MA1101-3 Introducción al Álgebra
Profesor: Pablo R. Dartnell R.
Auxiliar: Felipe Hernández Castro

Resumen Final

Junio de 2019

1.-Logica Proposicional

- **[Tautologías básicas]**: Las siguientes proposiciones son tautologías:

  a) ***Dominancia***: $p \vee V \Leftrightarrow V, \quad p \wedge F \Leftrightarrow F$
  b) ***Identidad***: $p \wedge V \Leftrightarrow p, \quad p \vee F \Leftrightarrow p$
  c) ***Idempotencia***: $p \wedge p \Leftrightarrow p, \quad p \vee p \Leftrightarrow p$
  d) ***Doble negación***: $\neg(\neg p) \Leftrightarrow p$
  e) ***Tercio excluso***: $p \vee \overline{p} \Leftrightarrow V$
  f) ***Consistencia***: $p \wedge \overline{p} \Leftrightarrow F$
  g) ***Absorción***: $p \vee (p \wedge q) \Leftrightarrow p, \quad p \wedge (p \vee q) \Leftrightarrow p$
  h) ***Relajación***: $p \wedge q \Rightarrow p, \quad p \Rightarrow p \vee q$
  i) ***Caracterización de la implicancia***: $(p \Rightarrow q) \Leftrightarrow \overline{p} \vee q$

- **[Álgebra Booleana]**: Son tautologías:

  - ***Leyes de De Morgan:***
    $\overline{p \wedge q} \Leftrightarrow \overline{p} \vee \overline{q}, \quad \overline{p \vee q} \Leftrightarrow \overline{p} \wedge \overline{q}$
  - ***Conmutatividad:***
    Del $\vee$: $p \vee q \Leftrightarrow q \vee p$
    Del $\wedge$: $p \wedge q \Leftrightarrow q \wedge p$
  - ***Asociadtividad***
    Del $\vee$: $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
    Del $\wedge$: $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
  - ***Distributividad***
    Del $\wedge$ con respecto al $\vee$:
    $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
    Del $\vee$ con respecto al $\wedge$:
    $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

- **[Tautologías relevantes]**: Otras tautologías a tener en cuenta son:

  a) ***Doble implicancia***: $(p \Leftrightarrow q) \iff (p \Rightarrow q) \wedge (q \Rightarrow p)$
  b) ***Modus Ponens***: $p \wedge (p \Rightarrow q) \Rightarrow q$
  c) ***Transitividad***: $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
  d) ***Contrareciproca***: $(p \Rightarrow q) \iff (\overline{q} \Rightarrow \overline{p})$
  e) ***Contradicción***:
     - Forma 1: $q \iff (\overline{q} \implies F)$
     - Forma 2: $[(p \Rightarrow q) \Leftrightarrow V] \Leftrightarrow [p \wedge \overline{q}] \Rightarrow F$

- **[Negación de cuantificadores]**:

  a) $\overline{(\exists x)p(x)} \Leftrightarrow (\forall x)\overline{p(x)}$
  b) $\overline{(\forall x)p(x)} \Leftrightarrow (\exists x)\overline{p(x)}$

- **[Existencia y unicidad]**: Se define el cuantificador de existencia y unicidad $(\exists!)$ como sigue:

$$(\exists! x)p(x) \Leftrightarrow [(\exists x)p(x)] \wedge [(\forall x)(\forall y)\{(p(x) \wedge p(y)) \Rightarrow (x = y)\}]$$

2.-Inducción

- **[Principio de inducción]**: Sea $n_0 \in \mathbb{N}$ y $P(n)$ una función proposicional, se tiene que la proposición:

$$\forall n \geq n_0, P(n) \tag{1}$$

Es equivalente a:

$$\underbrace{P(n_0)}_{\textit{Caso base}} \wedge \ [\forall n \geq n_0, \ \underbrace{P(n)}_{\textit{H.I. (débil)}} \ \Rightarrow P(n+1)]$$

Observación: Este tipo de inducción también es conocida como inducción débil.

- **[Principio de inducción Fuerte]**: También tenemos que la proposición (1) es equivalente a:

$$\underbrace{P(n_0)}_{\textit{Caso base}} \wedge \ [\forall n \geq n_0, \underbrace{P(n_0) \wedge \cdots \wedge P(n)}_{\textit{H.I. (fuerte)}} \Rightarrow P(n+1)]$$

Esta inducción es llamada inducción fuerte pues ocupa completamente la hipótesis inductiva.

3.-Conjuntos

- **[Nociones básicas]**:
  - ***Conjunto Referencia***: Es el conjunto al cual pertenecen todos los elementos con los que se va a trabajar. Si denotamos E al conjunto de referencia, tenemos que $x \in E$ es siempre verdad.
  - ***Conjunto vacío***: Se define el conjunto $\emptyset$ como el conjunto que no posee elementos, es decir $x \in \emptyset$ es siempre falso.
- **[Definiciones Básicas]**: Sean A y B conjuntos, se define:
  - *Igualdad:*
    $A = B \Leftrightarrow (\forall x \in E,\ x \in A \Leftrightarrow x \in B)$
  - *Inclusión:*
    $A \subseteq B \Leftrightarrow (\forall x \in E,\ x \in A \Rightarrow x \in B)$
  - *Unión:*
    $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$
  - *Intersección:*
    $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$
  - *Complemento:*
    $x \in A^c \Leftrightarrow x \notin A$
  - *Diferencia:*
    $A \setminus B := A \cap B^c$
  - *Diferencia simétrica:*
    $A \triangle B := A \setminus B \cup B \setminus A = (A \cup B) \setminus (A \cap B)$
- **[Propiedades de inclusión]**: Sean $A, B, C, D \subseteq E$ conjuntos:
  a) $\emptyset \subseteq A \subseteq E$
  b) $A \cap B \subseteq A \subseteq A \cup B$
  c) Si $A \subseteq C$ y $B \subseteq D$ entonces $A \cap B \subseteq C \cap D$ y $A \cup B \subseteq C \cup D$
- **[Propiedades de igualdad]**: Sean $A, B \subseteq E$ conjuntos:
  a) $A \cup \emptyset = A, \quad A \cap \emptyset = \emptyset$
  b) $A \cup E = E, \quad A \cap E = A$
  c) $(A^c)^c = A, \quad A \cap A^c = \emptyset, \quad A \cup A^c = E$
  d) *Ley de De Morgan*
     - $(A \cup B)^c = A^c \cap B^c$
     - $(A \cap B)^c = A^c \cup B^c$
- **[Equivalencias útiles]**: Son equivalentes:
  I) $A \subseteq B$
  II) $B^c \subseteq A^c$
  III) $A \cap B^c = \emptyset$
  IV) $B \cup A^c = E$
- **[Producto Cartesiano]**: Para $A \subseteq E$ y $B \subseteq F$ se define el conjunto $A \times B$ como: $A \times B := \{(a,b) | a \in A \wedge b \in B\}$
- **[Algunas propiedades]**: Sí $A_1, A_2 \subseteq E$ y $B_1, B_2 \subseteq F$ entonces:
  1. $A_1 \times \emptyset = \emptyset \times B_1 = \emptyset$
  2. $A_1 \subseteq A_2$ y $B_1 \subseteq B_2 \Longrightarrow A_1 \times B_1 \subseteq A_2 \times B_2$
  3. $(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$
  4. $(A_1 \times B_1) \cup (A_2 \times B_2) \subseteq (A_1 \cup A_2) \times (B_1 \cup B_2)$
- **[Conjunto potencia]**: Se define el conjunto potencia (o tambien llamado conjunto de las partes) $\mathcal{P}(A)$ al conjunto de todos los subconjuntos de A:

  $$\mathcal{P}(A) = \{X \subseteq E | X \subseteq A\}$$

  Obs. : $\emptyset \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$ siempre.
- **[Unión e intersección de Conjuntos potencia]**:
  1. $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
  2. $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cup B)$
- **[Partición de conjuntos]**: Llamaremos a $\mathcal{C} \subset \mathcal{P}(A)$ partición de A si se cumple:
  - $\forall C \in \mathcal{C}, C \neq \emptyset$
  - $\forall C_1, C_2 \in \mathcal{C}$ si $C_1 \neq C_2$, entonces $C_1 \cap C_2 = \emptyset$
  - $\mathcal{C}$ cubre A: $\bigcup\limits_{C \in \mathcal{C}} C = A$

4.- Funciones

- **[Definición Función]**: Una función de A a B ($f : A \longrightarrow B$) es una 3-tupla $f = (A, B, G)$ que satisface:
  - $G \subseteq A \times B$
  - $\forall a \in A, \exists! b \in B,\ (a,b) \in G$

  Obs. : Para clarificar conceptos:
  - Podemos escribir $b = f(a)$ pues b -dado a- posee un unico valor.
  - $G = \{(a,b) \in A \times B \mid b = f(a)\} = \{(a, f(a)) \in A \times B \mid a \in A\}$
  - A es llamado dominio de f ($Dom\ f$) y B codominio de f ($Cod\ f$).

- **[Igualdad de Funciones]**: Si $f : A \longrightarrow B$ y $g : C \longrightarrow D$ son funciones, entonces $f = g$ si y solo si:
  - $Dom\ f = Dom\ g$
  - $Cod\ f = Cod\ g$
  - $\forall x \in Dom\ f, f(x) = g(x)$

  Obs. : Esta definición de igualdad nos dice básicamente que ambas 3-tuplas son iguales: $(A, B, G_f) = (C, D, G_g)$
- **[Inyectividad]**: Diremos que una función $f : A \to B$ es inyectiva si:
$$\forall x_1, x_2 \in A,\ f(x_1) = f(x_2) \Longrightarrow x_1 = x_2$$
- **[Epiyectividad]**: Diremos que una función $f : A \to B$ es epiyectiva si:
$$\forall y \in B, \exists x \in A,\ y = f(x)$$
- **[Biyectividad]**: Diremos que una función $f : A \to B$ es biyectiva si es epiyectiva e inyectiva a la vez, o equivalentemente:
$$\forall y \in B, \exists! x \in A,\ y = f(x)$$
- **[Inversa]**: Dada $f : A \to B$, se define $f^{-1} : B \to A$ como:
$$\forall x \in A, \forall y \in B, f^{-1}(y) = x \Leftrightarrow y = f(x)$$

  Observación:
  - $\forall x \in A, f^{-1}(f(x)) = x$
  - $\forall y \in B, f(f^{-1}(y)) = y$
- **[Composición]**: Dadas $f : A \to B$ y $g : B \to C$, se define $g \circ f$ como:
$$\forall x \in A, (g \circ f)(x) = g(f(x))$$

  Observación: La composición asocia: $h \circ (g \circ f) = (h \circ g) \circ f$
- **[Propiedades con la composición]**: Dadas $f : A \to B$ y $g : B \to C$:
  a) Si f y g son inyectivas (epiyectivas, biyectivas respectivamente) entonces $g \circ f$ es inyectiva (epiyectiva, biyectiva respectivamente)
  b) Si $g \circ f$ inyectiva entonces f inyectiva
  c) Si $g \circ f$ epiyectiva entonces g es epiyectiva
- **[Teorema de la inversa]**: Sean $f : A \to B$ y $g : B \to A$. Tenemos que f es biyectiva con inversa g si se satisfacen al menos 2 de las siguientes condiciones:
  - $g \circ f = id_A$
  - $f \circ g = id_B$
  - g es biyectiva
- **[Inversa de a composición]**: Si $f : A \to B$ y $g : B \to C$ biyectivas, entonces
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$
- **[Conjunto Imagen]**: Sea $f : A \longrightarrow B$ función, y $C \subseteq A$. Se define el conjunto imagen de C por f:
$$f(C) = \{f(x) \in B \mid x \in C\}$$
- **[Equivalencia epiyectividad]**: $f : A \longrightarrow B$ es epiyectiva si y solo si $f(A) = B$
- **[Propiedades Imagen]**:
  i) $A \subseteq C \Longrightarrow f(A) \subseteq f(C)$
  ii) $f(A \cap C) \subseteq f(A) \cap f(C)$
  iii) $f(A \cup C) = f(A) \cup f(C)$
- **[Conjunto Preimagen]**: Sea $f : A \longrightarrow B$ función, y $D \subseteq B$. Se define el conjunto preimagen de D por f:
$$f^{-1}(D) = \{x \in A \mid f(x) \in D\}$$
- **[Propiedades PreImagen]**:
  i) $B \subseteq D \Longrightarrow f^{-1}(B) \subseteq f^{-1}(D)$
  ii) $f^{-1}(B \cap D) = f(B) \cap f^{-1}(D)$
  iii) $f^{-1}(B \cup D) = f^{-1}(B) \cup f^{-1}(D)$
- **[Inclusiones relevantes]**: Sea $f : A \longrightarrow B$, con $C \subseteq A$ y $D \subseteq B$, entonces:
  - $C \subseteq f^{-1}(f(C))$
  - $f(f^{-1}(D)) = D \cap f(A)$ En particular: $f(f^{-1}(D)) \subseteq D$
- **[Inyectividad y sobreyectividad]**: Sea $f : A \longrightarrow B$ función. Se tiene:
  i) f es inyectiva si y solo si:
$$\forall y \in B, f^{-1}(\{y\}) = \emptyset \vee (\exists! x \in A, f^{-1}(\{y\}) = \{x\}$$
  ii) f es epiyectiva si y solo si:
$$\forall y \in B, f^{-1}(\{y\}) \neq \emptyset$$

III) f si es biyectiva, entonces:

$$\forall C \subseteq B, f^{-1}(\{y\}) = (\{f^{-1}(y)\})$$

5.- Relaciones

- **[Relación]**: Es una tripleta $(A, B, \mathcal{R})$ que cumple $\mathcal{R} \subset A \times B$. Si $(a, b) \in \mathcal{R}$ denotamos $a\mathcal{R}b$
- **[Propiedades de relaciones]**: Una relación R en A es:
  - **Refleja**: si $\forall x \in A$, $x\mathcal{R}x$
  - **Simétrica**: si $\forall x, y \in A$, $x\mathcal{R}y \Leftrightarrow y\mathcal{R}x$
  - **Antisimétrica**: si $\forall x, y \in A$, $x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow y = x$
  - **Transitiva**: $\forall x, y, z \in A$, $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$
- **[Ejemplo de relación]**: En $\mathbb{Z}$ se define la relación divisibilidad, que se anota $a|b$ si existe $q \in \mathbb{Z}$ tal que $b = qa$.
- **[Relación de orden]**: $\mathcal{R}$ es una relación de orden en A, si es una relación **refleja**, **antisimétrica** y **transitiva**. **Observación:** $\mathcal{R}$ es un orden total si para todo $x, y \in A$, xey son comparables, es decir $x\mathcal{R}y$ o $y\mathcal{R}x$.
- **[Relación de equivalencia]**:$\mathcal{R}$ es una relación de equivalencia en A, si es una relación **refleja**, **simétrica** y **transitiva**.
- **[Clase de equivalencia]**: Dado un elemento $a \in A$ se define:
$$[a]_{\mathcal{R}} = \{x \in A \mid a\mathcal{R}x\}$$
- **[Conjunto cuociente]**: Al conjunto de las clases de equivalencia de una relación $\mathcal{R}$ se le llama conjunto cuociente, definido por:
$$A/\mathcal{R} := \{[a]_{\mathcal{R}} \mid a \in A\}$$
- **[Equivalencias relevantes]**: Sea $\mathcal{R}$ relación de equivalencia en A y $x, y \in A$. Son equivalentes:
  I) $[x]_{\mathcal{R}} \subseteq [y]_{\mathcal{R}}$
  II) $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \emptyset$
  III) $x\mathcal{R}y$
  IV) $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$

  Obs.: Con esto se deduce que $A/\mathcal{R}$ es una partición de A.
- **[Congruencia modular]**: Sea $n \in \mathbb{N}$. Se define $\mathbb{Z}$ la relación $\equiv_n$ por:
$$a \equiv_n b \Longleftrightarrow n|(a - b)$$
- **[Teorema de División Entera]**: Sean $a, m \in \mathbb{Z}$ con $m \neq 0$. Entonces existe un único par $q, r \in \mathbb{Z}$ tal que $a = q \cdot m + r$ y $0 \leq r < |m|$.
- **[Corolario]**: $\mathbb{Z}_n$ $(:= Z/ \equiv_n)$ tiene n elementos:
$$\mathbb{Z}_n = \{[r]_n \mid 0 \leq r < n\}$$

6.- Sumatorias

- **[Sumatoria]**: Sea $(a_i)_{i \geq m}$ secuencia de números. Para $n \geq m$ se define la sumatoria de los términos de $(a_i)_{i \geq m}$ por:
$$\sum_{k=m}^{n} a_k = \begin{cases} a_m & \text{si } n = m \\ a_n + \sum_{k=m}^{n-1} a_k & \text{si } n > m \end{cases}$$
- **[Propiedades importantes]**: Se tienen las siguientes propiedades:
  I) $\sum\limits_{k=m}^{n} 1 = n - m + 1$
  II) $\sum\limits_{k=m}^{n} \lambda a_k = \lambda \sum\limits_{k=m}^{n} a_k$
  III) $\sum\limits_{k=m}^{n} (a_k \pm b_k) = \sum\limits_{k=m}^{n} a_k \pm \sum\limits_{k=m}^{n} b_k$
  IV) $\sum\limits_{k=m}^{n} a_k = \sum\limits_{k=m+s}^{n+s} a_{k-s}$ para $s \in \mathbb{Z}$
  V) $\sum\limits_{k=m}^{n} a_k = \sum\limits_{k=m}^{s} a_k + \sum\limits_{k=s+1}^{n} a_k$
  VI) $\sum\limits_{k=m}^{n} (a_k - a_{k+1}) = a_m - a_{n+1}$
- **[Sumas importantes]**: Algunas sumas relevantes:
  - $\sum\limits_{k=0}^{n} k = \dfrac{n(n+1)}{2}$
  - $\sum\limits_{k=0}^{n} k^2 = \dfrac{n(n+1)(2n+1)}{6}$
  - $\sum\limits_{k=0}^{n} a^k = \dfrac{a^{n+1} - 1}{a - 1}$ con $a \neq 1$
- **[Índices disjuntos]**: Sea $(a_k)_{k \in [1..n]}$ una secuencia de números reales y sean $I, J \subseteq [1..n]$ disjuntos. Entonces:
$$\sum_{k \in I \cup J} a_k = \sum_{k \in I} a_k + \sum_{k \in J} a_k$$

Obs.:$[1..n] = \{1, ..., n\}$

- **[Intercambio de sumas dobles]**: Para una sumatoria doble $\sum\limits_{k=1}^{n}\sum\limits_{j=1}^{m} a_{kj}$ cuyos **límites inferiores y superiores no dependen de los índices**, se tiene:

$$\sum_{k=1}^{n}\sum_{j=1}^{m} a_{kj} = \sum_{j=1}^{m}\sum_{k=1}^{n} a_{kj}$$

7.- Conjuntos finitos

- **[Conjunto finito]**: Un conjunto A se dice finito si posee finitos elementos, es decir si $\exists n \in \mathbb{N}$ tal que existe una función $f : A \to [1..n]$.

- **[Cardinal finito]**: Sea A un conjunto finito. Definimos el cardinal de A - denotado por $|A|$- como el único $n \in \mathbb{N}$ para el que existe una enumeración $a_1, ..., a_n$ de A.

- **[Propiedades varias]**:

  1. $|A| = 0 \Leftrightarrow A = \emptyset$
  2. $|A| = |B| \Leftrightarrow \exists f : A \to B$ biyectiva.
  3. Si B es finito y $A \subseteq B$, entonces A es finito y $|A| \leq |B|$
  4. Si A, B finitos disjuntos entonces $|A \cup B| = |A| + |B|$
  5. Si $B \subseteq A$ con A finito, entonces $|A \setminus B| = |A| - |B|$. En particular si $|A| = |B|$ entonces $A = B$
  6. Si A, B finitos, entonces $|A \cup B| = |A| + |B| - |A \cap B|$.

- **[Equivalencia para funciones]**: Si A, B finitos con $|A| = |B|$ y sea $f : A \longrightarrow B$ función. Son equivalentes:

  - f es inyectiva.
  - f es epiyectiva.
  - f es biyectiva.

- **[Propiedad importante]**: Sean A, B conjuntos con B finito. Se tiene:

  1. A es finito y $|A| \leq |B|$ si y solo si existe $f : A \to B$ inyectiva.
  2. A es finito y $|A| = |B|$ si y solo si existe $f : A \to B$ biyectiva.

- **[Cardinal producto]**: Sean A, B conjuntos finitos, se tiene que $|A \times B| = |A| \cdot |B|$

- **[Conjunto de funciones]**: Sean A, B conjuntos, se define:

$$B^A := \{f : A \to B \mid f \text{ es función}\}$$

Además, se cumple que $|B^A| = |B|^{|A|}$.

- **[Cantidad de inyecciones]**: Sean A, B conjuntos tales que $|A| = k$ y $|B| = n$. Se tiene que:

$$\begin{aligned}\frac{n!}{(n-k)!} &= |\{f : A \longrightarrow B | f \text{ es inyectiva }\}| \\ &= \#\text{ de k- tuplas } B^k \text{ sin repeticiones.}\end{aligned}$$

- **[Coeficiente Binominal]**: Para dos enteros n y k, $n \geq 0$, se define

$$\binom{n}{k}$$

Este numero representa el numero de subconjuntos de tamaño k que posee un conjunto de tamaño n. Se verifica que $\forall n \in \mathbb{N}, \forall k \in \mathbb{N}$ tal que $0 \leq k \leq n$:

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

- **[Propiedades relevantes]**:

  a) $\binom{n}{k} = \binom{n}{n-k}$
  b) $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$

- **[Binomio de Newton]**: Sean $x, y \in \mathbb{R}$, $n \in \mathbb{N}$, entonces:

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

- **[Cardinal de la imagen de un conjunto]**: Si $f : A \longrightarrow B$ función, entonces $|f(A)| \leq |A|$

8.- Conjuntos Infinitos

- **[Conjunto numerable]**: Un conjunto A se dira numerable si $|A| = |\mathbb{N}|$. En particular tenemos que $\mathbb{Z}$ y $\mathbb{Q}$ son numerables.

- **[Propiedades Cardinal infinito]**: Sea A conjunto infinito, entonces:

  I) Si A infinito y B finito, entonces $|A| = |A \cup B| = |A \setminus B|$
  II) $\forall k \in \mathbb{N}$, existe un conjunto B_k tal que $B_k \subseteq A$ y $|B_k| = k$.
  III) $|A| \geq |\mathbb{N}|$ es decir el cardinal de los naturales es **el menor cardinal infinito**.

Obs.: Si $|A| \leq |\mathbb{N}|$ entonces A es numerable.

- [**Álgebra de numerables**]:

  I) La unión numerable o finita de conjuntos numerables o finitos $(A_i)_{i\in I}$ (con $I \subseteq \mathbb{N}$) es a lo más numerable, es decir:

  $$A := \bigcup_{i\in I} A_i$$

  Cumple que $|A| \leq |\mathbb{N}|$

  II) La unión finita de conjuntos numerables $(A_i)_{i=1}^n$ es numerable, es decir:

  $$A := \bigcup_{i=1}^{n} A_i$$

  Es numerable.

  III) La unión numerable de conjuntos numerables $(A_i)_i^n$ es numerable, es decir:

  $$A := \bigcup_{i\in\mathbb{N}} A_i$$

  Es numerable.

  IV) El producto cartesiano finito de conjuntos numerables $(A_i)_{i=1}^n$ es numerable, es decir:

  $$A := \prod_{i=1}^{n} A_i$$

  Es numerable.

- [**Producto numerable de finitos**]: El producto de una familia numerable de conjuntos finitos de tamaño dos no es numerable.

- [**Cardinal del conjunto potencia**]: El cardinal del conjunto potencia de un conjunto es mayor que el cardinal del conjunto, es decir: $|A| < |\mathcal{P}(A)|$.

- [**Cardinal Real**]: Se tiene que $|\mathcal{P}(\mathbb{N}) \leq |[0,1]|$. Esto implica que: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |[0,1]| = |\mathbb{R}|$

9.- Estructuras algebraicas

- [**Ley de composición interna**]: Dado $A \neq \emptyset$. Se define una l.c.i. como:

$$\begin{array}{rccc} *: & A\times A & \to & A \\ & (x,y) & \to & x*y \end{array}$$

- [**Estructura algebrica**]: Si $*$ es l.c.i. en A, $(A,*)$ es llamado estructura algebraica. Si existe otra l.c.i Δ denotaremos $(A,*,\Delta)$

- [**Definiciones varias**]: Sea $(A,*)$ estructura algebrica:

  I) $*$ es **asociativa** si:

  $$\forall x,y,z \in A, (x*y)*z = x*(y*z)$$

  II) $e \in A$, se dira **neutro** para $*$ si:

  $$\forall x \in A, e*x = x*e = x$$

  III) Si e neutro, y $x \in A$, diremos que x tiene **inverso** si existe $y \in A$ tal que:

  $$x*y = y*x = e$$

  IV) $*$ es **conmutativa** si:

  $$\forall x,y \in A, x*y = y*x$$

  V) $a \in A$ es **absorbente** si:

  $$\forall x \in A, x*a = a*x = a$$

  VI) $a \in A$ es **idempotente** si

  $$a*a = a$$

  VII) $a \in A$ es **cancelable** si $\forall y,z \in A$:

  $$a*y = a*z \Rightarrow y = z$$
  $$y*a = z*a \Rightarrow y = z$$

  VIII) Dado $(A,*,\Delta)$ diremos que Δ **distribuye** con respecto a $*$ si $\forall x,y,z \in A$:

  $$x\Delta(y*z) = (x\Delta y)*(x\Delta z)$$
  $$(y*z)\Delta x = (y\Delta x)*(z\Delta x)$$

- [**Cancelabilidad**]: Sea $(A,*)$ e.a., se tiene que $a \in A$ es cancelable si y solo si las funciones $I_a(x) = a*x$ y $D_a(x) = x*a$ para $x \in A$ son inyectivas

- [**Unicidad del neutro**]: Una e.a. $(A,*)$ posee a lo más un neutro.

- [**Unicidad del inverso**]: Si la e.a. $(A,*)$ tiene neutro e y $*$ es asociativa, entonces los inversos (en el caso en que existan) son únicos.

- [**Propiedades varias**]: Si $(A,*)$ es e.a. asociativa con neutro e, entonces también cumple:

  I) Si $x \in A$ posee inverso, entonces x^{-1} también. Más aún $(x^{-1})^{-1} = x$.

II) Si $x, y \in A$ poseen inversos, entonces $x * y$ también y se tiene $(x * y)^{-1} = y^{-1} * x^{-1}$

III) Si $x \in A$ posee inverso, entonces x es cancelable.

10.- Homomorfismos

- **[Homomorfismos]**: Una función $f : A \to B$ es un **homomorfismo** entre las estructuras algebraicas $(A, *)$ y (B, Δ) si:

$$\forall x, y \in A,\ f(x * y) = f(x) \Delta f(y)$$

  - Si f inyectiva se dirá **monomorfismo**.
  - Si f es epiyectiva se dirá **epimorfimo**.
  - Si f es biyectiva se dirá **isomorfismo**.
  - Si $(A, *) = (B, \Delta)$ los homomorfismo se llaman **endomorfismos**. Si son biyectivos se llaman **automorfismos**

- **[Props epimorfismos]**: Si $f : A \to B$ epimorfismo entre $(A, *)$ y (B, Δ), entonces se tienen las siguientes propiedades:

  I) Si $(A, *)$ es asociativa, entonces (B, Δ) tambien lo es.

  II) Si $(A, *)$ es conmutativa, entonces (B, Δ) tambien lo es.

  III) Si e es neutro para $(A, *)$, entonces $f(e)$ lo es para (B, Δ).

  IV) Si a tiene inverso b para $(A, *)$, entonces $f(a)$ tiene inverso $f(b)$ para (B, Δ).

- **[Props. más generales]**: Sea f un homomorfismo de $(A, *)$ a (B, Δ), con neutros e_A y e_B:

  I) Si $e_B \in f(A)$, entonces $e_B = f(e_A)$.

  II) Si $e_B \in f(A)$ y $a \in A$ tiene inverso b, entonces $f(a)$ tiene inverso $f(b)$.

- **[Composición]**: Si $f : A \to B$ un homeomorfismo de $(A, *)$ en (B, Δ) y $g : B \to C$ un homemorfismo de (B, Δ) en $(C, \bullet)$, entonces la composición de f con g, $g \circ f : A \to C$, es un homomorfismo de $(A, *)$ en $(C, \bullet)$.

- **[Estructuras isomorfas]**: Dos estructuras $(A, *)$ y (B, Δ) son isomorfas, denotado $(A, *) \cong (B, \Delta)$, si existe una función $f : A \to B$ isomorfismo.
  Obs.: $\cong$ es una relación de equivalencia.

- **[Isomorfismo inverso]**: Si $f : A \to B$ es un isomorfimos entre $(A, *)$ y (B, Δ), entonces $f^{-1} : B \to A$ es un isomorfismo entre (B, Δ) y $(A, *)$.

- **[Estructura de funciones]**: Sea $(B, *)$ una e.a., entonces $(B^A, *)$ sera una e.a., donde si $f, g \in B^A$ definimos $f * g : A \to B$ por:

$$(f * g)(x) = f(x) * g(x)$$

- **[Propiedades varias]**:

  I) Si $(B, *)$ es asociativa, entonces $(B^A, *)$ también.

  II) Si $(B, *)$ es conmutativa, entonces $(B^A, *)$ también.

  III) Si $(B, *)$ tiene neutro e, entonces $f \in (B^A, *)$ dado por $f(x) = e$ (función constante) es neutro de $(B^A, *)$

- **[Estructura de pares ordenados]**: Sean $(A_1, *_1)$ y $(A_1, *_1)$ e.a., se define la l.c.i. $\otimes$ sobre $A_1 \times A_2$ por: Para $(a_1, a_2), (b_1, b_2) \in A_1 \times A_2$:

$$(a_1, a_2) \otimes (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$$

- **[Propiedades varias]**:

  I) Si $(A_1, *_1)$,$(A_2, *_2)$ son asociativas, entonces $(A_1 \times A_2, \otimes)$ también.

  II) Si $(A_1, *_1)$,$(A_2, *_2)$ son conmutativas, entonces $(A_1 \times A_2, \otimes)$ también.

  III) Si $(A_1, *_1)$,$(A_2, *_2)$ poseen neutros e_1 y e_2, entonces $(A_1 \times A_2, \otimes)$ posee neutro (e_1, e_2)

  IV) Si a_1, a_2 poseen inversos b_1, b_2 en $(A_1, *_1)$,$(A_2, *_2)$, entonces (a_1, a_2) posee inverso (b_1, b_2) en $(A_1 \times A_2, \otimes)$.

11.- Grupos

- **[Grupo]**: Sea $(G, *)$ una e.a., diremos que:
  - Es **grupo** si $*$ es asociativa, tiene neutro y todo elemento posee inverso.
  - Es **grupo abeliano** si es grupo y $*$ es conmutativa.

- **[Propiedades grupos]**: Sea $(G, *)$ grupo, entonces:

  I) $\forall a, b \in G, a * x_1 = b \Leftrightarrow x_1 = a^{-1} * b$
  $\forall a, b \in G, x_2 * a = b \Leftrightarrow x_1 = b * a^{-1}$
  Es decir, las ecuaciones tienen una única solución.

  II) $\forall a \in G$ las funciones $I_a(x) = a * x$ y $D_a(x) = x * a$ son biyectivas.

  III) El unico elemento idempotente es el neutro.

  IV) Si (K, Δ) una e.a. y $f : G \to K$ homomorfismo, entonces $(f(G), \Delta)$ es grupo.

v) Si (K, Δ) una e.a., un homomorfismo $f : G \to K$ es monomorfismo (inyectivo) si y solo si $f^{-1}(\{e_K\}) = \{e_G\}$

- [**Grupos importantes**]:
  - Si $(G, *)$ es grupo (abeliano) y $A \neq \emptyset$, entonces $(G^A, *)$ es grupo (abeliano)
  - Si $(G_1, *_1)$, $(G_2, *_2)$ son grupos (abelianos), entonces $(G_1 \times G_2, \otimes)$ es grupo (abeliano).
- [**Subgrupo**]: Sea $(G, *)$ grupo y $\emptyset \neq H \subseteq G$. Diremos que H es subgrupo de G si $(H, *)$ es grupo.
- [**Propiedades subgrupos**]:
  1. Si $e \in G$ es el neutro de G y $e_H \in H$ es neutro de H entonces $e = e_H$.
  2. Además, sea $x \in H$. $x^{-1} \in G$ es el inverso de x en $(G, *)$, y $\overline{x}$ es el inverso de x en $(H, *)$. Entonces $x^{-1} = \overline{x}$.
- [**Caracterización Subgrupos**]: Sea $H \neq \emptyset$. Entonces:

$$(H, *) \text{ es subgrupo de } (G, *) \Leftrightarrow \forall x, y \in H,\ x * y^{-1} \in H$$

- [**Subgrupo imagen**]: Sea $(G, *)$ grupo, (K, Δ) una estructura algebraica y $f : G \longrightarrow K$ un morfismo. Si H es subgrupo de $(G, *)$, entonces $f(H)$ es subgrupo de $(f(G), \Delta)$.
- [**Traslación**]: Sea H subgrupo de $(G, *)$. Definimos traslación de H en $a \in G$ por la izquierda como:

$$a * H = \{a * h \mid h \in H\}$$

- [**Cardina traslación**]: Sea H subgrupo de $(G, *)$, el conjunto de las traslaciones de H particiona G, además el cardinal de cada traslación coincide con el de H ($\forall a \in G$, $|a * H| = |H|$)
- [**Lagrange**]: Si $(H, *)$ es subgrupo del grupo finito $(G, *)$, entonces $|H|$ divide a $|G|$.

12.- Anillos y Cuerpos

- [**Anillo**]: Una e.a. $(A, +, \cdot)$ se llamará anillo si:
  - $(A, +)$ es grupo abeliano.
  - $\cdot$ es asociativa y posee elemento neutro en $A \setminus \{0\}$.
  - $\cdot$ distribuye con respecto a $+$.

En el caso de ser $\cdot$ conmutativo, $(A, +, \cdot)$ será anillo conmutativo.

- [**Morfismos de anillos**]: $f : A \to B$ Sera morfismo entre dos anillos $(A, +, \cdot)$ y $(B, +, \cdot)$ si:

$$f(x + y) = f(x) + f(y)$$
$$f(x \cdot y) = f(x) \cdot f(y)$$
$$f(1) = 1$$

- [**Algebra en anillos**]: Si $(A, +, \cdot)$ es anillo y $x, y \in A$:
  - $0 \cdot x = x \cdot 0 = 0$
  - $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$
  - $(-x) \cdot (-y) = x \cdot y$
  - $-x = (-1) \cdot x = x \cdot (-1)$
- **Algebra de anillos**]: Sea $(A, +, \cdot)$ un anillo conmutativo.
  1. $\forall k, l \in \mathbb{Z}$, $\forall a, b \in A$, $k(a + b) = ka + kb$, $(k + l)a = ka + la$ y $(ka)(lb) = (kl)(ab)$
  2. $\forall x, y \in A$, $\forall n \in \mathbb{N}$, $(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$
  3. $\forall x \in A$, $\forall n \in \mathbb{N}$, $x^{n+1} - 1 = (x - 1) \sum_{k=0}^{n} x^k$
- [**Divisores de cero y dominio de integridad**]: Sea $(A, +, \cdot)$ un anillo. Un elemento $a \neq 0$ es divisor de 0 si $\exists y \neq 0$ tal que $a \cdot y = 0$ o $y \cdot a = 0$.
A un anillo conmutativo y sin divisores de 0 lo llamaremos dominio de integridad.
- [**Propiedad**]: Si $(A, +, \cdot)$ anillo, entonces:

$$a \text{ es cancelable en } (A, \cdot) \Leftrightarrow a \text{ no es divisor de cero}$$

- [**Cuerpo**]: Una estructura $(\mathbb{K}, +, \cdot)$ se llamará cuerpo si:
  - $(\mathbb{K}, +, \cdot)$ es anillo conmutativo.
  - Todo elementos en $K \setminus \{0\}$ es invertible para $\cdot$.

Equivalentemente $(\mathbb{K}, +, \cdot)$ sera cuerpo si y solo si:

  - $(\mathbb{K}, +)$ es grupo abeliano.
  - $(\mathbb{K} \setminus \{0\}, \cdot)$ es grupo abeliano.
  - $\cdot$ distribuye con respecto a $+$.

- [**Caracterización cuerpos finitos**]: Si $(\mathbb{K}, +, \cdot)$ es cuerpo, entonces $\mathbb{K}$ no tiene divisores de 0 ($\mathbb{K}$ es dominio de integridad).
El reciproco se tiene si $|\mathbb{K}|$ es finito, es decir:

Si $(\mathbb{K}, +, \cdot)$ es dominio de integridad con $|\mathbb{K}|$ finito, entonces $(\mathbb{K}, +, \cdot)$ es cuerpo.

13.- Numeros Complejos

- **[Formalidad]**: Identificamos $\mathbb{C} = \mathbb{R}^2$, de manera que se definen las operaciones $+$ y $\cdot$ para $z = (a,b), w = (c,d) \in \mathbb{C}$ por:
$$\begin{aligned} z + w &= (a+c, b+d) \\ z \cdot w &= (ac - bd, ad + bc) \end{aligned}$$
- **[Unidad Imaginaria]**: Se define $i = (0,1)$
- **[Forma cartesiana]**: La expresión $a + bi$, $a, b \in \mathbb{R}$ es la forma cartesiana de $z = (a,b)$.
Ademas se define:
    - $Re(z) = a$ (Parte real)
    - $Im(z) = b$ (Parte imaginaria)
- **[Coordenadas Polares]**: Para $z \in \mathbb{C} \setminus \{0\}$ se define el par $(r, \theta) \in (0, \infty) \times [0, 2\pi)$ donde:
    - r es la distancia de z al origen, se llama modulo de z y se anota $r = |z|$.
    - θ es el angulo que se forma entre el eje X (real) y el segmento que une el origen con z. Se llama argumento (principal) de z y se anota $arg(z)$.
- **[Forma polar]**: Para $\theta \in \mathbb{R}$ anotamos $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. La expresión $|z|e^{iarg(z)}$ es la forma polar de z.
- **[Props varias]**:
    - I) $\forall \alpha, \beta \in \mathbb{R}$, $e^{i\alpha} \cdot e^{i\beta} = e^{i\alpha + \beta}$
    - II) $|zw| = |z| \cdot |w|$
    - III) $arg(zw) \equiv arg(z) + arg(w)$ $(mod\ 2\pi)$
    - IV) $|z^k| = |z|^k$
    - V) $(e^{i\theta})^k = e^{i(k\theta)}$
- **[Conjugado]**: Sea $z = a + bi \in \mathbb{C}$, se define $\overline{z} = a - bi$
- **[Función Conjugado]**: La conjugación es un automorfismo en $(\mathbb{C}, +, \cdot)$, es autoinversa y restringida a $\mathbb{R}$ es la identidad.
- **[Desigualdad triangular]**: Si $z, w \in \mathbb{C}$, entonces $|z + w| \leq |z| + |w|$.
- **[Raices**: Sean $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$. Diremos que z es una raíz $n-$esima de w si $z^n = w$.
- **[Soluciones]**: Sean $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$, si $w = re^{i\theta}$ (forma polar) entonces la ecuación $z^n = w$ tiene n soluciones, dadas por:
$$w_k = \sqrt[n]{r} \cdot e^{i\frac{(\theta + 2\pi k)}{n}}$$
- **[Prop]**: Sean $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$, entonces la suma de las raíces n-ésimas vale 0:
$$\sum_{k=0}^{n-1} w_k = 0$$
- **[Muchas propiedades]**: Sean $z, w \in \mathbb{C}$
    - a) $\overline{\overline{z}} = z$.
    - b) $z \in \mathbb{R} \iff z = \overline{z}$.
    - c) $\overline{z + w} = \overline{z} + \overline{w}$ y $\overline{z - w} = \overline{z} - \overline{w}$.
    - d) $\overline{zw} = \overline{z} \cdot \overline{w}$. Si $w \neq 0$ $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.
    - e) Si $\lambda \in \mathbb{R}$, entonces $\overline{\lambda z} = \lambda \overline{z}$.
    - f) $Re(z) = Re(\overline{z})$ y $Im(z) = -Im(\overline{z})$.
    - g) $Re(z) = \frac{1}{2}(z + \overline{z})$ y $Im(z) = \frac{1}{2i}(z - \overline{z})$
    - h) Si $z \neq 0$, entonces $z^{-1} = \frac{1}{|z|} e^{-iarg(z)}$
    - i) $|z| = |\overline{z}|$
    - j) $arg(\overline{z}) = 2\pi - arg(z)$
    - k) $z \cdot \overline{z} = |z|^2$
    - l) Si $z \neq 0$, entonces $z^{-1} = \frac{\overline{z}}{|z|^2}$.
    - m) Si $w \neq 0$, entonces $|\frac{z}{w}| = \frac{|z|}{|w|}$.

14.- Polinomios

- **[Polinomio]**: Si $(\mathbb{K}, +, \cdot)$ cuerpo, llamamos polinomio en $\mathbb{K}$ (denotado $p \in \mathbb{K}[x]$) a una función:
$$\begin{aligned} p: \quad \mathbb{K} &\longrightarrow \quad \mathbb{K} \\ x &\longrightarrow \quad p(x) = \sum_{k=0}^{n} p_k x^k \end{aligned}$$
donde $n \in \mathbb{N}$ y $p_k \in \mathbb{K}$ constantes.
- **[Igualdad de polinomios]**: Si $p \in \mathbb{K}[x]$ y $q \in \mathbb{K}[x]$ con $p(x) = \sum_{k=0}^{n} p_k x^k$ y $q(x) = \sum_{k=0}^{m} q_k x^k$ entonces:
$$p = q \Leftrightarrow (n = m \wedge \forall k \in \{0, ..., 1\},\ p_k = q_k$$
- **[Grado]**: Si $p \in \mathbb{K}[x]$ con $p(x) = \sum_{k=0}^{n} p_k x^k$ llamamos $gr(p) = n$ con n el mayor numero tal que $p_n \neq 0$. Si $p(x) = 0$ definimos $gr(P) = -\infty$.
Obs.: Si $p_n = 1$, p se dira polinomio mónico.

- **[Anillo de polinomios]**: Si $(\mathbb{K}, +, \cdot)$ es cuerpo, entonces $(\mathbb{K}[x], +, \cdot)$ es anillo conmutativo que no posee divisores de 0.

- **[Suma y producto de polinomios]**: Si $p, q \in \mathbb{K}[x]$ con $gr(p) = n$ y $gr(q) = m$ entonces $gr(p+q) \leq \text{máx}\{n, m\}$ con:
$$(p+q)(x) = \sum_{k=0}^{\text{máx}\{n,m\}} (p_k + q_k)x^k$$
Además $gr(p \cdot q) = gr(p) + gr(q)$.

- **[Inversos]**: En $(\mathbb{K}[x], +, \cdot)$ los únicos polinomios con inversos son los de grado 0.

- **[Teorema de la División]**: Sean $p, d \in \mathbb{K}[x]$ con $d \neq 0$. Entonces existe un único par $q, r \in \mathbb{K}[x]$ tal que
    1. $p = q \cdot d + r$
    2. $gr(r) < gr(d)$

  Obs.: A q se le llama cociente, a r resto, y d divisor de p con resto r.

- **[Teorema del resto]**: Sea $p \in \mathbb{K}[x]$ y $c \in \mathbb{K}[x]$ y $c \in \mathbb{K}$. El resto de dividir P por el polinomio $(x-c)$ es exactamente $p(c)$

- **[Raíz]**: $c \in \mathbb{K}$ es raíz de $p \in \mathbb{K}[x]$ si $p(c) = 0$.

- **[Prop raíces]**: $c \in \mathbb{K}$ es raiz de $p \in \mathbb{K}[x] \Leftrightarrow (x-c)|p(x)$ (el resto es 0).
  Definimos $\mathcal{Z}(p)$ como el conjunto de raíces de p.

- **[Prop varias]**:
    1. Si $c_1, c_2, ..., c_k$ raíces distintas de p entonces $(x-c_1)(x-c_2)...(x-c_k)|p(x)$.
    2. Si $p \in \mathbb{K}[x]$ con $gr(p) = n \geq 1$ entonces p posee a lo más n raíces distintas.
    3. Sean $n \geq 0$ y $p, q \in K[x]$ con $gr(p) \leq n$ y $gr(q) \leq n$. Si p y q coinciden en $n+1$ puntos, entonces son iguales.

- **[TFA (D'Alembert)]**: Si $p \in \mathbb{C}[x]$ es tal que $gr(p) = n \geq 1$ entonces p posee al menos una raíz en $\mathbb{C}$.
  Se deduce mediante esto que el polinomio p debe poseer n raíces en $\mathbb{C}$.

- **[Factorización compleja]**: Si $p \in \mathbb{C}[x]$ es tal que $gr(p) = n \geq 1$ entonces existen $\alpha, c_1, ..., c_m \in \mathbb{C}$ y naturales $l_1, ..., l_m \geq 1$ tales que $gr(p) = l_1 + ... + l_m$ y:
$$p(x) = \alpha(x-c_1)^{l_1}...(x-c_m)^{l_m}$$

- **[Raíz conjugada]**: Si $p \in \mathbb{C}[x]$ tiene todos sus coeficientes reales, y $z \in \mathbb{C}$ es raíz de P entonces $\overline{z}$ es también raíz de p.

- **[Factorización real]**: Si $p \in \mathbb{R}[x]$ es tal que $gr(p) = n \geq 1$, entonces existen $\alpha, c_1, ..., c_m, p_1, q_2, ..., p_s, q_s \in \mathbb{R}$ tales que:
$$p(x) = \alpha(x-c_1)..(x-c_m)(x^2+p_1x+q_1)..(x^2+p_sx+q_s)$$
Donde c_k son las raíces del polinomio y $(x^2+p_1x+q_1), ..., (x^2+p_sx+q_s)$ no tienen raíces reales, y $\alpha = p_n$ en p.

- **[Coeficientes enteros]**: Sea $p \in \mathbb{R}[x]$. si $\frac{r}{s} \in \mathbb{Q}$ (r y s primos relativos) es una raíz de p entonces $r|p_0$ y $s|p_n$.

- **[Ultima propiedad]**: Si $p \in \mathbb{R}[x]$ es mónico, con coeficientes $p_0, ..., p_{n-1} \in \mathbb{Z}$ entonces toda raíz racional de p es entera y divide a p_0.