

Álgebra y

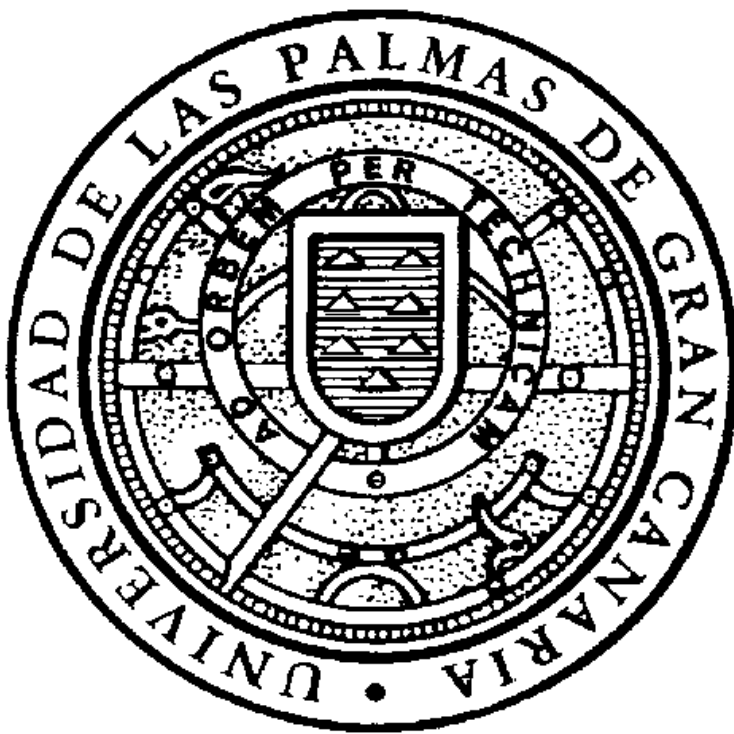
Matemática

Discreta

Curso: 1º

Ingeniería Técnica Informática de Sistemas

Universidad de Las Palmas de Gran Canaria



Lógica Proposicional

Término: Sinónimo de palabra (con significado propio o no).

Proposición Lógica: Agrupación de términos de la que se puede averiguar si su contenido es verdadero o falso. Ej: La mesa es redonda ; $3 + 2 = 5$

Clasificación

- **Atómicas:** Si no puede subdividirse en otras proposiciones más pequeñas y siempre son afirmativas. Ej: Está lloviendo ; $3 + 2 = 5$
- **Moleculares:** Pueden subdividirse en otras proposiciones enlazadas y/o modificadas por algunos términos. Ej: Llueve y es de día

La mesa no es redonda No la mesa es redonda Molecular

Conectores Proposicionales

Términos usados para enlazar y/o modificar.

1. Negación: NO Símbolo: $\neg$ Conector monádico
2. Conjunción: Y y Símbolo: $\wedge$
3. Disyunción No Exclusiva: o Símbolo: $\vee$
4. Disyunción Exclusiva: o o Símbolo: $\oplus$
5. Condicional: si entonces Símbolo: $\rightarrow$
6. Bicondicional: si y sólo si Símbolo: $\leftrightarrow$

Del 2 al 6 son conectores Diádicos.

Formulación Algebraica

Para las proposiciones atómicas se utilizan variables proposicionales que van de la p a la z .

Para las moleculares se utilizan fórmulas lógicas que van de la P a la Z .

Está lloviendo = p Si llueve entonces me mojo = q

Valor Lógico de una Proposición: 0 cuando es falsa y 1 cuando es verdadera.

Álgebra de Proposiciones

Se encarga de la construcción y estudio de las proposiciones. Se basa en:

Axioma 1: Toda proposición es verdadera o falsa.

Axioma 2: Toda proposición molecular tendrá un valor de verdadero o falso dependiendo de las proposiciones atómicas que la compongan y de los conectores que la modifican y/o enlazan.

Axioma 3: El valor lógico de las proposiciones se establece en unas tablas llamadas tablas de verdad.

Reglas de Inferencia

Argumento Deductivo: Conjunto de proposiciones, una de ellas llamada conclusión que se sigue del resto, llamadas premisas.

p, q premisas

p

q conclusión

$p1$

p2

.

. [p1, p2, .. , pn] ! C

pn

C

Un argumento es válido cuando, siendo ciertas las premisas, la conclusión no puede ser falsa.

Deducción Formal

Es una secuencia finita de fórmulas de forma que a partir de las premisas llegamos a la conclusión. Estas fórmulas pueden ser:

- Premisas
- Supuestos Provisionales: Fórmula que se introduce transitoriamente y ha de ser cancelada antes de llegar a la conclusión.
- Fórmulas de Nueva Creación: Fórmulas que se crean a partir de las reglas de inferencia.

♦ Clasificación

A). Reglas Básicas de Inferencia: El mínimo conjunto de reglas necesario para llevar a cabo cualquier deducción formal. (Gentzen 1934)

Condicional:

De Inserción: Teorema de la Deducción (TD) p

.

.

q_____

p ! q

De Eliminación: Modus Ponens (MP). Si el antecedente vale 1, el consecuente tiene que valer 1.

p ! q

p_____

q

Conjunción:

De Inserción: Producto (Prod). Si p vale 1 y q vale 1, p " q tiene que valer

• p

q

p " q

De Eliminación: Simplificación (Simp) $\frac{p \text{ " } q \quad p \text{ " } q}{p \quad q}$

p q

Disyunción No Exclusiva:

De Inserción: Adición (Ad) $\frac{p}{p \text{ " } q} \quad \frac{q}{p \text{ " } q}$

p " q p " q

De Eliminación: Casos (Cas) $\frac{p \text{ " } q \quad p \quad q}{p}$

.

.

r

q

.

.

r

r

Negación:

De Inserción: Absurdo (Abs) $\frac{p \quad \neg p}{p}$

.

.

$\frac{q \quad \neg q}{q}$

$\neg p$

De Eliminación: Doble Negación (DN) $\frac{\neg \neg p}{p}$

p

Bicondicional:

De Inserción: Introducción del Coimplicador (ICO) $p \rightarrow q$

$q \rightarrow p$

$p \rightarrow q$

De Eliminación: Eliminación del Coimplicador (ECO) $p \rightarrow q, p \rightarrow q$

$p \rightarrow q, q \rightarrow p$

El símbolo que se utiliza para representar los conectores lógicos se llama conectiva lógica.

Operación Lógica

Es la aplicación de operadores para modificar y/o enlazar proposiciones y generar una nueva proposición.

1. *Negación*: Se aplica el operador ($\neg$) a una proposición para cambiar su valor de verdad.

p	$\neg p$
1	0
0	1

2. *Conjunción*: Se aplica el operador ($\wedge$) a dos proposiciones $p \wedge q$. Vale 1 sólo cuando las dos proposiciones valen 1.

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

3. *Disyunción No Exclusiva*: Se aplica el operador ($\vee$) a dos proposiciones. Vale 1 cuando al menos una de las variables vale 1.

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

4. *Disyunción Exclusiva*: Se aplica el operador ($\oplus$) a dos proposiciones. Vale 1 cuando sólo una de las variables vale 1.

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

5. *Condicional*: Se aplica el operador (!) a dos proposiciones. Vale 1 siempre, excepto cuando el antecedente vale 1 y el consecuente 0.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

6. *Bicondicional*: Se aplica el operador (!) a dos proposiciones. Vale 1 cuando ambas variables tienen el mismo valor lógico.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Ecuaciones

$$p \rightarrow q \equiv \neg(p \wedge \neg q) \quad p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

Hay que tener en cuenta los paréntesis y darles prioridad.

$$(p \rightarrow q) \wedge (q \rightarrow p) = p \leftrightarrow q$$

p	q	$(p \rightarrow q)$ (1)	$(q \rightarrow p)$ (2)	$1 \rightarrow 2$	
0	0	1	1	1	Propiedad indeterminada o
0	1	1	0	0	contingente (puede ser
1	0	0	1	0	verdadera o falsa)
1	1	1	1	1	

$$p \leftrightarrow \neg p$$

p	$\neg p$	$p \leftrightarrow \neg p$	
1	0	0	!
0	1	0	

$$q \leftrightarrow \neg q$$

q	$\neg q$	$q \leftrightarrow \neg q$	
1	0	0	!
0	1	0	

Se llama implicación tautológica a un condicional tautológico (!).

$(p \rightarrow q) \rightarrow (\neg p \rightarrow \neg q)$

REGLAS DERIVADAS

Silogismo (Sil). $A \rightarrow B$

$B \rightarrow C$

$A \rightarrow C$

Regla de Mutación (Mut). $A \rightarrow (B \rightarrow C)$

$B \rightarrow (A \rightarrow C)$

Identidad (Id). A

A

Contraposición (CPr). A

$B \rightarrow A$

Dilema (Dil). Dil1. $A \rightarrow B$ Dil2. $\neg A \rightarrow \neg B$

$A \rightarrow C$ $C \rightarrow A$

$B \rightarrow C$ $C \rightarrow B$

$C \rightarrow C$

Dil3. $\neg A \rightarrow \neg B$

$C \rightarrow A$

$D \rightarrow B$

$\neg C \rightarrow \neg D$

Modus Tollens (MT). $A \rightarrow B$

$\neg B$

$\neg A$

Introducción Doble Negación (IDN). A

$\neg \neg A$

ECQ. $A \rightarrow \neg A$

B

Silogismo Disyuntivo (SD). $A \vee B$

$\neg A$

B

Principio No Contradicción (PNC) TEOREMA

Teorema: Argumento deductivo con 0 premisas.

PTE: $A \vee \neg A$

De Morgan (DM) $\neg(A \vee B)$ $\neg(A \vee B)$

$\neg A \vee \neg B$ $\neg A \vee \neg B$

Identidad (IDN) A - 1. A

$\neg\neg A$ 2. $\neg A$

3. $A \vee \neg A$ Prod 1,2

4. $\neg\neg A$ Abs 2-3

ECQ A $\neg A$ - 1. $A \vee \neg A$

B 2. $\neg B$

3. A Simp 1

4. $\neg A$ Simp 1

5. $A \vee \neg A$ Prod 3, 4

6. $\neg\neg B$ Abs 2 - 5

7. B DN 6

$[(p \vee r) \vee (q \vee s)] [(p \vee q) \vee (r \vee s)]$

1. $[(p \vee r) \vee (q \vee s)]$

2. $p \vee q$

3. p Simp 2

4. q Simp 2

5. p $\vee$ r Simp 1

6. q $\vee$ s Simp 1

7. $r \text{ MP } 5, 3$

8. $s \text{ MP } 6, 4$

9. $r \text{ " } s \text{ Prod } 7, 8$

10. $(p \text{ " } q) (r \text{ " } s)$

11. $[(p \text{ r}) \text{ " } (q \text{ s})] [(p \text{ " } q) (r \text{ " } s)]$

PTE: $A \text{ " } \neg A$ 1. $\neg(A \text{ " } \neg A)$

2. A

3. $A \text{ " } \neg A \text{ Ad } 2$

4. $(A \text{ " } \neg A) \text{ " } \neg(A \text{ " } \neg A) \text{ Prod } 3, 1$

5. $\neg A$

6. $A \text{ " } \neg A \text{ Ad } 5$

7. $(A \text{ " } \neg A) \text{ " } \neg(A \text{ " } \neg A) \text{ Prod } 6, 1$

8. $\neg\neg(A \text{ " } \neg A) \text{ Abs } 1 - 7$

9. $A \text{ " } \neg A \text{ DN } 8$

$p \text{ r } -1. p \text{ r } 8. s$

$\neg q \text{ s } -2. \neg q \text{ s } 9. \neg s \text{ SD } 3, 6$

$r \text{ " } \neg s -3. r \text{ " } \neg s 10. s \text{ " } \neg s \text{ Prod } 8, 9$

$\neg r \text{ " } t -4. \neg r \text{ " } t 11. \neg s \text{ Abs } 8 - 10$

$\neg t -5. \neg t 12. \neg\neg q \text{ MT } 2, 11$

$\neg p \text{ " } q 6. \neg r \text{ SD } 4, 5 13. q \text{ DN } 12$

7. $\neg p \text{ MT } 1, 6 14. \neg p \text{ " } q \text{ Prod } 7, 13$

$\neg(A \text{ " } B)$ - 1. $\neg(A \text{ " } B)$

$\neg A \text{ " } \neg B 2. \neg(\neg A \text{ " } \neg B)$

3. A

4. B

5. $A \text{ " } B \text{ Prod } 3, 4$

6. $(A \rightarrow B) \rightarrow \neg(A \rightarrow B)$ Prod 5, 1
7. $\neg B$ Abs 4 – 6
8. $\neg A \rightarrow \neg B$ Ad 7
9. $(\neg A \rightarrow \neg B) \rightarrow \neg(\neg A \rightarrow \neg B)$ Prod 8, 2
10. $\neg A$ Abs 3 – 9
11. $\neg A \rightarrow \neg B$ Ad 10
12. $(\neg A \rightarrow \neg B) \rightarrow \neg(\neg A \rightarrow \neg B)$ Prod 11, 2
13. $\neg\neg(\neg A \rightarrow \neg B)$ Abs 2 – 12
14. $\neg A \rightarrow \neg B$ DN 13
- $(p \rightarrow q) \rightarrow (s \rightarrow t)$ 1. $(p \rightarrow q) \rightarrow (s \rightarrow t)$ 9. $\neg t$ MT 2, 8
- $t \rightarrow r$ 2. $t \rightarrow r$ 10. $\neg s \rightarrow \neg t$ Prod 4, 9
- $\neg(r \rightarrow q)$ 3. $\neg(r \rightarrow q)$ 11. $\neg(s \rightarrow t)$ DM 10
- $\neg s \rightarrow \neg q$ 4. $\neg s$ 12. $\neg(p \rightarrow q)$ MT 1, 11
5. q 13. $\neg p \rightarrow \neg q$ DM 12
6. $\neg r \rightarrow \neg q$ DM 3 14. $\neg q$ Simp
7. $\neg\neg q$ IDN 5 15. $q \rightarrow \neg q$ Prod 5, 14
8. $\neg r$ SD 6, 7 16. $\neg q$ Abs 5 – 15
17. $\neg s \rightarrow \neg q$ TD 4 – 16

Conjuntos

Conjunto: Colección o reunión de objetos.

Elemento: Cada uno de los objetos de un conjunto.

Simbología

Mayúsculas Conjunto Minúsculas Elemento

$x \in A$ x pertenece o está en A .

Determinación de un Conjunto

a). Por extensión: Citando todos los elementos que caen en el conjunto.

$A = \{a, e, i, o, u\}$

b). Por comprensión: dando una propiedad característica (todos se pueden definir por esa característica). $A = \{\text{vocales}\}$

- Conjunto Vacío: es el conjunto formado por 0 elementos. ($\emptyset$)
- Conjunto Unitario: es el conjunto formado por 1 elemento. $A = \{1\}$ $A = \{x\}$

Representación Gráfica

Diagrama de Venn:

$a \in A$ $a \notin A$

$i \in A$ $o \notin A$

$u \in A$

Simbología Algebraica

$\forall$. Cuantificador universal (para todo, para cualquier).

$\therefore$. Se verifica que..

$\exists$. Cuantificador existencial (existe algún, existe al menos uno...).

$\nexists$. No existe ningún...

$\exists!$. Existe un único...

$\wedge$. Tal que...

$\Rightarrow$. Implicación lógica

$\Leftrightarrow$. Si y sólo si...

$\subset$. Subconjunto de... ; Está incluido en...

$\cup$. Conjunción $\vee$. Disyunción

Subconjunto

A es subconjunto de B, si todo elemento de A también está en B.

Partes de un conjunto

Sea $A \subseteq E$. $\mathcal{P}(A) = \{S / S \subseteq A\}$ $A = \{x, y\}$ $\mathcal{P}(A) = \{\emptyset, \{x, y\}, \{x\}, \{y\}\}$

Igualdad de conjuntos

Dos conjuntos son iguales cuando tienen los mismos elementos:

$$\{1, 2\} = \{2, 1\} \quad \{1, 2\} \cup \{1, 2, 5\} = \{1, 2, 5\} \quad A \cap B = A \cap (B \cap B) = A$$

Operaciones con Conjuntos

Unión: Es un nuevo conjunto formado por añadir elementos que están en A a todos los elementos que están en B.

$$A = \{x, y\} \quad B = \{z\} \quad C = \{x, y, z\} \quad A \cup B = A \cup C = \{x, y, z\}$$

$$A \cup B = \{x \in E / x \in A \vee x \in B\} \subseteq E$$

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

Propiedades de la Unión:

$$1^\circ. A \cup A = A \text{ (Ley de Idempotencia)}$$

$$2^\circ. A \cup B = B \cup A \text{ (Conmutativa)}$$

$$3^\circ. (A \cup B) \cup C = A \cup (B \cup C) \text{ (Asociativa)}$$

$$4^\circ. A \cup \emptyset = A \text{ (}\emptyset \text{ es el elemento neutro)}$$

$$5^\circ. A \cup E = E \text{ (E es el elemento absorbente)}$$

Intersección: Es un nuevo conjunto formado por todos los elementos que están en A y al mismo tiempo están en B.

$$A \cap B = \{x \in E / x \in A \wedge x \in B\} \subseteq E$$

$$A \cap B = \emptyset$$

Conjuntos disyuntos (no tienen ningún elemento en común)

Propiedades de la Intersección:

$$1^\circ. A \cap A = A \text{ (Idempotencia)}$$

$$2^\circ. A \cap B = B \cap A \text{ (Conmutativa)}$$

$$3^\circ. (A \cap B) \cap C = A \cap (B \cap C) \text{ (Asociativa)}$$

$$4^\circ. A \cap E = A \text{ (E es el elemento neutro)}$$

$$5^\circ. A \cap \emptyset = \emptyset \text{ (}\emptyset \text{ es el elemento absorbente)}$$

Complementario: Es un nuevo conjunto formado por todos los elementos que no están en A. $A^c = \{x \in E / x \notin A\} \subseteq E$

Propiedades del Complementario:

$$1^\circ. A \cap A^c = \emptyset$$

$$2^\circ. A \cap A = E$$

$$3^\circ. A = A$$

$$4^\circ. \cap = E$$

$$5^\circ. E = \cap$$

$$6^\circ. A \cap B \neq B \cap A \text{ E}$$

Diferencia: Es un nuevo conjunto formado únicamente por los elementos que están en A y no están en B. $A - B = \{x \in E / x \in A \text{ y } x \notin B\}$

E

Propiedades:

$$1^\circ. A - B = A \cap B^c$$

$$2^\circ. A - B = (A \cap B)^c \cap A$$

$$3^\circ. A - B = A \cap A^c \cap B^c = \emptyset$$

$$4^\circ. A - B = B - A = \emptyset \text{ si } A = B$$

Diferencia Simétrica: Está formada por todos aquellos elementos que están en A o están en B, pero no en los dos al mismo tiempo.

$$A \oplus B = (A - B) \cup (B - A)$$

Propiedades:

$$1^\circ. A \oplus B = (A \cup B) - (A \cap B)$$

$$2^\circ. A \oplus B = B \oplus A$$

$$3^\circ. A \oplus (B \cap C) = (A \oplus B) \cap C$$

Cardinales

El cardinal de A está asociado al número de elementos de A.

$$|A| = \text{card}(A) \quad A = \{1, 2, 3\} \mid |A| = 3 \quad B = \{4, 5\} \mid |B| = 2$$

Primer Axioma: $\cap \in E : |A| \geq 0$

Segundo Axioma: $|A \cup B| = |A| + |B| \text{ si } A \cap B = \emptyset$

$A \oplus B = (A - B) \cup (B - A)$ Sólo cuando son

$$|A| = |(A - B) \cup (A \cap B)| = |A - B| + |A \cap B| \text{ distintos}$$

$$|A - B| = |A| - |A \cap B|$$

$$|A \cap B| \text{ genérico}$$

$$|A \cap B| = |(A - B) \cup (A \cap B) \cup (B - A)| = |A - B| + |A \cap B| + |B - A|$$

$$|A \cap B| = |A - B| + |A \cap B| + |B - A| = [|A| - |A \cap B|] + |A \cap B| + [|B| - |A \cap B|]$$

$$|A \cap B| = |A| + |B| - |A \cup B| \text{ UNIÓN}$$

Diferencia Simétrica

$$|A \Delta B| = |A - B| + |B - A| = |A| - |A \cap B| + |B| - |A \cap B| = |A| + |B| - 2|A \cap B|$$

Ejercicios:

$$\bullet [(A \cap B) \cap ((A \cap B) \cap (A \cap B))] \cap ((A \cap B) \cap (A \cap B)) =$$

$$[A \cap (B \cap B)] \cap (A \cap A) \cap B$$

$$\bullet E$$

$$[(A \cap B) \cap A] \cap B = [(A \cap A) \cap (B \cap A)] \cap B = B$$

"

$$\bullet [[A \cap (B \cap C)] \cap (A \cap C)] \cap [B \cap (A \cap C)] =$$

$$[[A \cap (A \cap C)] \cap [(B \cap C) \cap (A \cap C)] \cap [B \cap (A \cap C)]] =$$

$$[[A \cap A] \cap [(B \cap C) \cap (A \cap C)] \cap [B \cap (A \cap C)]] =$$

E

$$= [(A \cap C) \cap (A \cap C)] \cap B \cap [(B \cap C) \cap (A \cap C)] = "$$

Producto Cartesiano

Par Ordenado: Conjunto de dos elementos en los que sí se tiene en cuenta el orden en que aparecen los elementos. (x, y) .

(x, y) no tiene porqué ser $= (y, x)$. si $(x, y) = (u, v) \Rightarrow x = u \wedge y = v$.

Terna Ordenada: Conjunto de tres elementos en los que sí se tiene en cuenta el orden en que aparecen los elementos. (x, y, z) .

n-Tupla Ordenada: Conjunto de n elementos en los que sí se tiene en cuenta el orden en que aparecen los elementos.

$$A \times B \cap E : A \times B = \{(x, y) / x \in A \wedge y \in B\}$$

$$A \times B \times C \cap E : A \times B \times C = \{(x, y, z) / x \in A \wedge y \in B \wedge z \in C\}$$

Propiedades

$$\bullet A \times B = \{(x, y) : x \in A, y \in B\}$$

$$|A \times B| = |A| \times |B|$$

- $\bullet A \times B = B \times A$
- $\bullet A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $\bullet A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $\bullet (A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
- $\bullet (A \times B) \cup (C \times D) \supseteq (A \cup C) \times (B \cup D)$
- $\bullet (A - B) \times C = (A \times C) - (B \times C)$
- $\bullet A \times B = (A \times B) \cup (A \times B)$

Grafos

A cualquier subconjunto de un producto cartesiano de dos conjuntos se le llama *grafo*. $G \subseteq A \times B$

$$\text{Pr1}(G) \subseteq A; \text{Pr2}(G) \subseteq B$$

Grafo Recíproco o Inverso

$$G = \{(y, x) : (x, y) \in G\}$$

$$G = \{(y, 2), (y, 1), (x, 3)\} \quad G = \{(2, y), (1, y), (3, x)\}$$

Composición entre los grafos

$$G \circ F = \{(x, z) : \exists y : (x, y) \in F; (y, z) \in G\}$$

$$F \subseteq A \times B; G \subseteq B \times C \quad G \circ F \subseteq A \times C$$

$$R = \{(a, 1), (b, 1), (c, 2), (d, 3), (e, 2), (f, 4)\}$$

$$S = \{(a, 4), (b, 3), (c, 2), (d, 1), (e, 5), (f, 6)\}$$

$$S = \{(4, a), (3, b), (2, c), (d, 1), (e, 5), (f, 6)\}$$

$$R \circ S = \{(4, 1), (3, 1), (2, 2), (1, 3), (5, 2), (6, 4)\}$$

$$S \circ R = \{(a, d), (b, d), (c, c), (d, b), (e, c), (f, a)\}$$

$$G \circ F \subseteq F \circ G$$

$$(R \circ S) \subseteq S \circ R$$

$$(G \circ F) = F \circ G$$

$$\{(z, x) : (x, z) \in G \circ F\} = \{(y, x) : \exists z : (y, z) \in F; (z, x) \in G\}$$

$$\} \neq (z, x) \in G$$

Establecer una correspondencia entre un conjunto A y B, consiste en asociar elementos de A a elementos de B.

$$\bullet \text{ } f = (F, A, B)$$

$$\exists y \in B \text{ } \exists x \in A$$

$$(x, y) \in F \text{ } y = f(x)$$

Conjunto Original de F: Elementos del conjunto original que tienen imagen. (or f).

Conjunto Imagen: Elementos del lado final que son imagen de algunos del inicial. $\text{Im}(f)$ o $f(A)$.

$$\text{or } f = \{x \in A / \exists y \in B : y = f(x)\}$$

$$f(A) = \{y \in B / \exists x \in A : y = f(x)\}$$

Correspondencia Recíproca

$f = (F ; B \times A)$ Está asociado al grafo inverso.

$$y = f(x) \neq x = f(y) \text{ } x \neq y \text{ } y \text{ imagen de } x \text{ } x \neq y \text{ } x \text{ antiimagen de } y$$

Composición

$$g \circ f = (G \circ F; A, C) \text{ } g \circ f(x) = g(f(x))$$

Propiedades:

$$1. \text{ } x_1 \neq x_2 \neq f(x_1) \neq f(x_2) \text{ } y \neq f(A) \neq y = f(x) \text{ } x \neq A.$$

$$2. \text{ } f(x_1 \neq x_2) = f(x_1) \neq f(x_2)$$

$$3. \text{ } f(x_1 \neq x_2) \neq f(x_1) \neq f(x_2)$$

$f : A \neq B$ es aplicación; $g : B \neq C$ es aplicación $\neq g \circ f : A \neq C$ también es Aplicación.

Fotocopia

$$15. \text{ } G = \{(b, b), (b, c), (a, d), (d, b)\} \text{ } H = \{(a, a), (c, a), (d, a)\}$$

$$G = \{(b, b), (c, b), (d, a), (b, d)\} \text{ } H = \{(a, a), (a, c), (a, d)\}$$

$$(G \circ H) = H \circ G = \{(d, a), (d, c), (d, d)\}$$

$$(H \neq G) = \{(b, b), (b, c), (a, d), (d, b), (a, a), (c, a), (d, a)\}$$

$$\text{ran}(H) \neq \text{ran}(F) = \{y / \exists x : (x, y) \in F\} \text{ (conjunto de las segundas proyecciones)}$$

$\text{dom}(F) \neq$ conjunto de las primeras proyecciones.

$$\text{dom}(F) = \{x \mid \exists y : (x, y) \in F\}$$

$$16. N \rightarrow N \quad F = \{(x, y) \mid 4x + y = 24\}$$

$$F = \{(0, 24), (1, 20), (2, 16), (3, 12), (4, 8), (5, 4), (6, 0)\}$$

$$\text{dom}(F) = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\text{ran}(F) = \{24, 20, 16, 12, 8, 4, 0\}$$

$$F \circ F = \{(24, 0), (20, 1), (16, 2), (12, 3), (8, 4), (4, 5), (0, 6)\}$$

$$F \circ F = \{(5, 8), (6, 24)\}$$

Relación Binaria

Correspondencia entre un grafo y sí mismo. $F : A \rightarrow A$

$f = (R; A, A); f(x) = y; (x, y) \in R; x \in R$ y la imagen de x es y .

x está Relacionado con y

" $x, y \in Z : x \in R \vee x \in R^4 \wedge y \notin R^3 \wedge y \notin R^4$ "

" $A, B \in E : A \in R \wedge B \in A \wedge B$ "

Propiedades que pueden cumplir o no, las Relaciones Binarias:

1. Reflexiva: " $x \in A : x \in R x$ "

2. Simétrica: " $x, y \in A : x \in R y \vee y \in R x$ "

3. Antisimétrica: " $x, y \in A : x \in R y \wedge y \in R x \rightarrow x = y$ "

4. Transitiva: " $x, y, z \in A : x \in R y \wedge y \in R z \rightarrow x \in R z$ "

5. Conexa: " $x, y \in A : x \in R y \vee y \in R x$ "

Relaciones de Equivalencia

Es una relación reflexiva, simétrica y transitiva.

Una correspondencia de elementos con sí mismos, en la que todo x está relacionado con x , todo x está relacionado con y , e y con x , y con x , y con z , luego x con z . Se utiliza el signo " $\sim$ ".

Sea A , " $\sim$ " relación de equivalencia definida en A :

" $a \in A : [a] = \{x \in A \mid x \sim a\}$ " $a \in A : a \in [a]$ pues $a \sim a$.

clase de equivalencia del elemento a .

En la clase de un elemento están todos los elementos del conjunto relacionados con ese elemento.

Si un elemento no está en la clase de otro, ninguno de los elementos de la última clase puede estar en la clase del primer elemento. Si un elemento está en la clase de otro, todos los elementos de dicha clase estarán en la clase del primer elemento. **$a \sim b \iff [a] = [b]$**

• Conjunto Cociente

Contiene las distintas clases de equivalencias.

$A/\sim = \{[a], a \in A\}$! nos da los distintos tipos de elementos que hay en un conjunto.

$$x + y = 2k \iff x \sim y \iff x - y = 2k; x = 2k - y;$$

$$[a] = \{x = 2k - a\}, k \in \mathbb{Z} \quad [0] = \{x = 2k - 0\} = \{0, 2, 4, 6, 8\} \text{ Pares}$$

$$[1] = \{x = 2k - 1\} = \{-1, 1, 3, 5, 7, 9\} \text{ Impares}$$

$$\mathbb{Z} / \sim = \{[0], [1]\}$$

Sea $A, \{C_1, C_2, C_3, \dots, C_j\}, C_i \in A$

son partición de A si: 1. $\bigcup C_i = A$

2. C_i no tienen elementos en común.

$$9. \mathbb{R} - \{0\}; \sim: a, b \in \mathbb{R} : a \sim b \iff a + (1/a) = b + (1/b)$$

$$1. \text{ Reflexiva: } x \in \mathbb{R} : x + (1/x) = x + (1/x) \iff x \sim x$$

$$2. \text{ Simétrica: } x, y \in \mathbb{R} : x + (1/x) = y + (1/y) \iff y + (1/y) = x + (1/x) \iff y \sim x$$

$$3. \text{ Transitiva: } x, y, z \in \mathbb{R} : x + (1/x) = y + (1/y); y + (1/y) = z + (1/z) \iff$$

$$x + (1/x) = z + (1/z) \iff x \sim z$$

$$[a] \in \mathbb{R} : [a] = \{x \in \mathbb{R} - \{0\} / x \sim a\} = \{x + (1/x) = a + (1/a)\} \quad [a] = \{a, (1/a)\}$$

$$11. \text{ Reflexiva: } x \in \mathbb{R} : x^2 + x^2 = x^2 + x^2 \iff x \sim x$$

$$\text{Simétrica: } x, y \in \mathbb{R} : x^2 + y^2 = y^2 + x^2 \iff x \sim y$$

$$\text{Transitiva: } x, y, z \in \mathbb{R} : x^2 + y^2 = y^2 + z^2 \iff x \sim z$$

$$[a] \in \mathbb{R} : [a] = \{x \in \mathbb{R} : x^2 + x^2 = a^2 + a^2\}$$

$$\text{Sea } N; E(n) : a, b \in N : a \sim b \iff E(a) = E(b)$$

$$\text{Reflexiva: } x \in N : x \sim x \iff E(x) = E(x)$$

$$\text{Simétrica: } x, y \in N : x \sim y \iff E(x) = E(y) \iff E(y) = E(x)$$

$$\text{Transitiva: } x, y, z \in N : x \sim y \iff E(x) = E(y); E(y) = E(z) \iff E(x) = E(z)$$

$$\{a \mid \exists x (x \in A \wedge f(x) = a)\} = \{E(x) = a\}$$

$$[a^2] = \{x \mid [a^2, (a+1)^2]\} [a] = \{[E(a)]^2 - ((E(a)+1)^2 - 1)\}$$

$$N/\sim = \{[a^2]\}$$

Relación de Orden

Relación con las propiedades reflexiva, antisimétrica y transitiva.

$a < b$! a anterior a b o b posterior a a

$\mathbb{Z}; a \mid b$! $a \mid b \mid \mathbb{N} \mid a \mid b$! $a \mid b$ (a divide a b) } Divisibilidad

La relación de orden por excelencia es el " $<$ ".

Preorden: Relación que es reflexiva y transitiva.

Aplicaciones

Sea $f = (F; A, B)$ correspondencia. f es una aplicación si:

1. Todo elemento de A tiene imagen ! or $f = A$

2. La imagen es única. ! $f(x) = y_1 \mid f(x) = y_2 \mid y_1 = y_2$

$f : \mathbb{N} \rightarrow \mathbb{N}; f(x) = x \mid f(4) = \pm 2$ } No es aplicación.

$f : \mathbb{Z} \rightarrow \mathbb{Z}; f(x) = x^2$ } Sí es aplicación.

Clasificación de Correspondencia

Inyectiva: Dos elementos **no** pueden tener la misma imagen.

$\mathbb{N} \rightarrow \mathbb{R}; f(x) = x$ } Inyectiva $f : \mathbb{Z} \rightarrow \mathbb{Z}; f(x) = x^2$ } No Inyectiva

(porque $(-1)^2 = 1$ y $1^2 = 1$, dos elementos

distintos con misma imagen)

Sobreyectiva: Todo elemento del conjunto final es imagen de al menos uno del conjunto inicial.

$\mathbb{N} \rightarrow \mathbb{Z}; y = f(x); x \in \mathbb{Z} \mid y = x^2; x = \pm \sqrt{y}$ } No Sobreyectiva

Biyectiva: Cuando es inyectiva y sobreyectiva al mismo tiempo.

$f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x/2$ Aplicación; Inyectiva, Sobreyectiva } Biyectiva.

Inyectiva : $(x_1/2) = (x_2/2) \mid x_1 = x_2$

$\mathbb{N} \rightarrow \mathbb{A} \mid f(x) = y \mid \mathbb{B} \mid g(f(x)) = z \mid \mathbb{C}$

$$g \circ f(x) = z_1 ; g \circ f(x) = z_2 \quad ! \quad g(f(x)) = z_1 ; g(f(x)) = z_2 \quad ! \quad z_1 = z_2$$

Si f y g son inyectivas, $g \circ f$ también es inyectiva.

Si f y g son sobreyectivas, $g \circ f$ también es sobreyectiva.

$$18. f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$a. f(x, y) = (x, x^2 y - y)$$

$$1. \text{ Inyectiva: } f(x_1, y_1) = f(x_2, y_2) \quad ! \quad (x_1, x_1^2 y_1 - y_1) = (x_2, x_2^2 y_2 - y_2) \quad ! \quad x_1 = x_2$$

$$x_1^2 y_1 - y_1 = x_2^2 y_2 - y_2 \quad \} \quad y_1(x_1^2 - 1) = y_2(x_2^2 - 1) ; y_1 = y_2 \quad ! \quad (x_1^2 - 1) / (x_2^2 - 1) \quad !$$

$! \quad \text{si } x_1^2 - 1 \neq 0 \quad ! \quad y_1 = y_2. \text{ Es inyectiva en } f : \mathbb{R} \times \mathbb{R} - \{1, -1\}.$

$$2. \text{ Sobreyectiva: } (z, t) \in \mathbb{R} \times \mathbb{R} : (z, t) = f(x, y) \quad \} \quad ! \quad (z, t) = (x, x^2 y - y) \quad !$$

$$! \quad z = x ; t = x^2 y - y \quad ! \quad t = z^2 y - y \quad ! \quad t = y(z^2 - 1) \quad ! \quad y = t / (z^2 - 1)$$

Es sobreyectiva en $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R} - \{(1, 0), (-1, 0)\}$

Si $g \circ f$ es inyectiva $! \quad f$ es inyectiva

$$f(x_1) = f(x_2) \quad ! \quad g(f(x_1)) = g(f(x_2)) \quad ! \quad g \circ f(x_1) = g \circ f(x_2) \quad ! \quad x_1 = x_2 \quad ! \quad f \text{ es inyectiva.}$$

Si $g \circ f$ es sobreyectiva $! \quad g$ es sobreyectiva

$$(z, t) \in \mathbb{R} \times \mathbb{R} : z = g \circ f(x) \quad ! \quad z = g(f(x)) \quad ! \quad g \text{ es sobreyectiva.}$$

Si $g \circ f$ es biyectiva $! \quad f$ es inyectiva y g es sobreyectiva

Relación de Equivalencia Inducida por una Aplicación

La relación de equivalencia inducida por una aplicación dice que 2 elementos están relacionados cuando sus imágenes son iguales.

$$(x_1, x_2) \in A : x_1 R x_2 \quad ! \quad f(x_1) = f(x_2).$$

Estructuras

Ley de Composición Interna (LCI), $\cdot$, definida sobre un conjunto E , una aplicación de $E \times E \rightarrow E$

$$(a, b) \mapsto a \cdot b$$

Propiedades que se pueden cumplir:

$$\text{Conmutativa: } (a, b) \in E : a \cdot b = b \cdot a$$

$$\text{Asociativa: } (a, b, c) \in E : (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

$$\text{Elemento Regular: } a \in E \text{ es regular : a la izquierda : } (b, c) \in E : a \cdot b = a \cdot c \quad ! \quad b = c$$

: a la derecha : " b, c " E : b " a = c " a ! b = c

Elemento Neutro: e " E, " x " E : e " x = x " e = x

Elemento Simétrico: a' es simétrico de a ! a " a' = a' " a = e

Distributiva: (E, ", °) (a " b) ° c = (a ° c) " (b ° c)

La estructura más pequeña que existe es un conjunto y una L.C.I. (E, ") " Grupoide o Magma.

Grupoide: Es una estructura formada por un conjunto y su l.c.i. Si un grupoide cumple además la propiedad asociativa, se le llama **semigrupo**. Si además de esto, cumple la conmutativa, se le llama **semigrupo conmutativo o abeliano**.

Si el semigrupo tiene elemento neutro se le llama **semigrupo unitario o monoide**.

Grupo: Es una estructura formada por un conjunto y una l.c.i., que cumple la propiedad del **elemento neutro**, la **asociativa**, y todo elemento tiene **elemento simétrico**. Si además el grupo cumple la conmutativa, se le llama **grupo abeliano o conmutativo**.

Subgrupo: Si dado un grupo G, tenemos un subconjunto de G, que también cumple las propiedades de grupo, se le llama subgrupo. $H \subset G$.

El grupo y subgrupo más pequeños que hay es el formado por el elemento neutro.

Grupo Finito: Grupo formado por un número finito de elementos.

$(a \cdot b)' = b' \cdot a'$ (a')' = a sólo si G es conmutativo: $(a \cdot b)' = a' \cdot b'$

Homomorfismo: Cuando la imagen de la operación del lado inicial, coincide con la operación de las imágenes del lado final. $f(a \cdot b) = f(a) \cdot f(b)$

Clasificación de Homomorfismo:

Si el homomorfismo es inyectivo Monomorfismo

Si es sobreyectivo Edimorfismo

Si es biyectivo Isomorfismo

Dos estructuras son isomorfas si existe un isomorfismo entre las dos (los elementos de un lado se comportan igual que los del otro lado).

Teorema de Caracterización de Subgrupos:

Sea $(G, *)$ grupo, " " $H \subset G$, $H \neq \emptyset$! " a, b " H : $a * b \in H$

" a, b " H : $a * b \in H$ H H G

" a " H : $a' \in H$

$(\mathbb{Z}, +)$ grupo $2 \subset \mathbb{Z} = \{2 \cdot h, h \in \mathbb{Z}\}$ Demostrar: $2 \subset \mathbb{Z}$

$$0 = 2 \cdot 0 - 0 = 2 \cdot 0 - 0 = 0 \in \mathbb{Z}$$

$$x, y \in \mathbb{Z} : x + y' = x + (-y) = x - y \in \mathbb{Z}$$

$$x + y' = 2h_1 + (2h_2)' = 2h_1 + (-2h_2) = 2(h_1 - h_2) \in \mathbb{Z}$$

Congruencias Módulo un Subgrupo

Sea $(G, *)$ grupo, y sea $H \subseteq G$

$a, b \in G : a \sim_i b \iff a' * b \in H$ congruencia a la izq mod. H

$$a \sim_i b \iff b * a' \in H$$

$\sim_i$

$$1. a' * a = e \in H \implies a \sim_i a$$

$$2. a \sim_i b \iff a' * b \in H \iff (a' * b)' \in H \iff b' * a \in H \iff b \sim_i a$$

$$3. a \sim_i b \iff (a' * b) * (b' * c) \in H \iff a' * c \in H \iff a \sim_i c$$

$$b \sim_i c$$

$$[a]_i = a * H \quad [a]_i d = H * a$$

$$[e]_i = e * H = H \quad [h]_i = h * H = H \quad (h \in G; h \in H)$$

Sea $H \subseteq G$! si $[a]_i = [a]_i d \iff a \in G$! H es un Subgrupo de G y se llama

Subgrupo Normal $H \subseteq G$

Teniendo en cuenta el Teorema de Caracterización de Subgrupos:

$$H \subseteq G \iff a \in G : a * H * a' \in H$$

Homomorfismo entre grupos

$$f : (G, *) \rightarrow (G', \circ) \text{ aplicación } a, b \in E : f(a * b) = f(a) \circ f(b)$$

$$1). f(e) = e' \implies f(e) = f(e) \circ e'$$

$$f(e) = f(e * e) = f(e) \circ f(e)$$

$$f \in \text{Hom}$$

$$2). f(a') = (f(a))' \implies f(a') \circ f(a) = f(a) \circ f(a')$$

$$f(a' * a) = f(a * a')$$

$$f(e) = e'$$

Núcleo de un Homomorfismo de Grupos

$$\text{Ker } f = \{x \in G \mid f(x) = e'\}$$

Aquellos x del grupo inicial cuya imagen sea el elemento neutro del grupo final. En $\text{Ker } f$ sólo ha de estar e para que sea inyectiva, si hay dos elementos en el núcleo ya no es inyectiva.

$$7). f : (\mathbb{R}^*, \cdot) \rightarrow (\mathbb{R}^*, \cdot) \quad f(x) = x^2 \text{ demostrar } f \text{ Hom entre grupos}$$

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

$$f(x \cdot y) = (x \cdot y)^2 = (x \cdot y) \cdot (x \cdot y) = x \cdot x \cdot y \cdot y = x^2 \cdot y^2 = f(x) \cdot f(y)$$

$$\text{Ker } f = \{x \in \mathbb{R}^* \mid f(x) = 1\} \quad x^2 = 1 \quad ; \quad x = \pm 1; \quad \text{Ker } f = \{-1, 1\}$$

$$\text{Ker } f \subseteq G$$

$$H \subseteq G; \quad H \subseteq \text{Ker } f \quad a, b \in H : x \cdot y' \in H$$

$$H \subseteq \text{Ker } f \subseteq G \quad \text{Ker } f \subseteq G \quad ! \quad x, y \in \text{Ker } f : x \cdot y' \in \text{Ker } f$$

$$1. \text{Ker } f \subseteq \text{Ker } f \quad ! \quad f(e) = e' \quad ! \quad e \in \text{Ker } f$$

$$2. \quad x, y \in \text{Ker } f : x \cdot y' \in \text{Ker } f \quad ! \quad f(x \cdot y') = f(x) \cdot f(y') = e' \cdot (f(y))' = e' \cdot e' = e'$$

$$\text{Ker } f \subseteq G \quad f(x) = x^2 \quad \text{Ker } f = \{-1, 1\} \quad [a]_i = a \in \text{Ker } f = \{-a, a\} \quad \text{Ker } f \subseteq G$$

$$[a]_d = \text{Ker } f \quad a = \{-a, a\}$$

$$\text{Im } f \subseteq G' \quad y \in G' : y = f(x)$$

$$1. f(e) = e' \in f(G)$$

$$2. \quad f(a), f(b) \in f(G) : f(a) \cdot f(b)' \in f(G) : f(a) \cdot f(b)' = f(a \cdot b') \in G$$

$$7). \text{Im } f = \mathbb{R}^*, +$$

$$y \in \mathbb{R}^* : y = f(x) \quad y = x^2 \quad x = \pm \sqrt{y} \quad y \neq 0$$

$$(G, *) \quad \langle a \rangle \text{ potencias de } a \in G$$

$$n > 0 : a = a \cdot a \cdot a \dots a \text{ (n veces)}$$

$$a = n = 0 : a^0 = e$$

$$n < 0 : a = a' \cdot a' \cdot a' \dots a' \text{ (n veces)}$$

$$(\mathbb{R}^*, \cdot) \quad 5 = 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 1$$

$$(\mathbb{Z}, +) \quad 5 = 5 + 5 + 5 + 5 + 5 \cdot 5 = 0$$

Subgrupo engendrado por un elemento

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq \langle a \rangle \leq G$$

subgrupos engendrados o generados por a .

$$\langle a \rangle \leq G, \langle a \rangle \leq G \implies x, y \in \langle a \rangle : x * y' \in \langle a \rangle$$

$$1. \langle a \rangle \leq \langle a \rangle \implies e = a^0 \in \langle a \rangle$$

$$2. a \in \langle a \rangle \implies a * (a')' \in \langle a \rangle$$

$$a * (a')' = a * a * a \dots * a * (a * a * a \dots * a)' = a \in \langle a \rangle$$

Orden de Grupo. Número de elementos que tiene un grupo.

Si el grupo es de orden contable, se llama *grupo finito*.

Un Grupo es Cíclico si mediante potencias de un elemento puedo generar todos los elementos del grupo. Se dice que el grupo es engendrado por dicho elemento. Si un elemento genera un grupo, su simétrico también.

La primera potencia no nula, tal que a^n elevado a ella me da el neutro, se llama *orden de elemento*.

$$\text{orden}(e) \text{ siempre } 1 \implies O(e) = 1$$

$$O(a) = k \implies a^k = e \text{ (k entero no nulo más pequeño tal que } a^k = e)$$

$$O(a) = k \implies \langle a \rangle = \{a^0, a, a^2, a^3, \dots, a^{k-1}\} \implies |\langle a \rangle| = k$$

Teorema de Lagrange para grupos finitos

El orden de un subgrupo divide siempre al orden del grupo.

$$\text{si } O(a) = |G| \implies G \text{ es cíclico}$$

$$a \in G; O(a) \text{ ha de dividir al } |G|$$

$$|G| = 1 \implies G = \{e\} \implies \text{cíclico ya que su orden es primo}$$

Orden	Sim	*	e
1	e	e	e

$$|G| = 2 \implies G = \{e, a\} \implies \text{cíclico engendrado por } a$$

Sim	orden	*	e	a
e	1	e	e	a
a	2	a	a	e

$$|G| = 3 \implies G = \{e, a, a^2\} \implies \text{cíclico generado por } a \text{ y } a^2 \implies \langle a \rangle = \langle a^2 \rangle$$

Orden	*	e	a	a^2
1	e	e	a	a^2
3	a	a	a^2	e

3	a^2	a^2	e	a
---	-------	-------	---	---

Orden	*	e	a	a^2	a^3	Sim
1	e	e	a	a^2	a^3	e
4	a	a	a^2	a^3	e	a^3
2	a^2	a^2	a^3	e	a	a^2
4	a^3	a^3	e	a	a^2	a

$|G| = 4$ $G = \langle a \rangle = \langle a^3 \rangle$! cíclico $(a^2)^2 = a = e$; luego orden de a^2

$O(a') = k$! $(a') = a' * a' * a' \dots * a' (k \text{ veces}) = (a * a * a \dots * a)' = (a)' = e' = e$

$|G| = 4$! no cíclico $G\{e, a, b, c\}$ **Grupo Klein K4**

Sim	orden	*	e	a	b	c
e	1	e	e	a	b	c
a	2	a	a	e	c	b
b	2	b	b	c	e	a
c	2	c	c	b	a	e

Subgrupo Impropio. Subgrupo formado por e o por todo el grupo.

Inducción Matemática e Inducción Completa

Se basa en: siempre $n \in \mathbb{N}$

1). Se demuestra la fórmula en cuestión para un primer elemento.

2). Se establece la Hipótesis de Inducción, que es, suponer que la afirmación es cierta hasta $n = k$. $1 + 3 + 5 \dots + (2k - 1) = k^2$

3). Demostrar la afirmación para el siguiente elemento, $n = k+1$.

$$1 + 3 + 5 \dots + (2(k+1) - 1) = (k+1)^2$$

$$1 + 3 + 5 \dots (2k-1) + (2(k+1)-1) =$$

$$k^2 + (2(k+1)-1) =$$

$$k^2 + 2k + 2 - 1 = k^2 + 2k - 1 = (k + 1)^2$$

$$\%(A \rightarrow \neg A)$$

A B

A B

A

B

A

A B

A B