I2 Discretas

lmfros

September 2017

1. Teoria de Conjuntos

Definición 1.1. Subconjunto: Sean A y B conjuntos. Diremos que A es subconjunto de otro conjunto B si:

$$\forall x.(x \in A \rightarrow x \in B)$$

Si cada elemento de a es un elemento de B.

$$A \subseteq B$$

Definición 1.2. Axioma de Extension: Dos conjuntos A y B son iguales si se cumple que:

$$A \subseteq B \land B \subseteq A$$

o de manera equivalente:

$$\forall A, B : \forall x.(x \in A \leftrightarrow x \in B) \rightarrow A = B$$

Observacion:

Los conjuntos no tienen elementos repetidos $\{x, x\} = \{x\}$

Definición 1.3. Subconjunto Propio Diremos que A es subconjunto propio de B si:

$$A \subseteq B \land A \neq B, \text{ o alternativamente }, A \subseteq B \land B \nsubseteq A.$$

Notacion:

$$A \subsetneq B$$

Corolario 1.3:

$$B \nsubseteq A \leftrightarrow \exists x \in B \text{ se cumple } x \notin A. \tag{1}$$

Definición 1.4. Axioma del conjunto vacio

$$\exists X, \text{ tal que } \forall x, x \notin X.$$

Notacion: $\varnothing$ o $\{\}$.

Teorema 1.1. *El conjunto vacio es subconjunto de todos los conjuntos.*

$$\forall A, \textit{ se tiene que } \varnothing \subseteq A.$$

Demostración. $\forall x\ x \in \varnothing\ \rightarrow x \in A$ el conjunto vacio no tiene elementos, por lo que $x \in \varnothing$ es falso y la implicancia es trivialmente verdadera. □

Teorema 1.2. *El conjunto vacio es unico.*

Demostración. Por contradiccion, suponer que existen al menos dos conjuntos vacios, $\varnothing_1$,$\varnothing_2$, por el teorema anterior tenemos que $\varnothing_1$ es vacio $\rightarrow \varnothing_1 \subseteq \varnothing_2$. Analogamente, como $\varnothing_2$ es vacio $\rightarrow \varnothing_2 \subseteq \varnothing_1$. Por el Axioma de extensión, $\varnothing_1 = \varnothing_2$ por lo que llegamos a una contradicción. □

Definición 1.5. Axioma de abstracción:
Si φ es una propiedad sobre objetos, entonces $\{x|\varphi(x)\}$ es un conjunto tal que $x \in A \leftrightarrow \varphi(x)$
Definición 1.6. Axioma de separacion:
φ es una propiedad y C es conjunto "sano"(No creado con el axioma de separacion), entonces

$$A = \{x|x \in C \land \varphi(x)\}$$

Es un conjunto.

1.1. Operaciones:

- Union:
$$A \cup B = \{x|x \in A \lor x \in B\}$$
$$A \subseteq A \cup B$$
- Interseccion:
$$A \cap B = \{x|x \in A \land x \in B\}$$
$$A \cap B \subseteq A$$
- Diferencia:
$$A/B = \{x|x \in A \land x \notin B\}$$
$$A/B \cap B/A = \varnothing$$
- Conjunto Potencia:
$$P(A) = \{X|X \subseteq A\}$$
El conjunto de todos los subconjuntos de A.
$$\varnothing, A \in P(A)$$

Definición 1.7. Suma: Se define la funcion $sum(x, y)$ como:

- $sum(m, 0) = m$
- $sum(m, \delta(n)) = \delta(sum(m, n))$

Es conmutativa y asociativa.
Definición 1.8. Multiplicacion: Se define la funcion $mult(x, y)$ como:

- $mult(m, 0) = 0$
- $mult(m, \delta(n)) = sum(m, mult(m, n))$

Es conmutativa y asociativa.

1.2. Leyes:

Consideremos un $\mathcal{U}$ sano fijo.

Definición 1.9. Complemento:
Sea $A \subseteq \mathcal{U}$, el complemento de A denotado como A^c es:

$$A^c = \{x | x \in \mathcal{U} \land x \notin A\}$$

Teorema 1.3. *Propiedades:*

- *Asociatividad:*

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

Demostración.

$$A \cup (B \cup C) = \{x | x \in A \lor x \in B \cup C\}$$
$$B \cup C = \{x | x \in B \lor x \in C\}$$
$$A \cup B \cup C = \{x | x \in A \lor x \in B \lor x \in C\}$$

Por asociatividad de $\lor$,

$$A \cup B \cup C = \{x | (x \in A \lor x \in B) \lor x \in C\}$$
$$A \cup B = \{x | x \in A \lor x \in B\}$$
$$(A \cup B) \cup C = \{x | (x \in A \cup B) \lor x \in C\}$$

□

- *Comnuatividad:*

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

- *Idempotencia:*

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

- *Absorbcion:*

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

- *Elemento Neutro:*

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

- *Distributivdad:*

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

- *De Morgan:*

$$(A \cap B)^c = A^c \cup B^c$$
$$(A \cup B)^c = A^c \cap B^c$$

- *Elemento Inverso:*

$$A \cup A^c = \mathcal{U}$$
$$A \cap A^c = \varnothing$$

- *Dominacion:*

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

1.3. Operaciones Generalizadas:

Sea $\mathcal{S}$ un **conjunto de conjuntos**.

- Union generalizada:

$$\bigcup \mathcal{S} = \{x \mid \exists A \in \mathcal{S} \text{ tal que } x \in A\}$$

Notacion: $\bigcup \mathcal{S} = \bigcup\limits_{A \in \mathcal{S}} A$
Alternativamente, si $\mathcal{S}$ esta indexada:

$$\mathcal{S} = \{A_0, A_1, ..., A_{n-1}\}$$
$$\bigcup \mathcal{S} = \bigcup_{i=0}^{n-1} A_i$$
$$x \in \mathcal{S} \iff \exists i,\ 0 \leq i \leq n \text{ tal que } x \in A_i$$

- Intereseccion generalizada:

$$\bigcap \mathcal{S} = \{x \mid \exists A \in \mathcal{S} \text{ tal que } x \in A\}$$

Notacion: $\bigcap \mathcal{S} = \bigcap\limits_{A \in \mathcal{S}} A$
Alternativamente, si $\mathcal{S}$ esta indexada:

$$\mathcal{S} = \{A_0, A_1, ..., A_{n-1}\}$$
$$\bigcap \mathcal{S} = \bigcap_{i=0}^{n-1} A_i$$
$$x \in \mathcal{S} \iff \forall i,\ 0 \leq i \leq n \text{ tal que } x \in A_i$$

2. Relaciones

2.1. Definiciones basicas:

Definición 2.1. Sean $a, b \in \mathcal{U}$, se define el par ordenado (a, b) como:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Propiedad:

$$(a, b) = (c, d) \iff a = c \land b = d$$

Demostración. Por demostrar que:

$$(a,b) = (c,d) \iff a = c \land b = d$$

($\rightarrow$) Por definicion se sabe que,

$$(a,b) = \{\{a\},\{a,b\}\}$$

Supondremos que $(a,b) = (b,c)$, por lo tanto hay 2 casos:

- Caso 1: $a = b$

  $$\{\{a\},\{a,b\}\} = \{\{a\},\{a,a\}\}$$

  Por axioma de extension x2,

  $$\{\{a\},\{a,a\}\} = \{\{a\}\}$$

  Igualando lo anterior a lo supuesto,

  $$\{\{a\}\} = (c,d)$$
  $$\{\{a\}\} = \{\{c\},\{c,d\}\}$$

  Por axioma de extension, $c = d$ es la unica opcion para que sean iguales.Usando axioma de extension x2 nuevamente.

  $$\{\{a\}\} = \{\{c\}\}$$

  Por axioma de extension, $a = c$.
  Por lo tanto, a=b=c=d.

  $$a = b = c = d \iff a = c \land b = d$$

- Caso 2: $a \neq b$
  Dado el supuesto,

  $$\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$$

  Por axioma de extensión, se tiene que cumplir que:

  $$\{\{a\}\} = \{\{c\}\} \land \{\{a,b\}\} = \{\{c,d\}\}$$

  Usando el axioma de extension $a = c$
  Por lo tanto,

  $$\{\{a,b\}\} = \{\{a,d\}\}$$

  Despues por axioma de extension, $b = d$. Por lo tanto queda demostrado que,

  $$(a,b) = (c,d) \iff a = c \land b = d$$

$\square$

Nota:

$$(a,b) \neq (b,a)$$

Definición 2.2. Producto Cartesiano:

$$A \times B = \{(a,b) | a \in A \wedge b \in B\}$$
$$A_1 \times ... \times A_n = \{(a_1, a_2, ..., a_n) | a_1 \in A_1 \wedge ... \wedge a_n \in A_n\}$$

Ejemplos:

$$\mathbb{N} \times \mathbb{N} = \{(0,0), (1,0), ...\}$$
$$\mathbb{N} \times \mathbb{Z} = \{(0,-1), (1,-5), ...\}$$

Definición 2.3. Relacion:
El conjunto R es **relación** sobre $A_1, ..., A_n$ si $R \subseteq A_1 \times ... \times A_n$

Definición 2.4. Relaciones Binarias:
R es una relacion binaria si de dos conjuntos A y B,

$$R \subseteq A \times B$$

Ejemplo:

$$A = \{1,2\}$$
$$B = \{3,4\}$$

Una relacion puede ser:

$$R = \{(1,3), (2,4)\}$$

Ejemplo: Numero de relaciones posibles en conjuntos finitos.

Sea A conjunto con n elementos, el conjunto potencia $P(A)$:

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

Luego para $P(A \times B)$, donde A tiene n elementos y B tiene m elementos, entonces las posibles relaciones son 2^{mn}.
Cuando los conjuntos son iguales: $R \subseteq A \times A = A^2$ o en el caso general: $A \times ... \times A = A^n$
Definición 2.5. Relacion "menor que"($<$):

$$< \subseteq \mathbb{N}^2$$

Dados $m, n in \mathbb{N}$,

$$(m,n) \in < \iff m \in n$$

Ejemplos:

$$(1,3) \in <, \ (10,4) \notin <, \ (7,7) \notin <$$

Notacion de relaciones binarias:

$$(a,b) \in R \ ; \ R(a,b) \ ; \ a \, R \, b \ ; \ a \not R \, b$$
$$(1,7) \in < \ ; \ < (1,7) \ ; \ 1 \ < \ 7 \ ; \ 7 \not< 1$$

Definición 2.6. Relacion "divide"(—):

$$a|b \iff \exists k \in \mathbb{N} - \{0\} \text{ tal que } b = k * a$$

Ejemplo:

$$3|9 \;\; ; \;\; 7\not|9$$

Definición 2.7. Relacion equivalencia modulo n ($\equiv_n$):

$$a \equiv_n b \iff \exists k \in \mathbb{N} \text{ tal que } |a - b| = k * n$$

Ejemplo:

$$2 \;\equiv_7 23$$

$$|2 - 23| = 21 = 3 * 7$$

2.2. Propiedades de Relaciones:

S A.

Definición 2.8. Reflejaea R una relacion sobre un conjunto:
Si para cada $a \in A$ se tiene que $R(a, a)$

$$\forall a\big[(a, a) \in R\big] \tag{2}$$

Definición 2.9. Irrefleja:
Si para cada $a \in A$ no se tiene que $R(a, a)$

$$\forall a\big[(a, a) \notin R\big] \tag{3}$$

Definición 2.10. Simetrica:
Si para cada $a, b \in A$, si $R(a, b)$ entonces $R(b, a)$.

$$\forall a, b\big[(a, b) \in R \rightarrow (b, a) \in R\big] \tag{4}$$

Definición 2.11. Asimetrica:
Si para cada $a, b \in A$, si $R(a, b)$ entonces no es cierto que $R(b, a)$.

$$\forall a, b\big[(a, b) \in R \rightarrow (b, a) \notin R\big] \tag{5}$$

Definición 2.12. Antisimetrica:
Si para cada $a, b \in A$, si $R(a, b)$ y $R(b, a)$, entonces $a = b$.

$$\forall a, b\big[(a, b) \in R \wedge (b, a) \in R \rightarrow a = b\big] \tag{6}$$

Definición 2.13. Transitiva:
Si para cada $a, b, c \in A$, si $R(a, b)$ y $R(b, c)$, entonces $R(a, c)$.

$$\forall a, b, c\big[(a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R\big] \tag{7}$$

Definición 2.14. Conexa:
Si para cada $a, b \in A$, se tiene que $R(a, b)$ o $R(b, a)$.

$$\forall a, b\big[(a, b) \in R \vee (b, a) \in R\big] \tag{8}$$

Ejemplo 1:

Refleja, simétrica y antisimetrica

$$R_1 = \{(1,1),(2,2),(3,3)\}$$

Ejemplo 2:

Irrefleja, simétrica y Transitiva

$$R_2 = \{(1,2),(2,1),(1,1)\}$$

Ejemplo 3:

Irrefleja, asimétrica

$$R_3 = \{(1,2),(3,1))\}$$

Ejemplo 4: Relación "menor e igual"($\leq$)

Sea $a, b \in A$, $\leq$ es asimétrica ya que se cumple:

$$a \leq b \wedge b \leq a \rightarrow a = b$$

Sea $R_4 \subseteq\leq$,

$$R_4 = \{(1,1),(1,2),(1,3),(2,2),(2,3)\}$$

Es claro que además es refleja, transitiva y conexa.

Ejemplo 5: Relación "suboconjunto"($\subseteq$)

Sean A, B conjuntos, $\leq$ es asimétrica ya que se cumple:

$$A \subseteq B \wedge B \subseteq A \rightarrow A = B$$

Ejemplo 6:

Demostración. Demuestre que la relacion | es refleja, antisimetrica transitiva

- Refleja:
  Por demostrar que $\forall a \in \mathbb{N} - \{0\}$ se tiene que $a|a$.
  Para todo a se cumple que $a = a$, por lo tanto $a = 1 * a$ lo cual es la definición de divisor donde $k = 1$.

- Antisimetrica:

$$\forall a, b\big[(a,b) \in R \wedge (b,a) \in R \rightarrow a = b\big]$$

  Por demostrar,

$$\forall a, b\big[\ a|b\ \wedge\ b|a \rightarrow a = b\big]$$

  Usando la definicion,

$$b = k_1 * a\ , k_1 \in \mathbb{N} \tag{9}$$

$$a = k_2 * b \, , k_2 \in \mathbb{N} \tag{10}$$

Reemplazando (9) en (10),

$$a = k_1 * k_2 * a$$

Por lo tanto, $k_1 = k_2 = 1$
Reemplazando en (9),

$$a = b$$

- Transitiva:
  Por demostrar:

  $$\forall a, b, c \big[\, a|b \,\wedge\, b|c \rightarrow a|c \big]$$

  De nuevo, por definicion:

  $$b = k_1 * a \, , k_1 \in \mathbb{N}$$

  $$c = k_2 * b \, , k_2 \in \mathbb{N}$$

  Reemplazando (2.2) en (2.2),

  $$c = k_1 * k_2 * a$$

  Sea $k_1 * k_2 = K$ donde $K \in \mathbb{N}$

  $$c = K * a$$

  Por lo que:

  $$c|a$$

$\square$

2.3. Relaciones de equivalencia:

Definición 2.15. Una relacion R sobre A es una **relacion de equivalencia** si es refleja, simetrica y transitiva.
Notacion: "$\sim$"

Ejemplo:
Demuestre que la relacion equivalencia logica sobre $L(P) \times L(P)$:

$$\varphi \equiv \psi \iff \forall \sigma, \sigma(\varphi) = \sigma(\psi) \tag{11}$$

donde $\varphi, \psi \in L(P)$, es una relacion de equivalencia.

Demostración. $\varphi, \psi, \sigma \in L(P)$

- Refleja:
  Se quiere demostrar que:
  $$\forall \varphi [\varphi \equiv \varphi]$$
  Sabemos que:
  $$\varphi = \varphi$$
  Por lo tanto,
  $$\sigma(\varphi) = \sigma(\varphi)$$
  Y por definición,
  $$\forall [\sigma(\varphi) = \sigma(\varphi)] \iff \varphi \equiv \varphi$$
- Simetrica:
  Se quiere demostrar que:
  $$\forall \varphi, \phi [\varphi \equiv \psi \to \psi \equiv \varphi] \tag{12}$$
  Suponiendo el lado izquierdo,
  $$\varphi \equiv \psi$$
  Entonces,
  $$\sigma(\varphi) = \sigma(\psi)$$
  Por la conmutatividad de la igualdad,
  $$\sigma(\psi) = \sigma(\varphi)$$
  Por definicion de equivalencia logica,
  $$\psi \equiv \varphi$$
  Que es lo que queriamos demostrar en (12).

- Transitiva:
  Se quiere demostrar que:

$$\forall \varphi, \psi, \sigma \big[\varphi \equiv \psi \land \psi \equiv \sigma \to \varphi \equiv \sigma\big]$$

Suponiendo el lado izquierdo, tenemos:

$$\sigma(\varphi) = \sigma(\psi) \tag{13}$$

$$\sigma(\psi) = \sigma(\sigma) \tag{14}$$

Por la conmutatividad de la igualdad, y reemplazando (13) en (14).

$$\sigma(\varphi) = \sigma(\psi)$$

Y por definicion:

$$\varphi \equiv \psi$$

□

Definición 2.16. Clase de equivalencia:
Sea $\sim$ una relacion de equivalencia sobre un conjunto A y un elemento $x \in A$. La **clase de equivalencia** de x bajo $\sim$ es el conjunto:

$$[x]_\sim = \{y \in A | x \sim y\} \tag{15}$$

Propiedades:

1. $\forall x \in A, x \in [x]$

   Demostración. :
   Como $\sim$ es una relación de equivalencia, es refleja:

$$\forall x \in A, x \sim x$$

   Entonces,

$$x \in [x]$$

□

2. $x \sim y \iff [x] = [y]$

   Demostración. :
   ($\to$) Suponemos $x \sim y$,

   Definimos $[x]_\sim$ y $[y]_\sim$,

$$[x]_\sim = \{w \in A | x \sim w\}$$

$$[y]_\sim = \{z \in A | y \sim z\}$$

   Queremos llegar a que $[y] = [x]$, por lo que podemos usar el axioma de extension

$$[x] \subseteq [y] \land [y] \subseteq [x] \to [x] = [y]$$

- $[x] \subseteq [y]$

  Por simetria,
  $$x \sim w \iff w \sim x$$
  Con lo supuesto y por transitividad,
  $$w \sim x \wedge x \sim y \to w \sim y$$
  Por la definicion de clase de equivalencia,
  $$w \in [y]$$
  Como es un w arbitrario $\in A$,
  $$[x] \subseteq [y]$$

- $[y] \subseteq [x]$

  Por simetria,
  $$y \sim z \iff z \sim y$$
  Con el supuesto (reflejo) y por transitividad,
  $$z \sim y \wedge y \sim x \to z \sim x$$
  Por la definicion de clase de equivalencia,
  $$z \in [x]$$
  Como es un z arbitrario $\in A$,
  $$[y] \subseteq [z]$$
  Por lo tanto,$[x] = [y]$

($\leftarrow$) Supondremos $[x] = [y]$,

Si tomamos un z arbitrario que pertenece a $[x]$ y a $[y]$,

Pertenece a $[x]$:
$$z \in [x] \to x \sim z$$
Por simetria,
$$x \sim z \iff z \sim x \tag{16}$$
Pertenece a $[y]$:
$$z \in [y] \to y \sim z \tag{17}$$
Por transatividad de (16) y (17):
$$y \sim z \wedge z \sim x \to y \sim x$$

$\square$

3. Si $[x] \neq [y] \to [x] \cap [y] = \varnothing$

Demostración. :
Por contradicción, supongamos $[x] \neq [y]$ pero $[x] \cap [y] \neq \varnothing$. Entonces existe una z tal que pertenezca a la intersección.
Por la definición de intersección:

$$z \in [x] \wedge z \in [y]$$

Por definición de clase de equivalencia,

$$x \sim z \wedge y \sim z$$

Por simetría y transitividad,

$$x \sim y$$

Por la propiedad 2, esto implica que $[x] = [y]$ lo que contradice lo supuesto y hemos llegado a una contradicción. □

Definición 2.17. Conjunto cuociente:
Sea $\sim$ una relacion de equivalencia sobre un conjunto A. El **conjunto cuociente** de A con respecto a $\sim$ es el conjunto de todas las clases de equivalencia de $\sim$:

$$A/\sim = \{\ [x]\ | x \in A\}$$

Ejemplo:

Determine $\mathbb{N}/\equiv_4$:
(El conjunto de clases de equivalencias de la relación de equivalencia modulo 4 en $\mathbb{N}$).

$$[x]_{\equiv_4} = \{y \in \mathbb{N} | x \equiv_4 y\}$$
$$[0]_{\equiv_4} = \{4, 8, 12, ...\}$$
$$[1]_{\equiv_4} = \{1, 5, 9, ...\}$$
$$[2]_{\equiv_4} = \{2, 6, 10, ...\}$$
$$[3]_{\equiv_4} = \{3, 7, 11, ...\}$$
$$[4]_{\equiv_4} = \{4, 8, 12, ...\}$$
$$[0]_{\equiv_4} = [4]_{\equiv_4}$$

Por lo que se empieza a repetir las clases de equivalencia a partir de $[3]_{\equiv_4}$, y como los conjuntos no tienen elementos repetidos:

$$\mathbb{N}/\equiv_4 = \{[0], [1], [2], [3]\}$$

Definición 2.18. Índices en relaciones de equivalencia:
El **índice** de una relacion de equivalencia es la cantidad de clases de equivalencia que induce. Es decir, la cantidad de elementos de su conjunto cuociente.

Ejemplo:

En el ejemplo anterior, el modulo 4 (índice) en $\mathbb{N}$ induce 4 clases de equivalencia
Definición 2.19. Partición:
Sea A conjunto cualquiera y S colección de subconjuntos de A. S es **partición** de A si:

1. $\forall X \in S, X \neq \varnothing$

2. $\bigcup S = A$

3. $\forall X, Y \in S, X \neq Y$ entonces $X \cap Y = \varnothing$

Teorema 2.1. *Si $\sim$ es una relacion de equivalencia sobre un conjunto A, entonces $A/\sim$ es una partición de A.*

Demostración. Sabemos que,

$$A/\sim = \{\ [x]\ |x \in A\}$$

1. *Demostración.* Por demostrar que:

$$\forall X \in A/\sim, X \neq \varnothing$$

Por lo por la propiedad (1) de clases de equivalencia que:

$$\forall x \in A, x \in [x]$$

Esto implica que $[x] \neq \varnothing$. Y como el conjunto cuociente solo tiene clases de equivalencia, estas no son vacias.

$$\forall X \in A/\sim, X \neq \varnothing$$

□

2. *Demostración.* Por demostrar que:

$$\bigcup(A/\sim) = A \tag{18}$$

Dada la igualdad de conjuntos, se demostrara mediante el axioma de extensión.

- $\bigcup(A/\sim) \subseteq A$

$$x \in \bigcup(A/\sim) \rightarrow x \in Y, Y \in A/\sim$$

Donde Y es una clase de equivalencia. Por la definición de conjunto cuociente, "y"debe pertenecer a A.

$$x \in [y], y \in A$$

Por lo tanto,

$$x \in A$$

- $A \subseteq \bigcup(A/\sim)$ Tomando un x cualquiera en A, dada la propiedad (1) de clases de equivalencia.

$$x \in A \rightarrow x \in [x]$$

Por la definición de conjunto cuociente

$$[x] \in A/\sim \rightarrow \forall y \in [x], y \in \bigcup(A/\sim)$$

Un caso particular de y es x,

$$x \in \bigcup(A/\sim)$$

□

Por lo tanto, usando el axioma de extensión:

$$\bigcup(A/\sim) \subseteq A \wedge A \subseteq \bigcup(A/\sim) \to A = \bigcup(A/\sim)$$

3. $\forall X, Y \in A/\sim, si X \neq T$ entonces $X \cap Y = \varnothing$

Demostración. Como X,Y son conjuntos de equivalencia por teorema se cumple propiedad □

Como el conjunto cuociente cumple las tres propiedades de una particion, este es una particion a A. □

Teorema 2.2. *Sea S una particion cualquiera de A, entonces la relacion,*

$$x \sim y \iff \exists X \in S \; tal \; que \; \{x, y\} \subseteq X$$

es una relacion de equivalencia sobre A.
Un elemento x esta relacionado con y si ambos pertenecen al mismo conjunto de la particion.

Demostración. Por demostrar que es una relación de equivalencia:

- Refleja: Dado un $x \in A$ arbitrario, como S es particion:

  $$\exists Y \in S \text{ tal que } x \in Y$$

  Es equivalente a decir,

  $$\{x\} \subseteq Y \iff \{x, x\} \subseteq Y$$

  Y por el Teorema 2.2,

  $$x \sim x \iff \{x, x\} \subseteq Y$$

- Simétrica:

  $$x \sim y \to y \sim x$$
  $$\exists X \in S \text{ tal que } \{x, y\} \subseteq X \tag{19}$$

  Ya que S, es una particion de A

  $$\exists X \in S \text{ tal que } \{y, x\} \subseteq X$$

  Por lo que,

  $$y \sim x$$

- Transitividad:

  $$\exists X_1 \in S \text{ tal que } \{x, y\} \subseteq X_1$$
  $$\exists X_2 \in S \text{ tal que } \{y, z\} \subseteq X_2$$

  Por lo que,

  $$\{y\} \subseteq X_1 \cap X_2$$

Y por propiedad de partición

$$X_1 \cap X_2 \neq \varnothing \rightarrow X_1 = X_2$$

Por lo tanto,

$$\{x, y\} \in X_1 \wedge \{y, z\} \in X_1 \rightarrow \{x, z\} \in X_1$$

Y por definicion,

$$x \sim z \tag{20}$$

□

2.4. Construccion de conjuntos:

Ejemplo:
Definamos $\mathbb{N}_4$ como el conjunto cuociente de $\mathbb{N}$ modulo 4.

- $$\mathbb{N}_4 = \mathbb{N}/\equiv_4 = \{[0],[1],[2],[3]\}$$
- La suma modulo 4:
$$\begin{aligned}[i] +_4 [j] &= [i+j] \\ [3] +_4 [1] &= [4] = [0] \end{aligned} \tag{21}$$
- La multiplicacion modulo 4:
$$\begin{aligned}[i] *_4 [j] &= [i*j] \\ [3] *_4 [2] &= [6] = [2] \end{aligned} \tag{22}$$

Definición 2.20. La relación $\downarrow$ sobre $\mathbb{N}\times\mathbb{N}$ ($\mathbb{N}^2$) como:

$$(m,n)\downarrow(r,s) \iff m+s=n+r \iff m-n=r-s$$

Demostración. Por demostrar que $\downarrow$ es una relacion de equivalencia,

- Refleja:
$$(m,n)\downarrow(m.n) \iff m+n=m+n$$
Lo que claramente se cumple
- Simétrica: Se quiere demostrar:
$$(m,n)\downarrow(r,s)\rightarrow(r,s)\downarrow(m,n)$$
Tenemos que,
$$(m,n)\downarrow(r,s) \iff m-n=r-s \iff m+s=r+n \iff r+n=m+s \iff r-s=m-n$$
Por lo que,
$$r-s=m-n \iff (r,s)\downarrow(m,n)$$
- Transitividad: Se quiere demostrar:
$$(a,b)\downarrow(c,d)\wedge(c,d)\downarrow(e,f)\rightarrow(a,b)\downarrow(e,f)$$
De el lado izquerido tenemos 2 igualdades:
$$a-b=c-d \tag{23}$$
$$c-d=e-f \tag{24}$$
Remplazando (23) en (2.4):
$$a-b=e-f$$
Por lo tanto,
$$a-b=e-f \iff (a,b)\downarrow(e,f)$$

Por lo tanto, $\downarrow$ es una relacion de equivalencia. $\square$

Definición 2.21. Suma clase de equivalencia $\downarrow$:

$$[(m,n)] +_{\downarrow} [(r,s)] = [(m+r, n+s)]$$

Definición 2.22. Multiplicacion clase de equivalencia $\downarrow$:

$$[(m,n)] *_{\downarrow} [(r,s)] = [(m*s+n*r, m*r+n*s)]$$

2.5. Relaciones de orden

Definición 2.23. Una relación R sobre A es una **relación de orden parcial** si es refleja, antisimetrica y transitiva.
Notacion:

$$(x, y) \in \preceq,\ x \preceq y$$

Si $\preceq$ es una relación de orden parcial sobre A, diremos que el par $(A, \preceq)$ es un **orden parcial**.

Definición 2.24. Una relacion R es una **relación de orden total** si es una relación de orden parcial y además es conexa.

$$\forall x, y \in A, \text{ se tiene que } x \preceq y \vee y \preceq x$$

Si $\preceq$ es una relación de orden total sobre A, diremos que el par $(A, \preceq)$ es un **orden total**.

Definición 2.25. Sean $(A, \preceq)$ un orden parcial, $S \subseteq A$ $x \in A$:

1. x es **cota inferior** de S si:

$$\forall y \in S \rightarrow x \preceq y$$

   (Notar que x puede estar afuera de S)

2. x es **elemento minimal** de S si $x \in S$:

$$\forall y \in S(y \preceq x \rightarrow y = x)$$

3. x es **mínimo** si $x \in S$ y además es cota inferior

Definición 2.26. Sean $(A, \preceq)$ un orden parcial, $S \subseteq A$ $x \in A$:

1. x es **cota superior** de S si:

$$\forall y \in S \rightarrow y \preceq x$$

   (Notar que x puede estar afuera de S)

2. x es **elemento maximal** de S si $x \in S$:

$$\forall y \in S(x \preceq y \rightarrow y = x)$$

3. x es **máximo** si $x \in S$ y además es cota superior

Teorema 2.3. *Sea $(A, \preceq)$ un orden parcial y $S \subseteq A$ no vacio. Si S tiene un elemento minimo, este es único.*

Demostración. Por contradiccion, supongamos que existen dos elementos minimos: s_1, s_2, entonces:

$$s_1 \in S \wedge s_2 \in S \to \text{minimos}$$

Luego por antisimetria del orden parcial,

$$s_1 \preceq s_2 \wedge s_2 \preceq s_1 \to s_1 = s_2$$

Lo que contradice la duplicidad de mínimos supuesta. □

Notacion: Esto nos permite hablar de el mınimo o el máximo, que denotaremos por $min(S)$ y $max(S)$ respectivamente

Definición 2.27. Ínfimo:
Sea $(A, \preceq)$ un orden parcial y $S \subseteq A$ Diremos que s es un **ínfimo** de S si es una cota inferior, y para cualquier otra cota inferior S' se tiene que $S' \preceq S$. Es decir, el ínfimo es la mayor cota inferior.
Análogamente se define el **supremo** de un conjunto.

Ejemplo:
No hay supremo

$$(\mathbb{Q}, \leq) \text{ y } S = \{q \in \mathbb{Q} | q^2 < 2\}$$

Teorema 2.4. *Sea $(A, \preceq)$ un orden parcial y $S \subseteq A$. Si S tiene un supremo o ínfimo, este es único.*

Demostración. Por contradiccion,
Supondremos que existen s_1, s_2 supremos tal que $s_1 \neq s_2$, entonces s_1, s_2 son cotas superiores.
Si s_1 es supremo, entonces para toda cota superior s'

$$s_1 \preceq s' \to s_1 \preceq s_2$$

Si s_2 es supremo, entonces para toda cota superior s'

$$s_2 \preceq s' \to s_2 \preceq s_2$$

Por antisimetria,

$$s_1 = s_2$$

Lo que contradice lo supuesto. □

Notacion: Esto nos permite hablar de el mınimo o el máximo, que denotaremos por $sup(S)$ y $inf(S)$ respectivamente

Definición 2.28. Sea $(A, \preceq)$ un orden parcial. Este se dice **superiormente completo** si para cada $S \subseteq A$ no vacio, si S tiene cota superior, entonces tiene supremo.
De manera similar definimos el concepto de ser **inferiormente completo**.

Teorema 2.5. $(A, \preceq)$*es superiormente completo si y solo si es inferiormente completo*

3. Funciones y Cardinalidad

3.1. Funciones

Definición 3.1. Función:
Sea f una relacion binaria de A en B; Es decir $f \subseteq A \times B$.Diremos que f es una **función** de A en B si dado cualquier elemento $a \in A$, si existe un elemento $b \in B$ tal que $a\ f\ b$, este es único:

$$a\ f\ b \wedge a\ f\ c \rightarrow b = c$$

Notacion: Si $a\ f\ b$, se escribe como: $b = f(a)$.

- b es la *imagen* de a
- a es la *preimagen* de b

$$f : A \rightarrow B \Rightarrow f(a) = b \iff a\ f\ b$$

Definición 3.2. Función total:
Una función se dice **total** si para todo elemento a en el dominio existe un b tal que $f(a) = b$. Si no cumple lo anterior, se dice que es una funcion **parcial**.

Ejemplo:

Se puede definir funciones entre un conjunto y su conjunto potencia:

$$f : A \rightarrow P(A)$$

- $\forall a \in A, f_1(a) = \{a\}$
- $\forall a \in A, f_2(a) = A - \{a\}$
- $\forall a \in A, f_3(a) = \varnothing$

Definición 3.3. Caracteristicas de funciones:
Sea $f : A \rightarrow B$, $a \in A$ y $b \in B$.

1. Inyectiva: f es inyectiva si:
$$\forall a_1, a_2 \in A.\big[f(a_1) = f(a_2) \rightarrow a_1 = a_2\big]$$
Es decir, no existen dos elementos distintos en A con la misma imagen.

2. Sobreyectiva: f es sobreyectiva si:
$$\forall b.\big[\exists a \in A \text{ tal que } f(a) = b\big]$$
Si cada elemento b tiene preimagen a

3. Biyectiva: f es biyectiva si:
    - Si es inyectiva y sobreyectiva a la vez.
    - Si f es una funcion biyectiva entonces su inversa f^{-1} tambien lo es.

- La composicion de funciones biyectivas también es biyectiva ($f \circ g$)

Ejemplo 1:

Demostración. Sea $f : A \to P(A) : f(a) = \{a\}$. Por demostar que e f es inyectiva.

$$\forall a_1, a_2 \in A, \text{ se tiene que } f(a_1) = f(a_2) \to a_1 = a_2$$

Supongamos a_1 y a_2 arbitrarios, tales que:

$$f(a_1) = f(a_2)$$

Por definicion de la funcion:

$$\{a_1\} = \{a_2\}$$

Luego por axioma de extensión,

$$a_1 = a_2$$

Entonces,

$$\forall a_1, a_2 \in A, \text{ se tiene que } f(a_1) = f(a_2) \to a_1 = a_2$$

□

No es sobreyectiva ya que el conjunto vacio no tiene preimagen y por lo lo tanto no puede ser biyectiva.

Ejemplo 2:

Sea $f : A \to P(A), \forall a \in A, f(a) = \varnothing$, no es inyectiva ya que existen distintos a con la misma imagen $\varnothing$. Tampoco es sobreyectiva.

Ejemplo 3:

Sea $f : \mathbb{N} \to \mathbb{N}_4, \forall n \in N, f(n) = n \bmod 4$, no is inyectiva ya que por ejemplo:

$$[0] = [4]$$

Pero si es sobreyectiva porque cada imagen tiene al menos una preimagen.

Ejemplo 4:

Sea $f : \mathbb{N}_4 \to \mathbb{N}_4, \forall n \in \mathbb{N}_4; f(n) = (n + 2) \bmod 4$, es inyectiva ya que cada n tiene una solo una imagen.

$$f([0]) = [2]$$
$$f([1]) = [3]$$
$$f([2]) = [0]$$
$$f([3]) = [1]$$

Tambien es sobreyctiva ya que no existe un $[n]$ que no tenga preimagen. Por lo tanto, como es inyectiva y sobreyectiva, esta es biyectiva.

Teorema 3.1. *Principio de palomar:*
Sea $f : \mathbb{N}_m \to \mathbb{N}_n$, si $m > n$ entonces la funcion nunca sera inyectiva.
Es decir, necesariamente existiran $x, y \in \mathbb{N}_m$ tales que $x \neq y$, pero $f(x) = f(y)$.

Teorema 3.2. *Principio de palomar (para sobreyectividad):*
Sea $f : \mathbb{N}_m \to \mathbb{N}_n$, con $m < n$ entonces la funcion no puede ser sobreyectiva.

Corolario:
La unica forma que la funcion $f : \mathbb{N}_m \to \mathbb{N}_n$ sea biyectiva es que $m = n$.

Ejemplo 4:
Supongamos 30 alumnos y 7 dias, ¿Es posible que dos esten de cumpleaños el mismo dia? Si, pues $f : \mathbb{N}_30 \to \mathbb{N}_7$ no es inyectiva

3.2. Cardinalidad de conjuntos finitos

Definición 3.4. Sean A, B conjuntos. A es **equinumeroso** a B si y solo si existe $f : A \to B$ biyectiva.

$$A \approx B$$

A y B tienen el mismo tamaño si los elementos de A se pueden poner en correspondencia con los de B
Teorema 3.3. *La relacion "$\approx$."es una relacion de equivalencia.*

Demostración. :

- Refleja:
  Se quiere demostra que:

  $$\forall A\big[A \approx A\big]$$

  Si tomamos un A arbitrario, existe $f : A \to A$. Donde $f(a) = a, \forall a$, por lo tanto es una función inyectiva y sobreyectiva. Lo que implica que es biyectiva y se puede concluir que $A \approx A$, como tomamos un A arbitrario mediante generalización universal esto se cumple para cualquier conjunto.

- Simetrica:
  Se quiere demostrar que:

  $$\forall A, B\big[A \approx B \to B \approx A\big]$$

  Tomando el lado izquierdo $A \approx B$, entonces existe una función biyectiva tal que $f : A \to B$. Como esta funcion es invertible, tambien se cumple que $f^{-1} : B \to A$ es biyectiva y por lo ultimo $B \approx A$

- Transitiva:
  Se quiere demostrar que:

  $$\forall A, B, C\big[A \approx B \land B \approx C \to A \approx C\big]$$

  Tenemos que $A \approx B$ y $B \approx C$, por lo tanto existen las funciones biyectivas $f : A \to B$ y $g : B \to C$. La composición de funciones biyectivas también es biyectiva,por lo tanto dada la función $f \circ g : A \to C$ se puede concluir que $A \approx C$

□

Definición 3.5. La **cardinalidad** de un conjunto $A \subseteq S$ es un clase de equivalencia bajo $\approx$:

$$|A| = [A]_{\approx} = \{B \subseteq S | A \approx B\}$$

Por lo tanto, si A es equinumerosos con B entonces se que cumple por la propiedad (2) de clases de equivalencia que:

$$A \approx B \iff [A]_{\approx} = [B]_{\approx}$$

Lo que implica que:

$$|A| = |B|$$

Definición 3.6. Diremos que A es un conjunto **finito** si $A \approx n$, para algún $n \in \mathbb{N}$. Es decir, si existe una funcion biyectiva $f : A \to n = \{0, ..., n-1\}$
Se tiene que, $|A| = [n]_{\approx} = |n| = n$. Es decir, A tiene n elementos.

Lema 3.1. *Sean A y B conjuntos finitos tales que $A \cap B = \varnothing$ (Disjuntos). Entonces $|A \cup B| = |A| + |B|$*

Demostración. Por demostrar que $|A \cup B| = |A| + |B|$:
Sea $f : A \to \mathbb{N}_n$ y $g : B \to \mathbb{N}_m$ donde,:

$$A = \{a_1, ..., a_n\}$$
$$B = \{b_1, ..., a_m\}$$

Por lo tanto:

$$A \cup B = \{a_1, ..., a_n, b_1, ..., a_m\}$$

y,

$$\mathbb{N}_{m+n} = \{0, ..., n-1, n, ..., n + (m-1)\}$$

Entoces consideremeos la siguiente funcion:

$$h(x) = \begin{cases} f(x) & x \in A \\ g(x) + n & x \in B \end{cases}$$

Donde $h : A \cup B \to \mathbb{N}_{n+m}$.
Luego si h es una funcion biyectiva, entonces se cumple que $|A \cup B| = |A| + |B| = n + m$
Se debe notar que como A y B son conjuntos finitos, estos cumplen la definición (3.6) entonces f y g son funciones biyectivas.

1. <u>Inyectiva:</u> Sean $x_1, x_2 \in A \cup B$ arbitrarios. suponemos $h(x_1) = h(x_2)$.
   Se quiere demostrar que:

   $$\forall x_1, x_2 \in A \cup B. \big[h(x_1) = h(x_2) \to x_1 = x_2\big]$$

   a) $h(x_1) = h(x_2) < n$
   Por lo tanto $x_1, x_2 \in A$

   $$h(x_1) = f(x_1) = f(x_2) = h(x_2) \to x_1 = x_2$$

   Entonces f es inyectiva y h entonces también lo es para este caso.

   b) $h(x_1) = h(x_2) \geq n$
   Por lo tanto $x_1, x_2 \in B$
   $$h(x_1) = g(x_1) + n = g(x_2) + n = h(x_1)$$
   Entonces,
   $$g(x_1) = g(x_2) \to x_1 = x_2$$
   g es biyectiva y necesariamente inyectiva, por lo tanto h tambien lo es para este caso.

2. <u>Sobreyectiva:</u> Tomemos un $k \in \mathbb{N}_{n+m}$ arbitrario, entonces por demostrar que $h(x) = k$ o que:

   $$\forall k. \big[\exists x \in A \cup B \text{ tal que } h(x) = k\big]$$

   a) $k < n \to x \in A$
   Por lo tanto,
   $$h(x) = f(x)$$

f es biyectiva y necesariamente sobreyectiva, por lo tanto se cumple que:

$$\forall k. \big[\exists x \in A \text{ tal que } f(x) = k \big]$$

Por lo que se puede conlcuir,

$$h(x) = f(x) = k$$

y h es sobreyectiva para este caso.

b) $n \leq k < n + m \rightarrow x \in B$
Por lo que,

$$h(x) = g(x) + n$$

g es biyectiva y necesariamente sobreyectiva, por lo tanto se cumple que:

$$\forall c. \big[\exists x \in B \text{ tal que } g(x) = c \big]$$

Donde c se define como:

$$n \leq k < m + n$$
$$0 \leq k - n < m$$

entonces $c = k - n$
Por lo tanto, se puede concluir que:

$$h(x) = g(x) = k - n$$
$$h(x) = g(x) + n = k$$

Entonces, h también es sobreyectiva para el segundo caso.

Dado que h es inyectiva y sobreyectiva, podemos concluir que es biyectiva.
Queda demostrado que $|A \cup B| = |A| + |B| = n + m$ $\square$

Teorema 3.4. *Sea A un conjunto finito. Entonces se cumple que $|P(A)| = 2^{|A|}$*
Esto implica que $|A| < |P(A)|$

3.3. Cardinalidad de conjuntos infinitos

Ejemplo:
Sea $\mathbb{P} = \{2k|k \in \mathbb{N}\}$ el conjunto de numeros naturales pares. ¿Cual conjunto es mas grande, $\mathbb{N}$ o $\mathbb{P}$?
Sea $f : \mathbb{N} \to \mathbb{P}$ definidad como $f(x) = 2 * x$, luego $\mathbb{N} \approx \mathbb{P}$ y tienen la **misma cantidad de elementos**

Teorema 3.5. *A es un conjunto enumerable si $|A| = |\mathbb{N}|$*

Teorema 3.6. *Schröder-Bernstein $A \approx B$ si y solo si existen funciones inyectivas:*

$$f : A \to B \; y \; g : B \to A$$

Definición 3.7. Un conjunto A es enumerable si y solo si todos sus elementos se pueden poner en una lista infinita; es decir, si existe una sucesion infinita:

$$(a_0, a_1, a_2, ..., a_n, a_{n+1}, ...) \tag{25}$$

Tal que *todos* los elementos de A aparecen en la sucecion *una unica vez* cada uno.
Tambien puedo formar $f : \mathbb{N} \to A$ con $f(n) = a_n$ y A es enumerable

Ejemplo:
Demostar que $\mathbb{N} \times \mathbb{N}$ es enumerable:

```
suma=0
while true:
    i=0
    for i <= suma:
        print(i,suma-i)
    suma +=1
```

Teorema 3.7. *Teorema de Cantor:*
El intervalo real $(0, 1) \subseteq \mathbb{R}$ es infinito pero no es enumerable.

4. Analisis de Algoritmos