutativa*

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

4. *Ley Asociativa*

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C)$$

5. *Otras*

$$A \cup \varnothing = A$$
$$A \cap \varnothing = \varnothing$$
$$A \cup \mathcal{U} = \mathcal{U}$$
$$A \cap \mathcal{U} = A$$
$$\overline{\varnothing} = \mathcal{U}$$
$$\overline{\mathcal{U}} = \varnothing$$

## 1.3 Producto Cartesiano

Definición: Sean $A, B \subseteq \mathcal{U}$. Entonces,

$$A \times B = \{(a, b) / \, a \in A, b \in B\}$$

**Propiedades**

1. $A \times \varnothing = \varnothing$
2. $\varnothing \times A = \varnothing$
3. **NO** es Asociativa
4. **NO** es Conmutativa

## 1.4 Familia de Subconjuntos

Definición: Dado un conjunto A, una *familia de subconjuntos de A* es un subconjunto de $\mathcal{P}_{(A)}$.

$$\mathcal{F} \subseteq \mathcal{P}_{(A)}$$

### 1.4.1 Operaciones con Familias

Sea $\mathcal{F} \subseteq \mathcal{P}_{(A)}$, entonces:

1. **Unión**
$$\cup\mathcal{F} = \cup B = \{x \in A / \, x \in B \text{ para algún } B \in \mathcal{F}\}$$

2. **Intersección**
$$\cap\mathcal{F} = \cap B = \{x \in A / \, x \in B \text{ para todo } B \in \mathcal{F}\}$$

# 2 Relaciones

Definición: Sean A y B conjuntos no vacíos, una *relación de A en B* es un subconjunto de $A \times B$.
Notación: $R \subseteq A \times B$ ó $R \in \mathcal{P}_{(A \times B)}$

Por otro lado, sea A un conjunto. Se dice que *R es una relación en A* si $R \subseteq A \times A$("R en A").

## 2.1 Dominio e Imagen

Sea $R \subseteq A \times B$:

$$Dom(R) : \{x \in A / \, \exists y \in B \text{ tal que } x\mathcal{R}y\}$$

$$Im(R) : \{y \in B / \, \exists x \in A \text{ tal que } x\mathcal{R}y\}$$

## 2.2 Relación Inversa

Definición: Dada R en $A \times B$, se define $R^{-1} \subseteq B \times A$ tal que:

$$R^{-1} \; = \; \{(x, y) / \, (y, x) \in R\}$$

Además:

$$Dom(R) \; = \; Im(R^{-1})$$
$$Im(R) \; = \; Dom(R^{-1})$$

## 2.3 Propiedades de una relación de un conjunto en sí mismo

- **Reflexividad**
  R es reflexiva si:
  $$a\mathcal{R}a \; \forall a \in A$$
  R no es reflexiva si:
  $$\exists a \in A / \; a\not\mathcal{R}a$$
- **Simetría**
  R es simétrica si:
  $$a\mathcal{R}b \; \Rightarrow \; b\mathcal{R}a \; \forall a, b \in A$$
  R no es simétrica si:
  $$\exists a, b \in A / \; a\mathcal{R}b \; \wedge \; b\not\mathcal{R}a$$
- **Antisimetría**
  R es antisimétrica si(cualquiera de las dos sucede, pues son expresiones equivalentes):
  $$a\mathcal{R}b \; \wedge \; b\mathcal{R}a \; \Rightarrow \; a = b$$
  $$a\mathcal{R}b \; \wedge \; a \neq b \; \Rightarrow \; b\not\mathcal{R}a$$
  R no es antisimétrica si:
  $$\exists a, b \in A / \; a \neq b \; \wedge \; a\mathcal{R}b \; \wedge \; b\mathcal{R}a$$
- **Transitividad**
  R es transitiva si:
  $$a\mathcal{R}b \; \wedge \; b\mathcal{R}c \; \Rightarrow \; a\mathcal{R}c \; \forall a, b, c \in A$$
  R no es transitiva si:
  $$\exists a, b, c \in A / \; a\mathcal{R}b \; \wedge \; b\mathcal{R}c \; \wedge \; a\not\mathcal{R}c$$

De esta manera, podemos decir que:

- R es de **equivalencia** si es: reflexiva, simétrica y transitiva.
- R es de **orden** si es: reflexiva, antisimétrica y transitiva.
- R es de **orden total** si es: de orden y $\forall a, b \in A : a\mathcal{R}b \; \vee \; b\mathcal{R}a$

## 2.4 Relaciones de equivalencia

### 2.4.1 Propiedades de las relaciones de equivalencia

R en A, R es de equivalencia. Entonces:

$$A_1 \cup A_2 \cup ... \cup A_n = A$$
$$A_i \wedge A_j = \varnothing \text{ si } i \neq j$$

## Clases de equivalencia

R en A. R de equivalencia. $a \in A$. Entonces, definimos la *clase de a* como:

$$[a] = \overline{a} = \{b \in A / \, b\mathcal{R}a\}$$

El *conjunto cociente* es el conjunto de clases de R, y se nota:

$$A/\mathcal{R} = \{\overline{a}\}$$

### Particiones

A conjunto. A $\neq \varnothing$. $\mathcal{F} \subseteq \mathcal{P}_{(A)}$.
$\mathcal{F}$ es una *partición* de A si:

1. $B \neq \varnothing, \forall B \in \mathcal{F}$
2. $B_1, B_2 \in \mathcal{F}$, $B_1 \neq B_2 \Rightarrow B_1 \wedge B_2 = \varnothing$
3. $\cup\mathcal{F} = \cup B = A$

| Teorema 2.A |
| --- |
| R en A, R de equivalencia. |
| R induce una partición en A. |

| Teorema 2.B |
| --- |
| Dado un conjunto A $\neq \varnothing$. Sea $\mathcal{F}$ una partición de A. Entonces $\mathcal{F}$ induce una relación de equivalencia R en A. |

# 3 Funciones

Definición: Sea $R \subseteq A \times B$ una relación. Decimos que R es una función si:

1. $\forall a \in A, \exists b \in B / \, (a, b) \in R$
2. $(a, b) \in R \wedge (a, c) \in R \Rightarrow b = c$

otra manera de decirlo es: R es función si,

$$\forall a \in A, \exists! \, b \in B / \, (a, b) \in R$$

Notación: $f : A \to B / f_{(a)} = b$ si $(a, b) \in R$. Donde,
A = $Dom(f)$
B = $Codom(f)$
$Im(f) = \{y \in B / \exists x \in A$ tal que $f(x) = y\}$
Preimagen = $f^{-1}(y) = \{x \in A / f(x) = y\}$

## 3.1 Inyectividad, Sobreyectividad y Biyectividad

- **Inyectiva**
  Decimos que *f es inyectiva* si:

  $$f(a) = f(b) \Rightarrow a = b$$

  o lo que es lo mismo:

  $$a \neq b \Rightarrow f(a) \neq f(b)$$

- **Sobreyectiva**
  Decimos que *f es sobreyectiva* si:

  $$\forall b \in B, \exists a \in A / f(a) = b$$

  o lo que es lo mismo: $Im(f) = B$

- **Biyectiva**
  Decimos que *f es biyectiva* si:

  $$f \text{ es inyectiva } \wedge \ f \text{ es sobreyectiva}$$

## Función Inversible

Definición: Sea $f : A \to B$. Decimos que *f es inversible* si:

$$\exists g : A \to B / \, g \circ f = id_A \ \wedge \ f \circ g = id_B$$

Notación: $g = f^{-1}$ (*g es la inversa de f*)

# 4 Combinatoria

Definición: Dado un conjunto A finito, el *cardinal de A* es la cantidad de elementos de A.
Notación: $\#A = |A|$

## 4.1 Principios de conteo

### Primer principio de conteo

"Si una tarea puede efectuarse en k etapas, y la etapa j se puede desarrollar de $n_j$ formas distintas, entonces la tarea se puede desarrollar de $n_1 * n_2 * ... * n_k = n^k$ formas distintas."

### Segundo principio de conteo

"Cuando hay casos que son disjuntos, se *suman* las posibilidades de cada caso"

$$A = \cup_{j=1}^{k} A_j = A_1 \cup A_2 \cup ... \cup A_k$$

$$A_i \cap A_j = \varnothing \text{ si } i \neq j$$

$$\#A = \sum_{j=1}^{k} \#A_j = \#A_1 + \#A_2 + ... + \#A_k$$

## 4.2 Variación vs. Combinación

### Variación

Definición: Una variación de k elementos de X es una *cadena ordenada* de k elementos de X.

$$V_{(n,k)} = \frac{n!}{(n-k)!} = \binom{n}{k} k$$

De esta forma podemos deducir que la *cantidad de formas de ordenar n elementos* es:

$$V_{(n,n)} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

Una manera practica de verlo es: *"Agarro k elementos de un conjunto con n elementos y me importa el orden en que los agarro"*

### Combinación

Definición: Una combinación de k elementos de X es un subconjunto de k elementos de X.

$$C_{(n,k)} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Una manera práctica de verlo es: *"Agarro k elementos de un conjunto de n elementos sin importar el orden en que los agarro"*

**Propiedades de los números combinatorios**

1. $$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \; 1 \leq k \leq n$$

2. $$\binom{n}{k} = \binom{n}{n-k}$$

3. $$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n} = 2^n$$

Además, $\#\mathcal{P}_{(X)} = 2^{\#X}$

**Orden con repetición**

Sirve para resolver ejercicios del tipo: *"¿Cuántas palabras de n letras puedo formar si hay j letras que se repiten?"*

$$\frac{n!}{n_1!n_2!...n_j!}$$

donde $n_1, n_2...n_j$ es la cantidad de veces que se repite cada letra.

**Distribución de bolitas indistinguibles en cajas distintas**

Sirve para reolver ejercicios del tipo: *"Tengo n bolitas en k cajas indistinguibles. ¿De cuántas formas se pueden distribuir?"*

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}$$

# 5 Enteros

## 5.1 Definiciones previas

Estructura algebraica: Es una n-tupla formada por:

$$( \underbrace{A_1, ..., A_k}_{\text{Conjuntos} \neq \varnothing} \ ; \ \underbrace{op_1, ..., op_t}_{\substack{\text{Operaciones definidas sobre los} \\ \text{conjuntos anteriores}}} \ ) \ \ k + t = n$$

Grupo: Es una estructura algebraica

$$(G, \otimes)$$

$$\otimes : G \times G \to G$$

que cumple las siguientes propiedades:

- **Asociativa**
$$a \otimes (b \otimes c) \ = \ (a \otimes b) \otimes c$$
- **Existencia de Elemento Neutro**
$$\exists e \in G / \ a \otimes e = a, \ e \otimes a = a$$
- **Inverso**
$$\forall a \in G, \exists \overline{a} \in G / \ a \otimes \overline{a} = e \ \wedge \ \overline{a} \otimes a = e$$
- **Conmutativo**
$$a \otimes b = b \otimes a$$

Anillo Conmutativo: $(A, +, \otimes)$ es un anillo conmutativo si:

1. $(A, +)$ es un grupo conmutativo.
2. $\otimes$ es: asociativo, conmutativo, distributivo y tiene elemento neutro.

Cuerpo: $(K, +, \otimes)$ es un cuerpo si:

1. $(K, +, \otimes)$ es un anillo conmutativo.
2. $\forall a \in K, a \neq 0, \exists a^{-1} / \ a \otimes a^{-1} = 1$ (existe inverso)

Unidades de un anillo: A es un anillo, $a \in A$ es una unidad de un anillo si:

$$\exists b \in A / \ a \otimes b = 1 \ \wedge \ b \otimes a = 1$$

y se nota: $\mathcal{U}_{(A)}$ ("conjunto de unidades de A")

## 5.2 Divisibilidad en un anillo

Definición: A es un anillo, $a, b \in A$, $b \neq 0$. Decimos que "a es divisible por b", "a es múltiplo de b", "b es divisor de a" si:

$$\exists c \in A / \, a \, = \, bc$$

Notación: $b|a$

$Div(a) \, = \, \{b \in A / \, b|a\}$ ("conjunto de divisores de a")

### Propiedades

Sean $a, b, c \in \mathbb{Z}$

1. $a \leq b \, \Rightarrow \, a + c \leq b + c$
2. $a \leq b \, \wedge \, c \gneq 0 \, \Rightarrow \, ac \leq bc$
3. $ab \, = \, ac \, \wedge \, a \, \neq \, 0 \, \Rightarrow \, b \, = \, c$
4. $ab \, = \, 0 \, \Rightarrow \, a = 0 \, \vee \, b = 0$
5. $a|b \, \Leftrightarrow \, |a| \, | \, |b|$
6. $a|b \, \wedge \, b \neq 0 \, \Rightarrow \, |a| \leq |b|$
7. $a|b \, \wedge \, b|a \, \Rightarrow \, |a| \, = \, |b|$
8. $a|b \, \wedge \, a|c \, \Rightarrow \, a|b \pm c$
9. $a|b \, \wedge \, a|b \pm c \, \Rightarrow \, a|c$
10. $a|b \, \Rightarrow \, a|bc$
11. $a|b \, \Rightarrow \, a^n|b^n$ con $n \in \mathbb{N}$
12. $a|b \, \wedge \, a|c \, \Rightarrow \, a|\alpha b + \beta c$ con $\alpha, \beta \in \mathbb{Z}$

### 5.2.1 Algoritmo de división

Definición: Sea $a \in \mathbb{Z}$, $d \in \mathbb{Z} - \{0\}$. Entonces,

$$\exists! \, q, r \in \mathbb{Z} / \, a \, = \, d * q + r$$

Donde $q = \underbrace{q_d(a)}_{\text{cociente de dividir a por d}}$ y $r = \underbrace{r_d(a)}_{\text{resto de dividir a por d}}$ $0 \leq r \gneq |d|$

De esta manera podemos deducir que:

1. $d|a \, \Leftrightarrow \, r_d(a) = 0$
2. $0 \leq a \gneq |d| \, \Rightarrow \, r_d(a) = a$

## 5.3 Congruencias

Definición: Decimos que $\underbrace{a \equiv b(mod\, m)}_{\text{"a es congruente a b módulo m"}}$ si $m|a-b$

Teorema 5.A
R en $\mathbb{Z}$ tal que $aRb$ si $a \equiv b(m)$.
R es de equivalencia.

Teorema 5.B
Sea $d \in \mathbb{N}$. Entonces:

1. $a \equiv r_d(a)(mod\, d)$
2. $a \equiv b(mod\, d) \Leftrightarrow r_d(a) = r_d(b)$

**Propiedades**

1. $a_1 \equiv b_1(m) \wedge a_2 \equiv b_2(m) \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2(m)$
   $a_1 \equiv b_1(m) \wedge a_2 \equiv b_2(m) \Rightarrow a_1 * a_2 \equiv b_1 * b_2(m)$
2. $a_1 \equiv b_1(m) \wedge ... \wedge a_k \equiv b_k(m) \Rightarrow a_1 \pm ... \pm a_k \equiv b_1 \pm ... \pm b_k(m)$
   $a_1 \equiv b_1(m) \wedge ... \wedge a_k \equiv b_k(m) \Rightarrow a_1 * ... * a_k \equiv b_1 * ... * b_k(m)$
3. $a \equiv b(m) \Rightarrow a^n \equiv b^n(m)\ \forall n \in \mathbb{N}$
4. $a \equiv b(m) \Rightarrow ac \equiv bc(m)$

## 5.4 Maximo común divisor (MCD)

Definición: Sean $a, b \in \mathbb{Z}$ no ambos nulos, entonces $d \in \mathbb{Z}$ es el MCD de a y b si:

1. $d \gneq 0$
2. $d|a \wedge d|b$
3. $c|a \wedge c|b \Rightarrow c|d$

Notación: $d = MCD(a,b) = (a:b)$ **Propiedad**: $a, b \in \mathbb{Z}$, no ambos nulos, $c \in \mathbb{Z} - \{0\}$. Entonces,

$$(ca:cb) = |c|\,(a:b)$$

### 5.4.1 Combinación Entera

Definición: Una combinacion entera de a y b es un número de la forma $ra + sb$, con $r$, $s \in \mathbb{Z}$

Teorema 5.C

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Entonces:

$$\exists! \, d \in \mathbb{Z} / \, d \; = \; (a : b)$$

y además es la menor combinación entera positiva de a y b.

Lema

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Entonces:

$$(a : b) \; = \; (b : a - kb) \; \forall k \in \mathbb{Z}$$

En particular, si $b \neq 0$

$$k \; = \; q_b a \; \Rightarrow \; (a : b) \; = \; (b : r_b a)$$

## 5.5 Números Coprimos

Definición: Se dice que a y b son coprimos si $(a : b) = 1$.
Notación: $a \perp b$

## Propiedades

1. $a \perp b \; \wedge \; a | bc \; \Rightarrow \; a | c$
2. $a \perp b \; \wedge \; a \perp c \; \Rightarrow \; a \perp bc$
3. $a | c \; \wedge \; b | c \; \wedge \; a \perp c \; \Rightarrow \; ab | c$
4. $d = (a : b) \; \Rightarrow \; \frac{a}{d} \perp \frac{b}{d}$
5. $a \perp b \; \Rightarrow \; a^n \perp b^k$ con $n, k \in \mathbb{N}$
6. $a \perp c \; \Rightarrow \; (a : cb) \; = \; (a : b)$

### 5.5.1 Primos vs. Compuestos

Primo: Un número $p \in \mathbb{Z}$ si tiene exactamente 4 divisores.
Es decir, $div(p) = \{\pm 1; \pm p\}$ siendo $|p| \geq 1$
Compuesto: Un número $a \in \mathbb{Z}$ es compuesto si *no es primo* y $a \notin \{1, -1\}$

#### Propiedades

1. a es compuesto $\Rightarrow \; \exists a_1, \, a_2 / \, a = a_1 * a_2 \; \wedge \; 2 \leq |a_i| \leq |a| - 1$
2. $(a : p) \; = \; 1$ si $p \not| a$
   $(a : p) \; = \; p$ si $p | a$

## 5.6 Números Primos

Teorema 5.D
p primo y $p|ab \Rightarrow p|a \vee p|b$
Generalización:

$$p\,primo \wedge p|a_1 * a_2 * ... * a_k \Rightarrow \exists i/\, p|a_i \text{ con } 1 \leq i \leq k$$

Teorema 5.E
Existen infinitos números primos

### 5.6.1 $V_p$

Sea p primo. Entonces:

$$V_p : \mathbb{Z} - \{0\} \to \mathbb{N}_0 / \; V_p(a) \text{ es} \begin{cases} 0 & \text{si } p \not| a \\ k & \text{si } p^k|a \wedge p^{k+1} \not| a \end{cases}$$

**Propiedades**

1. $V_p(a * b) = V_p(a) + V_p(b)$
2. $V_p(a^n) = nV_p(a)$
3. $d|a \Rightarrow V_p(d) \leq V_p(a)$
4. $V_p \geq 0$

Teorema Fundamental de la Aritmética (TFA)
Sea $a \in \mathbb{Z} - \{-1, 0, 1\} \Rightarrow a = sg(a)p_1 * p_2 * ... * p_k$ siendo $p_j$ primo y $1 \leq j \leq k$
Además, la *factorización es única* en estos casos.

Corolario TFA
Si $a \in \mathbb{Z} - \{-1, 0, 1\} \Rightarrow \exists p\, primo,\, p \gneq 0 / \; p|a$

## 5.7 Mínimo Común Múltiplo (MCM)

Definición: Sean $a, b \in \mathbb{Z}$ no ambos nulos, el MCM entre a y b es un número $m \in \mathbb{Z}/$

- $m \gneq 0$
- $a|m \wedge b|m$
- $a|c \wedge b|c \Rightarrow m|c$

Notación: $m = [a : b]$

Teorema 5.F
Sean $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0 \Rightarrow |a * b| = (a : b)[a : b]$

## 5.8 Ecuaciones diofánticas

Definición: Una ecuación diofántica es una ecuación que se puede escribir de la siguiente forma:

$$ax + by = c \text{ con } a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$$

Teorema 5.G
Sean ax+by=c con $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$. Entonces:

1. La ecuacion tiene solución en $\mathbb{Z} \Leftrightarrow d|c$
2. Si $(x_0, y_0) \in \mathbb{Z}^2$ es una solución de la ecuación
   $\Rightarrow$ Sol=$\{(x, y) \in \mathbb{Z} / (x, y) = \underbrace{(x_0, y_0)}_{\text{Sol. particular}} + \underbrace{k(\frac{b}{d}, -\frac{a}{d})}_{\text{Sol. homogénea}} \text{ con } k \in \mathbb{Z}\}$

## 5.9 Ecuaciones de congruencia lineal

Definición: Una ecuación de congruencia lineal es una ecuación de la forma:

$$ax \equiv c(b) \text{ con } a, c \in \mathbb{Z},\ a \neq 0,\ b \in \mathbb{N}$$

Teorema 5.H
Sea $ax \equiv c(b)$ con $a, c \in \mathbb{Z}$, $a \neq 0$, $b \in \mathbb{N}$. Entonces:

1. La ecuacion tiene solución $\Leftrightarrow (a : b)|c$
2. Si $x_0$ es una solución de la ecuación
   $\Rightarrow$ Sol=$\{x \in \mathbb{Z} / x \equiv x_0(\frac{b}{(a:b)})\}$

### Inverso multiplicativo modular

Definición: $a^* \in \mathbb{Z}$ es el *inverso multiplicativo de* $a \in \mathbb{Z}$ *módulo* $m$
si $a.a^* \equiv 1(m)$.
Notemos que si m es primo, entonces:
Si $a \not\equiv 0(m) \Rightarrow$ a tiene inverso multiplicativo

**Propiedad cancelativa**

$$a \perp m \ \wedge \ a.c' \equiv a.c'(m) \ \Leftrightarrow \ c \equiv c'(m)$$

Teorema de Fermat

Sea p primo. Entonces:

1. $a^p \equiv a(p)$
2. $a^{p-1} \equiv 1(p)$ si $p \nmid a$

Teorema Chino del Resto (TChR)

$$\begin{cases} x \equiv & a_1(m_1) \\ x \equiv & a_2(m_2) \\ \vdots & \\ x \equiv & a_k(m_k) \end{cases} \qquad m_i \perp m_j \text{ si } i \neq j$$

Entonces,

$$\exists! \, x_0 / \, 0 \leq x_0 \leq \prod_{j=1}^{k} m_j \text{ tal que } x_0 \text{ es sol. del sistema}$$

# 6 Polinomios

Definición: Dado un cuerpo $\mathbb{K}(\mathbb{Q}, \mathbb{R}, \mathbb{C})$, f es un polinomio con coeficientes en $\mathbb{K}$ si se puede escribir como:

$$f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x^1 + a_0 = \sum_{k=0}^{n} a_k x^k$$

Notación: $\mathbb{K}_{[x]}$ es el conjunto de polinomios con coeficientes en $\mathbb{K}$.

**Definiciones importantes**

Igualdad de polinomios: Dados $f = \sum_{j=0}^{n} a_j x^j$ y $g = \sum_{j=0}^{m} b_j x^j$ en $\mathbb{K}_{[x]}$ decimos que:

$$f = g \Leftrightarrow n = m \wedge a_j = b_j \text{ con } 0 \leq j \leq n$$

Polinomio nulo: f es el polinomio nulo si $f = 0$.
Si f *no* es el polinomio nulo, entonces:

$$\exists N \in \mathbb{N}_0 / f = \sum_{j=0}^{N} a_j x^j \wedge a_N \neq 0$$

## 6.1 Operaciones en $\mathbb{K}_{[x]}$

Sean $f = \sum_{j=0}^{n} a_j x^j$ y $g = \sum_{j=0}^{n} b_j x^j$.
Entonces:

1. $f + g = \sum_{j=0}^{n} (a_j + b_j) x^j$
2. $f * g = \sum_{j=0}^{2n} c_j x^j$, $c_j = \sum_{i+k} a_i b_k$

Unas observaciones. Sea $\mathbb{K}$ cuerpo, $f, g \in \mathbb{K}_{[x]}$ no nulos. Entonces:

1. Si $f + g \neq 0 \Rightarrow gr(f+g) \leq max\{gr(f), gr(g)\}$
2. Si $f * g \neq 0 \Rightarrow gr(f+g) = gr(f) + gr(g)$

| Teorema 6.A |
| --- |
| $(\mathbb{K}_{[x]}, +, *)$ es un anillo conmutativo, siendo $\mathbb{K}$ cuerpo. Además, si $f * g = 0 \Rightarrow f = 0 \vee g = 0$ |

| Corolario T6.A |
| --- |
| $\mathbb{K}$ cuerpo, $f \in \mathbb{K}_{[x]}$. Entonces: <br> $f$ tiene inverso multiplicativo $\Leftrightarrow f \neq 0 \wedge gr(f) = 0$ |

## 6.2 Divisibilidad

Definición: Sean $f, g \in \mathbb{K}_{[x]}, \mathbb{K}$ cuerpo , $g \neq 0$. Se dice que si $g$ *divide a* $f$, entonces:

$$\exists q \in \mathbb{K}_{[x]} / \, f = g * q$$

Notación: $g|f$

**Propiedades**

1. $g \neq 0$, $g|0$
2. $g|f \Leftrightarrow cg|f$ con $c \in \mathbb{K} - \{0\} = \mathbb{K}^*$
3. $g|f \Leftrightarrow \frac{g}{cp(g)} | \frac{f}{cp(f)}$ con $f \neq 0$
4. $g|f \Leftrightarrow g|cf$ con $c \in \mathbb{K}^*$
5. $f$, $g$ no nulos, $g|f \wedge gr(g) = gr(f) \Rightarrow \exists c \in \mathbb{K}^* / \, f = cg$
6. $f|g \wedge g|f \Rightarrow f = cg$ con $c \in \mathbb{K}^*$
7. $f \notin \mathbb{K}$, $c|f \wedge cf|f$ si $c \in \mathbb{K}^*$. Es decir, f tiene como divisores cualquier constante y múltiplos de él mismo.

**Polinomios reducibles e irreducibles**

Irreducible: Decimos que $f \in \mathbb{K}_{[x]}$ es irreducible en $\mathbb{K}_{[x]}$ cuando $f \notin \mathbb{K}$ y los únicos divisores son $g = c$ ó $g = cf$ con $c \in \mathbb{K}^*$, y los *divisores mónicos* de f son 1 y $\frac{f}{cp(f)}$.

Reducible: Decimos que $f \in \mathbb{K}_{[x]}$ es reducible en $\mathbb{K}_{[x]}$ cuando $f \notin \mathbb{K}$ y

$$\exists g \in \mathbb{K}_{[x]} / \, g|f \wedge g \neq c \wedge g \neq cf \text{ siendo } c \in \mathbb{K}^*.$$

Es decir, $f$ tiene un divisor $g / \, 0 \lneq gr(g) \lneq gr(f)$

Teorema 6.B
Dado $f$, $g \in \mathbb{K}_{[x]}$ no nulos, entonces:

$$\exists! \, q, r \in \mathbb{K}_{[x]} / \, f = g * q + r \text{ con } r = 0 \vee gr(r) \lneq gr(g)$$

siendo q el cociente y r el resto de dividir f por g.

## 6.3 Máximo común divisor

Definición: Sean $f, g \in \mathbb{K}_{[x]}$ no ambos nulos. El Máximo Común Divisor entre f y g es el *polinomio mónico de mayor grado que divide tanto a f como a g*, y es *único*.
Notación: $(f : g)$

**Propiedades**

1. $(f:0) = \frac{f}{cp(f)} \; \forall f \in \mathbb{K}_{[x]}$
2. $(f:g) = (g:r_g(f)) \; \forall g \in \mathbb{K}_{[x]}$, $g$ no nulo.

Corolario MCD polinomios

Sean $f, g \in \mathbb{K}_{[x]}$, $g \neq 0$. Entonces,

1. $c \in \mathbb{K}^*$, $(c:f) = 1$
2. $g|f \Rightarrow (f:g) = \frac{g}{cp(g)}$

## 6.4 Algoritmo de Euclides

Defínción: $f, g \in \mathbb{K}_{[x]}$. Entonces $(f:g)$ es el último resto no nulo divididdo su coeficiente principal que aparece en las siguientes divisiones:

$$(f:g) = (g:r_1) = (r_1:r_2) = ... = (r_{k-1}:r_k) = (r_k:0) = \frac{r_k}{cp(r_k)}$$

Además, existen $s, t \in \mathbb{K}_{[x]} / \, (f:g) = s.f + t.g$

Corolario Algoritmo de Euclides

Sean $f, g \in \mathbb{K}_{[x]}$ no nulos. Entonces, $h = (f:g) \in \mathbb{K}_{[x]}$ es el único polinomio no nulo tal que:

1. $h$ mónico
2. $h|f \wedge h|g$
3. $q|f \wedge q|g \Rightarrow q|h$

## 6.5 Polinomios Coprimos

Definición: Sean $f, g \in \mathbb{K}_{[x]}$ no ambos nulos. Se dice que $(f:g) = 1$ ó $f \perp g \Leftrightarrow \exists s, t \in \mathbb{K}_{[x]} / \, sf + tg = 1$.

**Propiedades**

Sean $f, g \in \mathbb{K}_{[x]}$. Entonces,

1. $g \perp h$, $g|f \wedge h|f \Leftrightarrow gh|f$
2. $g \perp h$, $g|hf \Leftrightarrow g|f$

Observaciones

Sea $f$ irreducible en $\mathbb{K}_{[x]}$. Entonces,

1. $\forall g \in \mathbb{K}_{[x]}$, $(f : g)$
2. $\forall g, h \in \mathbb{K}_{[x]}$, $f|gh \Rightarrow f|g \vee f|h$

Teorema Fundamental de la Aritmética para polinomios

Sea $\mathbb{K}$ cuerpo, $f \in \mathbb{K}_{[x]}$ un polinomio no constante, entonces *existen únicos polinomio mónicos distintos* $g_1, g_2, ..., g_r$ en $\mathbb{K}_{[x]}$ tales que:

$$f = c * g_1^{m_1} * g_2^{m_2} * ... * g_r^{m_r} \text{ donde } c \in \mathbb{K}^*$$

(c es el coeficiente principal de f). Además, la unicidad de los factores es cierta salvo el orden.

## 6.6 Evaluación

Definición: Dado $f = a_n x^n + ... + a_1 x^1 + a_0 \in \mathbb{K}_{[x]}$ se define de forma natural una función:

$$f : \mathbb{K} \to \mathbb{K} / f(x) = a_n x^n + ... + a_1 x^1 + a_0$$

y denominamos a esta función f como *función evaluación.*

### Propiedades

Sean $f, g \in \mathbb{K}_{[x]}$. Entonces,

1. $(f + g)_{(x)} = f_{(x)} + g_{(x)}$
2. $(f * g)_{(x)} = f_{(x)} * g_{(x)}$

## 6.7 Raíz

Definición: Dado $f \in \mathbb{K}_{[x]}$, $a \in \mathbb{K}$. Decimos que *a es raíz de f* si:

$$f(a) = 0 \Leftrightarrow x - a | f \Leftrightarrow f = (x - a)q \text{ para algún } q \in \mathbb{K}_{[x]}$$

Teorema del Resto

$f \in \mathbb{K}_{[x]}$, $a \in \mathbb{K}$. Entonces $r_{x-a}(f) = f(a)$

Observaciones del Teorema del Resto

1. $f, g \in \mathbb{K}_{[x]}$, $g \neq 0 / \ g|f$ en $\mathbb{K}_{[x]}$, $a \in \mathbb{K}$. Entonces:

$$\text{Si } g(a) = 0 \ \Rightarrow \ f(a) = 0$$

2. $f, g \in \mathbb{K}_{[x]}$ no ambos nulos, $a \in \mathbb{K}$. Entonces:

$$f(a) = 0 \ \wedge \ g(a) = 0 \ \Leftrightarrow \ (g : f)_{(a)} = 0$$

## 6.8 Lema de Gauss

Sea $p = a_n x^n + ... + a_1 x^1 + a_0 \in \mathbb{Z}_{[x]}$, $a_n \neq 0 \ \wedge \ a_0 \neq 0$. Entonces:

$$\text{Si } r, s \in \mathbb{Z} - \{0\} \text{ con } r \perp s \ \wedge \ p(\frac{r}{s}) = 0 \ \Rightarrow \ r|a_0 \ \wedge \ s|a_n$$

## 6.9 Polinomio Interpolador de Lagrange

Definición: Sean $a_0, a_1, ...a_n; b_0, b_1, ..., b_n \in \mathbb{C}$, $n \geq 1$, $a_i \neq a_j$ si $i \neq j$. Entonces:

$$f \ = \ \sum_{k=0}^{n} b_k \underbrace{( \prod_{0 \leq j \leq n} \frac{x - a_j}{a_k - a_j})}_{L_k} \ = \ \sum_{k=0}^{n} b_k * L_k \text{ con } j \neq k$$

es el *único polinomio* $\in \mathbb{C}_{[x]}$ *nulo o de grado* $\leq n$ que satisface:

$$f(a_k) \ = \ b_k, \ 0 \leq k \leq n$$

Nota: Este polinomio sirve para encontrar polinomios de *grado mínimo* que *pasen por más de un punto.*

## 6.10 Multiplicidad de una raíz

Definición: Sea $f \in \mathbb{K}_{[x]}$ no nulo. Entonces, sea $m \in \mathbb{N}_0$, se dice que $a \in \mathbb{K}$ es *raíz de multiplicidad m de f* si:

$$(x - a)^m | f \ \wedge \ (x - a)^{m-1} \not| f$$

o equivalentemente:

$$\exists q \in \mathbb{K}_{[x]} / \ f = (x - a)^m * q, \ q(a) \neq 0$$

De esta manera, decimos que

1. $a$ es *raíz simple* de $f$ si:

$$(x - a) | f \ \wedge \ (x - a)^2 \not| f$$

2. $a$ es *raíz múltiple* de $f$ si:

$$(x-a)^2|f$$

Notación: $mult(a,f)=m$ ("la multiplicidad de a en f es m")

**Propiedades**

Sea $f \in \mathbb{K}_{[x]}$, $a \in \mathbb{K}$. Entonces:

1. a es raíz múltiple de $f \Leftrightarrow f(a)=0 \wedge f'(a)=0$
2. a es raíz simple de $f \Leftrightarrow f(a)=0 \wedge f'(a)\neq 0$

Teorema 6.C

$f \in \mathbb{K}_{[x]}$, $a \in \mathbb{K}$. Entonces:

$$mult(a,f)=m \Leftrightarrow f(a)=f'(a)=...=f^{m-1}(a)=0 \wedge f^m(a)\neq 0$$

Teorema Fundamental del Álgebra

$f \in \mathbb{C}_{[x]}$ no constante $\Rightarrow \exists a \in \mathbb{C} / f(a)=0$

Equivalentemente, todo polinomio no constante de grado n en $\mathbb{C}_{[x]}$ tiene n raíces contando su multiplicidad.

Observaciones

1. $f \in \mathbb{R}_{[x]}$, $z \in \mathbb{C}-\mathbb{R} \Rightarrow f(z)=0 \Leftrightarrow f(\overline{z})=0$
2. $f \in \mathbb{Q}_{[x]}$, $a,b,c \in \mathbb{Z} \Rightarrow f(a+b\sqrt{c})=0 \Leftrightarrow f(a-b\sqrt{c})=0$

# 7 Sumas - Recurrencias

Definición:

$$\sum_{k=i}^{n} a_k \;=\; \sum_{i \leq k \leq n} a_k \;=\; a_i + a_{i+1} + a_{i+2} + ... + a_n$$

**Propiedades**

1. **Ley distributiva**
$$\sum_{k=i}^{n} c.a_k \;=\; c \sum_{k=i}^{n} a_k$$

2. **Ley Asociativa**
$$\sum_{k=i}^{n} (a_k + b_k) \;=\; \sum_{k=i}^{n} a_k + \sum_{k=i}^{n} b_k$$

3. **Ley Conmutativa**
$$\sum_{k=i}^{n} a_k \;=\; \sum_{k=i}^{n} a_{p(k)}$$
siendo $p : I \to I$ una *función biyectiva*, $I = i, i+1, ..., n$

4. **Cambio de Índice**
$$\sum_{k \in I} a_k \;=\; \sum_{j \in J} a_{g(j)}$$
siendo $g : J \to I$" una *función biyectiva*, y $J, I$ conjuntos finitos.
Esta propiedad nos permite elegir si priorizamos la fórmula o el conjunto de índices.

## 7.1 Sumas Famosas

El objetivo es lograr que las sumas se parezcan a estas y luego usar la fórmula cerrada (la de la derecha).

1. **Suma de Gauss**
$$\sum_{k=1}^{n} k \;=\; \frac{n(n+1)}{2}$$

2. **Suma Geométrica**
$$\sum_{k=0}^{n} x^k \;=\; \frac{1 - x^{n+1}}{1 - x} \text{ con } x \neq 1$$

## 7.2 Sumas Múltiples

Definición:

1. **Índices Independientes**

$$\sum_{1\leq j,\, i\leq n} a_{ij} \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}$$

2. **Índices Dependientes**

$$\sum_{1\leq i\lneq j\leq n}^{a_{ij}} = \sum_{i=1}^{n-1}\sum_{j=i+1}^{n} a_{ij} \;=\; \sum_{j=2}^{n}\sum_{i=1}^{j-1} a_{ij}$$

Nota: En sumas de 3 índices dependientes, la letra que está en el medio SIEMPRE se queda en el medio.

## 7.3 Sucesiones

Definición: Una sucesión de elementos de A es una función $f : \mathbb{N} \to A/\ \underbrace{f(1)}_{a_1}, \underbrace{f(2)}_{a_2}, \underbrace{f(3)}_{a_3}, ...$

Notación: $a_n$, con $n \in \mathbb{N}$
Además, pueden definirse de dos maneras:

1. **Definida Explícitamente**

$$a_n \;=\; f(n)$$

2. **Definida Implícitamente**

$$\begin{cases} a_0 = 3 & (\text{"Valor Inicial"}) \\ a_n = 3a_{n-1} \text{ con } n \in \mathbb{N} & (\text{"Relación de Recurrencia"}) \end{cases}$$

   En este caso el objetivo es llegar a la fórmula explícita.

## 7.4 Relaciones de Recurrencia Lineal de Orden K

Definición: Las relaciones de recurrencia lineal son ecuaciones de la forma:

$$\alpha_0(n)a_n + \alpha_1(n)a_{n-1} + ... + \alpha_k(n)a_{n-k} = f(n) \text{ con } \alpha_0 \neq 0 \text{ y } \alpha_k \neq 0$$

Además,

1. Si las funciones $\alpha_j : \mathbb{N} \to \mathbb{C}$ son constantes, entonces se dice que la relación de recurrencia tiene *coeficientes constantes*.

2. Si $f$ es la función nula se dice que la relación de recurrencia lineal es *homogénea*, sino se dice que es *no homogénea*.

3. $\alpha_0(n)a_n + \alpha_1(n)a_{n-1} + ... + \alpha_k(n)a_{n-k} = 0$ es la *relación homogénea asociada* a (11).

4. El *orden* de la relación es la diferencia entre el n más grande y el n más chico.

### 7.4.1 Relaciones de Orden 1

**Relaciones de Recurrencia Lineal de Orden 1 con Coeficientes Constantes Homogéneas**

Definición: Hay dos maneras de definir este tipo de relaciones:

1. *Recursiva*: $X_n + \alpha X_{n-1} = 0$ con $\alpha \in \mathbb{C} - \{0\}$, $n \geq 1$

2. *Explícita*: $X_n = Kr^n$ (El objetivo es llegar de la forma recursiva a la explícita)

**Relaciones de Recurrencia Lineal de Orden 1 con Coeficientes Constantes NO Homogéneas**

Definición: Hay dos maneras de definir este tipo de relaciones:

1. *Recursiva*:

$$\begin{cases} X_n + \alpha X_{n-1} = T & \text{con } \alpha, T \in \mathbb{C} - \{0\},\ n \geq 1 \\ X_0 \end{cases}$$

2. *Explícita*:

$$\begin{cases} X_n = (-1)^n \alpha^n X_0 + T(\frac{(-\alpha)^n - 1}{-\alpha - 1}) & \text{si } \alpha \neq -1 \\ X_n = X_0 + nT & \text{si } \alpha = -1 \end{cases}$$

### 7.4.2 Relaciones de Orden 2

**Relaciones de Recurrencia Lineal con Coeficientes Constantes de Orden 2**

Definición:

$$\begin{cases} X_n + \alpha_1 X_{n-1} + \alpha_2 X_{n-2} = f(n) & \text{con } \alpha_1 \in \mathbb{C}, \alpha_2 \in \mathbb{C} - \{0\}, n \geq 2 \\ X_0,\ X_1 \end{cases}$$

Teorema 7.A

Si $Y_n$ y $Z_n$ son *soluciones de la relación de recurrencia* y además

$$Y_0 = Z_0 \ \wedge \ Y_1 = Z_1 \ \Rightarrow \ Y_n = Z_n \forall n \geq 0$$

**Propiedades**

Sea $X_n + \alpha_1 X_{n-1} + \alpha_2 X_{n-2} = 0$ con $\alpha_1 \in \mathbb{C}, \alpha_2 \in \mathbb{C} - \{0\}, n \geq 2$.
Entonces,

1. $X_n = r^n$ es solución de la ecuación $\Leftrightarrow$ $\underbrace{r^2 + \alpha_1 r + \alpha_2}_{\text{"Polinomio característico de la relación de recurrencia"}} = 0$

2. Si $Y_n$ y $Z_n$ son soluciones de la relación de recurrencia
   $\Rightarrow$ $aY_n + bZ_n$ es solución $\forall a, b \in \mathbb{C}$

3. Si $r^2 + \alpha_1 r + \alpha_2$ tiene 2 raíces distintas $r_1$ y $r_2$
   $\Rightarrow$ la *solución general* de la relación es $X_n = Ar_1^n + br_2^n$ con $A, B \in \mathbb{C}$

4. Si $r^2 + \alpha_1 r + \alpha_2$ tiene una raíz doble $r_1$
   $\Rightarrow$ la *solución general* de la relación $X_n = Ar_1^n + Bnr_1^n$ con $A, B \in \mathbb{C}$

## 7.5 Relaciones de Recurrencia Lineal NO Homógeneas

Teorema 7.B

Sea $Y_n$ la solución general de $X_n + \alpha_1 X_{n-1} + ... + \alpha_k X_{n-k} = f(n)$ y sea $Y_n^p$ una *solución particular* de la misma relación de recurrencia
$\Rightarrow$ $Y_n - Y_n^p$ es solución de la relación de recurrencia homogénea asociada
$\therefore$ La solución general es $Y_n = Y_n^p + Y_n^H$

**Método para hallar una solución particular (Orden 1 ó 2)**

Hay dos casos posibles:

1. $X_n + \alpha X_{n-1} + \beta X_{n-2} = p(n)\lambda^n$
   donde $p(n)$ es un polinomio de grado k y $\lambda \in \mathbb{R} - \{0\}$, vamos a proponer como solución particular:

   $$X_n^p = q(n)\lambda^n n^s$$

   donde $q(n)$ es un polinomio de grado k, y $s$ es la multiplicidad de $\lambda$ como raíz del polinomio característico asociado a la ecuación.

2. $X_n + \alpha X_{n-1} + \beta X_{n-2} = f(n)$
   donde $f(n) = p(n)\lambda^n cos(\alpha n)$ ó $f(n) = p(n)\lambda^n sen(\alpha n)$ siendo $p(n)$ un polinomio de grado k, $\lambda \in \mathbb{R} - \{0\}$, $\alpha \in \mathbb{R} - \{0\}$. Proponemos:

   $$X_n = \lambda^n n^s (q_1(n)cos(\alpha n) + q_2(n)sen(\alpha n))$$

   $q_1(n)$ y $q_2(n)$ son polinomios de grado k, y s es la multiplicidad de $z = cos(\alpha n) + isen(\alpha n)$ como raíz del polinomio característico.

**Solución en Complejos**

$$X_n + \alpha_1 X_{n-1} + \beta X_{n-2} = 0 \text{ con } \alpha \in \mathbb{R},\ \beta \in \mathbb{R} - \{0\}$$

El polinomio característico asociado tiene raíces $a + bi$ y $a - bi$ con $a, b \in \mathbb{R}$. Entonces, la solución general es:

$$X_n = A(a + bi)^n + B(a - bi)^n$$

La solución de arriba está bien pero **hay que escribirla de esta manera**:

$$X_n = |z|^n \left(Ccos(n\theta) + Dsen(n\theta)\right)$$

| Principio de superposición |
|---|
| Si $Y_n$ es una solución particular de $X_n + \alpha X_{n-1} + \beta X_{n-2} = f(n)$ y |
| $Z_n$ es una solución particular de $X_n + \alpha X_{n-1} + \beta X_{n-2} = g(n)$ |
| $\Rightarrow$ $Y_n + Z_n$ es solución particular de $X_n + \alpha X_{n-1} + \beta X_{n-2} = f(n) + g(n)$ |

## 7.6 Relaciones de Recurrencia Lineales de Mayor Orden

$$X_n + \alpha_1 X_{n-1} + ... + \alpha_k X_{n-k} = F(n)$$

La *solución general* es: $X_n = X_n^H + X_n^p$
La *solución particular* es: Análogo a lo visto en 7.5
La *solución homogénea* es:
Propongo $X_n = r^n \Rightarrow r^n + \alpha_1 r^{n-1} + ... + \alpha_k = 0$

1. Cada raíz proporciona tantas soluciones como su multiplicidad
2. Si la raíz $r_i \in \mathbb{R}$ tiene multiplicidad k $\Rightarrow r_i^n, nr_i^n, ..., n^{k-1}r_i^n$ son soluciones.
3. Si la raíz $z = r(cos(\alpha) + isen(\alpha))$ tiene multiplicidad k
   $\Rightarrow r^n cos(n\alpha), r^n sen(n\alpha), nr^n cos(n\alpha), nr^n sen(n\alpha), ..., n^{k-1}r^n cos(n\alpha), n^{k-1}r^n sen(n\alpha)$
   son soluciones.

# 8 Sistemas de Ecuaciones Lineales

Definición:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1k}x_k &= b_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2k}x_k &= b_2 \\ \vdots & \\ a_{n1}x_1 + a_{n2}x_2 + ... + a_{nk}x_k &= b_n \end{cases}$$

Es un sistema lineal con k incógnitas $x_1, x_2, ..., x_k$ con n ecuaciones. Donde $b_j$ son los *términos independientes* y $a_{ik} \in \mathbb{K}$ son los *coeficientes* del sistema.

**Matrices Asociadas al Sistema**

$$\mathrm{A} = \underbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nk} \end{bmatrix}}_{\text{Matriz de coeficientes}} \mathrm{x} = \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}}_{\substack{\text{Vector de} \\ \text{incógnitas}}} \quad \mathrm{b} = \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}}_{\substack{\text{Vector de} \\ \text{términos} \\ \text{independientes}}}$$

Si $b = 0 \Rightarrow \underbrace{\textit{Sistema homogéneo}}_{\text{Siempre tienen solución}}$

Notación:

$$\textit{Matriz ampliada del Sistema} : [A|b] \tag{1}$$

$$\textit{Sistema escrito matricialmente} : Ax = b \tag{2}$$

## 8.1 Operaciones Válidas

Si en un sistema de ecuaciones lineales se realizan las siguientes operaciones se obtiene un *sistema equivalente*(i.e. con el mismo conjunto solución)

1. Intercambiar ecuaciones.
2. Multiplicar una ecuación por un número $\lambda \in \mathbb{K}^*$.
3. Sumar a una ecuación un múltiplo de otra.

En términos de la matriz ampliada del sistema estas operaciones se traducen a lo que llamamos *operaciones elementales*:

1. $F_i \leftrightarrow F_j$
2. $F_i = \lambda F_i$, $\lambda \neq 0$
3. $F_i = F_i + \alpha F_j$

## 8.2 Matrices equivalenetes

### Equivalencia por filas

Defínción: Sean A y B matrices de $n \times k$. Decimos que *A es equivalente por filas a B* si aplicando finitas operaciones elementales a A se obtiene B.
Notación: $A \sim B$

Observaciones

1. A, B de $n \times k$. Entonces,

$$A\mathcal{R}B \text{ si } A \sim B, \text{ R es de equivalencia}$$

2. Si $[A|b] \sim [A'|b'] \Rightarrow Ax = b \wedge A'x = b'$ son equivalentes

Teorema 8.A
Dada una matriz A de $n \times k$, existe una única matriz E en FER/ $A \sim E$

### Forma Escalonada (FE)

Definición: Una matriz A de $n \times k$ está en FE si:

1. En cada fila no nula, el primer numero es un 1 ("uno principal").
2. Cada uno principal de una fila está mas a la derecha que el uno principal de la fila que está arriba.
3. Si hay filas nulas tienen que estar abajo.

### Forma Escalonada Reducida (FER)

Definición: Una matriz A de $n \times k$ está en FER si:

1. Está en FE.
2. En la columna donde está el uno principal todos los demas números son 0.

## 8.3 Métodos de Eliminación

### Método de Eliminiación Gaussiana (MEG)

Defínción: Dada la matriz $[A|b]$ ampliada de un sistema lineal, aplicar el MEG es obtener E *escalonado*/ $[A|b] \sim E$.

### Método de Eliminación de Gauss-Jordan (MEGJ)

Defínción: Dada la matriz $[A|b]$ ampliada de un sistema lineal, aplicar MEGJ es obtener E *escalonado reducido*/ $[A|b] \sim E$.

## 8.4 Rango de una matriz

Definición: Dada A de $n \times k$, el rango de A es la *cantidad de unos principales de la matriz escalonada reducida asociada a A*.
Notación: R(A) = rango(A) = Rg(A)

Observaciones

1. $Rg(A) \leq min\{\underbrace{n}_{\text{filas}}, \underbrace{k}_{\text{columnas}}\}$
2. E', E escalonadas/ $E \sim A \wedge E' \sim A$
   $\Rightarrow$ la cant. de 1s principales de E = la cant. de 1s principales de E'

Corolario de la definción

El Rg(A) es la *cantidad de 1s principales de cualquier matriz E escalonada/* $E \sim A$

## 8.5 Clasificación de los Sistemas Lineales

Sea $[A|b]$ la matriz ampliada de un sistema. Entonces:

1. $Rg(A) = Rg[A|b] \Rightarrow$ "Sistema Compatible" (SC)(i.e. tiene solución)
   (a) $Rg(A)$ = cant. variables/columnas
   $\Rightarrow$ "Sistema Compatible Determinado" (SCD)(i.e. tiene solución única)
   (b) $Rg(A) \neq$ cant. variables/columnas
   $\Rightarrow$ "Sistema Compatible Indeterminado" (SCI)(i.e. tiene infinitas soluciones)
2. $Rg(A) \neq Rg[A|b] \Rightarrow$ "Sistema Incompatible" (SI)(i.e. no tiene solución)

Corolarios

1. Si el sistema es homogéneo $\Rightarrow$ el sistema es compatible
2. La compatibilidad o incompatibilidad depende de A y de b. Puede pasar que $Ax = b_1$ sea compatible y que $Ax = b_2$ sea incompatible.
3. Si $Ax = b_1$ es compatible $\wedge$ $Ax = b_2$ es compatible
   $\Rightarrow$ ambos son SCD $\vee$ ambos son SCI

Nota: cant. de variables libres = cant. variables - Rg(A)

# 9 Matrices

Definición: $\mathbb{K}^{n\times m} = \{A/\ A \text{ es un conjunto con n filas y m columnas con coeficientes en } \mathbb{K}\}$

**Matriz Identidad**: $I_n \in \mathbb{R}^{n\times m}/\ (I_n)_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$

**Matriz Nula**: $0_{ij} = 0$

## 9.1 Operaciones entre matrices

1. **Producto por escalar**
   Si $A \in \mathbb{K}^{n\times m}$, $\alpha \in \mathbb{K}$. Entonces,

   $$B = \alpha A \in \mathbb{K}^{n\times m} \Leftrightarrow B_{ij} = \alpha A_{ij}$$

2. **Suma**
   $A, B \in \mathbb{K}^{n\times m}$. Entonces,

   $$C = A + B \in \mathbb{K}^{n\times m} \Leftrightarrow C_{ij} = A_{ij} + B_{ij}$$

3. **Producto**
   $A \in \mathbb{K}^{n\times m} \wedge B \in \mathbb{K}^m \times r$ (es decir, el nro de columnas de A TIENE que coincidir con el de filas de B, o viceversa). Entonces,

   $$C = A * B \Leftrightarrow C_{ij} = \sum_{k=1}^{m} A_{ik} * B_{kj}$$

   Osea se multiplica la *Fila de A con la Columna de B.*

### Propiedades

Sean $A, B, C$ matrices, $\alpha, \beta \in \mathbb{K}$. Entonces,

1. $A + B = B + A$
2. El producto entre matrices *NO siempre es conmutativo.*
3. $A + (B + C) = (A + B) + C$
4. $A + 0 = A$
5. Para cada $A \in \mathbb{K}^{n\times m}$, $\exists(-A) \in \mathbb{K}^{n\times m}/\ A + (-A) = 0$
6. $A * (B * C) = (A * B) * C$
7. $A * I = A$, $I * A = A$
8. $A * 0 = 0$, $0 * A = 0$
9. $A * (B + C) = A * B + A * C$ y $(B + C) * A = B * A + B * C$

10. $\alpha * (A + B) = \alpha * A + \alpha * B$
11. $\alpha * (A * B) = (\alpha * A) * B$
12. $(\alpha + \beta) * A = \alpha * A + \beta * A$
13. $\alpha * A = A * \alpha$
14. $(-1) * A = -A$
15. $(\alpha * A)^t = \alpha * A^t$
16. $(A + B)^t = A^t + B^t$
17. $(A * B)^t = B^t * A^t$
18. $(A^k)^t = (A^t)^k \ \forall k \in \mathbb{N}$

## 9.2 Otros tipos de matrices

1. **Matriz Diagonal**
   $A \in \mathbb{K}^{n \times m}$ es diagonal si $A_{ij} = 0$ si $i \neq j$
2. **Matriz Triangular Superior**
   $A \in \mathbb{K}^{n \times m}$ es triangular superior si $A_i j = 0$ cuando $i \gneq j$
3. **Matriz Triangular Inferior**
   $A \in \mathbb{K}^{n \times m}$ es triangular inferior si $A_i j = 0$ cuando $i \lneq j$
4. **Matriz Traspuesta**
   $A \in \mathbb{K}^{n \times m}$ se define $A^t \in \mathbb{K}^{n \times m} / \ (A^t)_{ij} = A_{ji}$
5. **Matriz Simétrica**
   $A \in \mathbb{K}^{n \times n}$ es simétrica si $A^t = A$
6. **Matriz Antisimétrica**
   $A \in \mathbb{K}^{n \times n}$ es antisimétrica si $A^t = -A$. Además, en la *diagonal tiene que haber solo 0s.*

## 9.3 Inversas

Definición: Sea $A \in \mathbb{K}^{n \times n}$, decimos que $B \in \mathbb{K}^{n \times n}$ *es inversa de* $A$ si:

$$A * B = Id \ \wedge \ B * A = Id$$

Además, decimos que $A \in \mathbb{K}^{n \times n}$ *es inversible* si tiene inversa.
Notación: $A^{-1}$ es la inversa de $A$, y viceversa.

| Teorema 9.A |
| --- |
| $A$ inversible $\Rightarrow$ $A$ tiene una única inversa |

Teorema 9.B

Sea $A \in \mathbb{K}^{n \times n}$ inversible. Entonces,

$Ax = b$ es SCD y Sol=$\{A^{-1} * b\}$

Corolario

Sea $A \in \mathbb{K}^{n \times n}$, $Rg(A) \lneq n \Rightarrow$ $A$ no es inversible

Teorema 9.C

Sea $A \in \mathbb{K}^{n \times n} \wedge Rg(A) = n \Rightarrow$ $A$ es inversible

Teorema 9.D

$A, B \in \mathbb{K}^{n \times n}$ inversibles. Entonces,

$A * B$ es inversible y $(A * B)^{-1} = B^{-1} * A^{-1}$

Teorema 9.E

$A, B \in \mathbb{K}^{n \times n}$ inversibles $\wedge A * B$ inversible $\Rightarrow \exists A^{-1}, B{-}1$

**Resumen del resumen**

Sea $A \in \mathbb{K}^{n \times n}$ (A matriz cuadrada). Son equivalentes:

1. $Rg(A) = n$
2. $A$ es inversible
3. $Ax = b$ es SCD
4. $Ax = 0$ es SCD
5. $A \sim Id$

## 9.4 Cheatsheet de producto de matrices

Esto es útil para encontrar contraejemplos.

1. $$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix} \quad F_1 \leftrightarrow F_2$$
2. $$\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha a & \alpha b \\ c & d \end{bmatrix} \quad F_1 = \alpha F_1$$

3.
$$\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ \alpha a + c & \alpha b + d \end{bmatrix} \quad F_2 = \alpha F_1 + F_2$$

4.
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha a & b \\ \alpha c & d \end{bmatrix} \quad C_1 = \alpha C_1$$

5.
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix} = \begin{bmatrix} a + \alpha b & b \\ c + \alpha d & d \end{bmatrix} \quad C_1 = \alpha C_2 + C_1$$

# 10 Espacios Vectoriales

Defincián: Un espacio vectorial es una estrucutura algebraica que consta de dos conjuntos y dos operaciones ($V$, $\mathbb{K}$, $\oplus$, $\otimes$).

- Los elementos de V se llaman *vectores*.
- Los elementos de $\mathbb{K}$ se llaman *escalares*. ($\mathbb{K}$ es un cuerpo / $\mathbb{K} = \mathbb{R}$ ó $\mathbb{C}$)

Las operaciones deben cumplir que:

$$\oplus : V \times V \to V$$

$$\otimes : \mathbb{K} \times V \to V$$

Para que una estructura se considere espacio vectorial tiene que cumplir 8 propiedades:

1. $u \oplus v = v \oplus u$
2. $u \oplus (v \oplus w) = (u \oplus v) \oplus w$
3. $\exists 0 \in V / \, V \oplus 0 = V$ (0 denota el elemento neutro de la suma)
4. Dado $v \in V$, $\exists (-v) \in V / \, v \oplus (-v) = 0$
5. $1 \otimes V = V$, $1 \in \mathbb{K}$ (1 denota el neutro de la multiplicación)
6. $\alpha \otimes (v \oplus w) = \alpha \otimes v \oplus \alpha \otimes w$
7. $(\alpha + \beta) \otimes v = \alpha \otimes v \oplus \beta \otimes v$
8. $(\alpha * \beta) \otimes v = \alpha \otimes (\beta \otimes v)$

Notación: V es un $\mathbb{K}$-ev ("V es un $\mathbb{K}$ espacio vectorial")

**Propiedades de los espacios vectoriales**

1. El neutro para la suma *es único*.
2. $0 * v = 0_v$ con $0, 0_v \in \mathbb{K}$
3. $\alpha * 0_v = 0_v$
4. $\alpha * v = 0 \;\Rightarrow\; \alpha = 0 \;\vee\; v = 0_v$
5. El opuesto de un vector *es único*.
6. $(-1) * v = -v$ con $(-1) \in \mathbb{K}$, $v, -v \in V$
7. $\alpha * \sum_{i=1}^{r} v_i = \sum_{i=1}^{r} \alpha * v_i$ con $\alpha \in \mathbb{K}$, $v_i \in V$

## 10.1 Subespacios Vectoriales

Defínción: Sea V un $\mathbb{K}$-ev con operaciones $\otimes$, $\oplus$. Decimos que *$S$ es un subespacio de $V$* si:

1. ($S$, $\mathbb{K}$, $\oplus$, $\otimes$) es un espacio vectorial.
2. $S \subseteq V$

Teorema 10.A
Sea V un $\mathbb{K}$-ev. S es un subespacio de V si:

1. $S \subseteq V$
2. $0_v \in S$
3. $v, w \in S \Rightarrow v + w \in S$
4. $\alpha \in \mathbb{K}$, $v \in S \Rightarrow \alpha * v \in S$

## 10.2 Combinación Lineal

Defínción: Dado V un $\mathbb{K}$-ev. Sean $v_1$, $v_2$, ..., $v_n \in V$, $w \in V$. Decimos que *$w$ es combinación lineal de $v_1$, ..., $v_n$* si existen $\alpha_1$, ...$\alpha_n \in \mathbb{K}$ tal que:

$$w = \alpha_1 * v_1 + \alpha_2 * v_2 + ... + \alpha_n * v_n = \sum_{i=1}^{n} \alpha_i * v_i$$

## 10.3 Espacio generado por un conjunto de vectores

Definición: Sea V un $\mathbb{K}$-ev. Sea $G = \{v_1, ..., v_n\} \subseteq V$. Entonces,

$$gen(G) = gen\{v_1, ..., v_n\} = \{v \in V / \text{ v es combinación lineal de los elementos de G } \} =$$
$$= \{v \in V / \exists \alpha_1, ..., \alpha_n \in \mathbb{K} \text{ tal que } v = \sum_{i=1}^{n} \alpha_i v_i\}$$

Teorema 10.B
V es un $\mathbb{K}$-ev. Sea $G = \{v_1, ..., v_r\} \subseteq V$. Entonces $S = gen(G)$ es un subespacio de V.

## 10.4 Conjunto generador de un subespacio

Defínción: V un $\mathbb{K}$-ev. El conjunto $G = \{v_1, ..., v_r\}$ es un conjunto generador del subespacio $S \subseteq V$ si $S = gen\{v_1, ...v_r\}$

Teorema 10.C
V es un $\mathbb{K}$-ev.

$$gen\{v_1, ..., v_r\} = gen\{v_1, v_r, v_{r+1}\} \Leftrightarrow v_{r+1} \in gen\{v_1, ..., v_3\}$$

## 10.5 Independecia/Dependencia Lineal

Definciones:

- El conjunto $\{v_1, v_2, ..., v_r\}$ es *linealmente independendiente* (li) si:

$$\alpha_1 * v_1 + \alpha_2 * v_2 + ... + \alpha_r v_r = 0_v \Rightarrow \alpha_i = 0 \text{ con } 1 \leq i \leq r$$

$$v_j \in V, \alpha_j \in \mathbb{K} \text{ con } 1 \leq j \leq r$$

- El conjunto $\{v_1, v_2, ..., v_r\}$ es *linealmente dependiente* (ld) si no es li.

Teorema 10.D
Sea $\{v_1, ..., v_r\} \subseteq V$ con $r \geq 2$. Entonces:

1. $\{v_1, ..., v_r\}$ es ld $\Leftrightarrow \exists v_i$ con $1 \leq i \leq r /$ $v_i$ es combinación lineal del resto
2. $\{v_1, ..., v_r\}$ es li $\Leftrightarrow$ ningún $v_i$ es combinación lineal del resto

Corolario
Sea $G = \{v_1, ..., v_r\}$ con $r \geq 2$. Entonces:
Existe $G_1 \subsetneq G$ tal que $gen(G) = gen(G_1) \Leftrightarrow$ G es ld

Observaciones

1. $\{v_1, ..., v_r\}$ es ld si algún $v_i = 0$
2. $\{v\}$ es li $\Leftrightarrow v \neq 0$
3. $Rg(A) = n \Rightarrow$ SCD $\Rightarrow$ es li

## 10.6 Base

Defnición: V un $\mathbb{K}$-ev. $\{v_1, ...v_n\} \subseteq V$. Decimos que *B es base de V* si:

1. $V = gen(B)$
2. B es li

Teorema 10.E

Sea $G = \{v_1, ..., v_r\}$ un conjunto generador de $S \neq \{0\}$. Entonces, existe $B \subseteq G / B$ es base de $S$.

Teorema 10.F

V un $\mathbb{K}$-ev. Sea $B = \{v_1, ..., v_r\}$ base de V. Entonces,

$$\forall v \in V, \exists! \, \alpha_1, ..., \alpha_r \in \mathbb{K} / \, v = \alpha_1 * v_1 + ... + \alpha_r * v_r$$

Teorema 10.G

V un $\mathbb{K}$-ev. Sea $B = \{v_1, ..., v_r\}$ base de V. Entonces,

$$\text{Si } \{w_1, ..., w_n\} \subseteq V \ \wedge \ n \gneq r \ \Rightarrow \ \{w_1, ..., w_n\} \text{ es ld}$$

Teorema 10.H

V un $\mathbb{K}$-ev.

$$B = \{v_1, ..., v_r\} \text{ y } B' = \{v'_1, ..., v'_n\} \text{ bases de V} \ \Rightarrow \ r = n$$

Observación: Puede haber infinitas bases para un conjunto pero esas infinitas bases tienen la misma cantidad de elementos.

**Dimensión de una base**

Definición: V un $\mathbb{K}$-ev. Sea $B = \{v_1, ..., v_r\}$ base de V. Se define la *dimensión de $V$* igual a n. Notación: $dim(V) = n$

Teorema 10.I

V un $\mathbb{K}$-ev. $dim(V) = n$.
Son equivalentes:

1. $gen\{v_1, ..., v_n\} = V$
2. $\{v_1, ..., v_n\} \subseteq V$
3. $\{v_1, ..., v_n\}$ es li

Nota: Esto sirve para probar que un conjunto determinado es base de otro sin tener que buscar generadores.

# Resumen de todas las propiedades

## 1 Conjuntos

1. *Leyes de De Morgan*

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

2. *Leyes Distributivas*

$$A \cap B(B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup B(B \cap C) = (A \cup B) \cap (A \cup C)$$

3. *Ley Conmutativa*

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

4. *Ley Asociativa*

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C)$$

5. *Otras*

$$A \cup \varnothing = A$$
$$A \cap \varnothing = \varnothing$$
$$A \cup \mathcal{U} = \mathcal{U}$$
$$A \cap \mathcal{U} = A$$
$$\overline{\varnothing} = \mathcal{U}$$
$$\overline{\mathcal{U}} = \varnothing$$

## 5 Enteros

### 5.2 Divisibilidad en un anillo

1. $a \leq b \Rightarrow a + c \leq b + c$
2. $a \leq b \wedge c \gneq 0 \Rightarrow ac \leq bc$
3. $ab = ac \wedge a \neq 0 \Rightarrow b = c$
4. $ab = 0 \Rightarrow a = 0 \vee b = 0$
5. $a|b \Leftrightarrow |a||b|$
6. $a|b \wedge b \neq 0 \Rightarrow |a| \leq |b|$

7. $a|b \wedge b|a \Rightarrow |a| = |b|$
8. $a|b \wedge a|c \Rightarrow a|b \pm c$
9. $a|b \wedge a|b \pm c \Rightarrow a|c$
10. $a|b \Rightarrow a|bc$
11. $a|b \Rightarrow a^n|b^n$ con $n \in \mathbb{N}$
12. $a|b \wedge a|c \Rightarrow a|\alpha b + \beta c$ con $\alpha, \beta \in \mathbb{Z}$

### 5.3 Congruencias

1. $a_1 \equiv b_1(m) \wedge a_2 \equiv b_2(m) \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2(m)$
   $a_1 \equiv b_1(m) \wedge a_2 \equiv b_2(m) \Rightarrow a_1 * a_2 \equiv b_1 * b_2(m)$
2. $a_1 \equiv b_1(m) \wedge ... \wedge a_k \equiv b_k(m) \Rightarrow a_1 \pm ... \pm a_k \equiv b_1 \pm ... \pm b_k(m)$
   $a_1 \equiv b_1(m) \wedge ... \wedge a_k \equiv b_k(m) \Rightarrow a_1 * ... * a_k \equiv b_1 * ... * b_k(m)$
3. $a \equiv b(m) \Rightarrow a^n \equiv b^n(m) \; \forall n \in \mathbb{N}$
4. $a \equiv b(m) \Rightarrow ac \equiv bc(m)$

### 5.5 Números Coprimos

1. $a \perp b \wedge a|bc \Rightarrow a|c$
2. $a \perp b \wedge a \perp c \Rightarrow a \perp bc$
3. $a|c \wedge b|c \wedge a \perp c \Rightarrow ab|c$
4. $d = (a : b) \Rightarrow \frac{a}{d} \perp \frac{b}{d}$
5. $a \perp b \Rightarrow a^n \perp b^k$ con $n, k \in \mathbb{N}$
6. $a \perp c \Rightarrow (a : cb) = (a : b)$

#### 5.6.1 $V_p$

1. $V_p(a * b) = V_p(a) + V_p(b)$
2. $V_p(a^n) = nV_p(a)$
3. $d|a \Rightarrow V_p(d) \leq V_p(a)$
4. $V_p \geq 0$

# 6 Polinomios

## 6.2 Divisivibilidad

1. $g \neq 0$, $g|0$
2. $g|f \Leftrightarrow cg|f$ con $c \in \mathbb{K} - \{0\} = \mathbb{K}^*$
3. $g|f \Leftrightarrow \frac{g}{cp(g)}|\frac{f}{cp(f)}$ con $f \neq 0$
4. $g|f \Leftrightarrow g|cf$ con $c \in \mathbb{K}^*$
5. $f$, $g$ no nulos, $g|f \wedge gr(g) = gr(f) \Rightarrow \exists c \in \mathbb{K}^* / f = cg$
6. $f|g \wedge g|f \Rightarrow f = cg$ con $c \in \mathbb{K}^*$
7. $f \notin \mathbb{K}$, $c|f \wedge cf|f$ si $c \in \mathbb{K}^*$. Es decir, f tiene como divisores cualquier constante y múltiplos de él mismo.

## 6.3 MCD

1. $(f : 0) = \frac{f}{cp(f)} \, \forall f \in \mathbb{K}_{[x]}$
2. $(f : g) = (g : r_g(f)) \, \forall g \in \mathbb{K}_{[x]}$, $g$ no nulo.

## 6.5 Polinomios Coprimos

1. $g \perp h$, $g|f \wedge h|f \Leftrightarrow gh|f$
2. $g \perp h$, $g|hf \Leftrightarrow g|f$

## 6.6 Evaluación

1. $(f + g)_{(x)} = f_{(x)} + g_{(x)}$
2. $(f * g)_{(x)} = f_{(x)} * g_{(x)}$

## 6.10 Multiplicidad de una raíz

1. a es raíz múltiple de $f \Leftrightarrow f(a) = 0 \wedge f'(a) = 0$
2. a es raíz simple de $f \Leftrightarrow f(a) = 0 \wedge f'(a) \neq 0$

# 7 Sumas - Recurrencias

1. **Ley distributiva**

$$\sum_{k=i}^{n} c.a_k = c \sum_{k=i}^{n} a_k$$

2. **Ley Asociativa**

$$\sum_{k=i}^{n}(a_k + b_k) \;=\; \sum_{k=i}^{n} a_k + \sum_{k=i}^{n} b_k$$

3. **Ley Conmutativa**

$$\sum_{k=i}^{n} a_k \;=\; \sum_{k=i}^{n} a_{p(k)}$$

siendo $p : I \to I$ una *función biyectiva*, $I = i, i+1, ..., n$

4. **Cambio de Índice**

$$\sum_{k\in I} a_k \;=\; \sum_{j\in J} a_{g(j)}$$

siendo $g : J \to I$" una *función biyectiva*, y $J, I$ conjuntos finitos.
Esta propiedad nos permite elegir si priorizamos la fórmula o el conjunto de índices.

### 7.4.2 Relaciones de Orden 2

Sea $X_n + \alpha_1 X_{n-1} + \alpha_2 X_{n-2} = 0$ con $\alpha_1 \in \mathbb{C}, \alpha_2 \in \mathbb{C} - \{0\}, n \geq 2$.
Entonces,

1. $X_n = r^n$ es solución de la ecuación $\Leftrightarrow$ $\underbrace{r^2 + \alpha_1 r + \alpha_2}_{\substack{\text{"Polinomio característico}\\ \text{de la relación de recurrencia"}}} = 0$

2. Si $Y_n$ y $Z_n$ son soluciones de la relación de recurrencia
$\Rightarrow$ $aY_n + bZ_n$ es solución $\forall a, b \in \mathbb{C}$

3. Si $r^2 + \alpha_1 r + \alpha_2$ tiene 2 raíces distintas $r_1$ y $r_2$
$\Rightarrow$ la *solución general* de la relación es $X_n = Ar_1^n + br_2^n$ con $A, B \in \mathbb{C}$

4. Si $r^2 + \alpha_1 r + \alpha_2$ tiene una raíz doble $r_1$
$\Rightarrow$ la *solución general* de la relación $X_n = Ar_1^n + Bnr_1^n$ con $A, B \in \mathbb{C}$

### 9.1 Operaciones entre matrices

Sean $A, B, C$ matrices, $\alpha, \beta \in \mathbb{K}$. Entonces,

1. $A + B \;=\; B + A$

2. El producto entre matrices *NO siempre es conmutativo.*

3. $A + (B + C) = (A + B) + C$

4. $A + 0 = A$

5. Para cada $A \in \mathbb{K}^{n\times m}$, $\exists(-A) \in \mathbb{K}^{n\times m} / \; A + (-A) = 0$

6. $A * (B * C) = (A * B) * C$
7. $A * I = A$, $I * A = A$
8. $A * 0 = 0$, $0 * A = 0$
9. $A * (B + C) = A * B + A * C$ y $(B + C) * A = B * A + B * C$
10. $\alpha * (A + B) = \alpha * A + \alpha * B$
11. $\alpha * (A * B) = (\alpha * A) * B$
12. $(\alpha + \beta) * A = \alpha * A + \beta * A$
13. $\alpha * A = A * \alpha$
14. $(-1) * A = -A$
15. $(\alpha * A)^t = \alpha * A^t$
16. $(A + B)^t = A^t + B^t$
17. $(A * B)^t = B^t * A^t$
18. $(A^k)^t = (A^t)^k \ \forall k \in \mathbb{N}$

## 10 Espacios Vectoriales

### Propiedades de los espacios vectoriales

1. El neutro para la suma *es único*.
2. $0 * v = 0_v$ con $0, 0_v \in \mathbb{K}$
3. $\alpha * 0_v = 0_v$
4. $\alpha * v = 0 \ \Rightarrow \ \alpha = 0 \ \vee \ v = 0_v$
5. El opuesto de un vector *es único*.
6. $(-1) * v = -v$ con $(-1) \in \mathbb{K}$, $v, -v \in V$
7. $\alpha * \sum_{i=1}^{r} v_i = \sum_{i=1}^{r} \alpha * v_i$ con $\alpha \in \mathbb{K}$, $v_i \in V$