Lógica

Profesor: Angel Perez

Diego Rodríguez

Estudiante de Matemáticas e Ingeniería Informática
Universidad Rey Juan Carlos
Curso 2023-2024
Página web
GitHub

d.rodriguezto.2023@alumnos.urjc.es

Índice

Terminología matemática

- Enunciados:
    - Teorema
    - Proposicion - resultado de un enunciado que propone algo (menor entidad que un teorema)
    - Lema - resultado cuya funcion es servir como herramienta auxiliar para probar otra cosa
    - Corolario - resultados que se obtienen como consecuencia de demostrar un teorema
    - Observacion - puntualizacion verdadera y suficientemente clara como para no necesitar demostracion
    - Conjeturas - resultado que se cree que es cierto pero no hay una demostración

Ejemplos:

Teorema 0.1 — Ultimo teorema de Fermat. Sea $n \geq 3$ un numero natural. La ecuacion

$$x^n + y^n = z^n$$

no tiene soluciones (salvo las triviales) en los numeros enteros.

- Fermat lo enuncia en 1637.
- Es una conjetura hasta que Andrew Wiles lo demuestra en 1995.

Conjetura 0.1 — de Goldbach. Sea $n > 2$ un numero natural par. Entonces n es suma de dos numeros primos.

Demostracion directa

Ejemplos:

Proposición 0.1. Sea n un numero natural impar. Entonces la division entera de n^2 entre 8 tiene resto 1.

Proof.

Como n es impar, se puede expresar como $n = 2m + 1$ con $m \in \mathbb{N}$. Asimismo, tenemos que

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 \Rightarrow n^2 = 4m(m+1) + 1$$

Luego $m(m+1)$ es un numero par $\Rightarrow m(m+1) = 2\ell$ con $\ell \in \mathbb{N}$.

$$n^2 = 4 \cdot 2\ell + 1 = 8\ell + 1 \Rightarrow \text{ El resto de } n^2 \text{ entre 8 es 1.}$$

■

Teorema 0.2 — de Pitagoras. Sean a la longitud de la hipotenusa de un triangulo rectangulo y b y c las longitudes de sus dos catetos. Entonces se cumple la igualdad

$$a^2 = b^2 + c^2$$

Proof.

Se puede demostrar de forma geométrica:

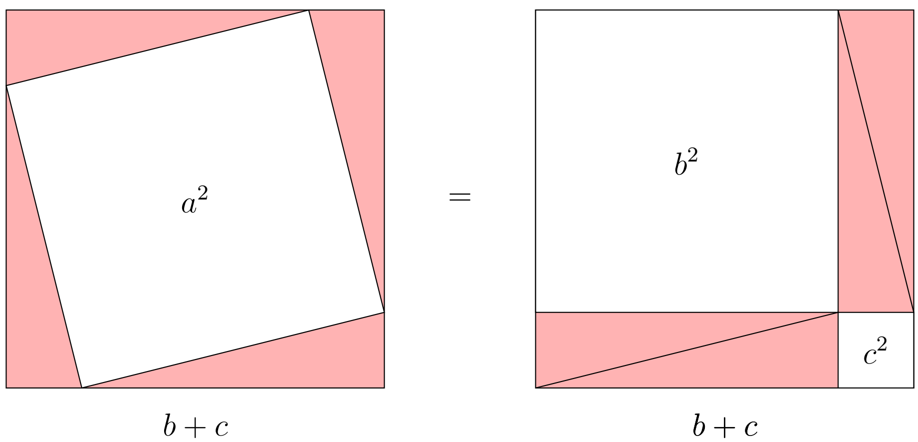


Figura 1. Demostracion del teorema de Pitagoras

■

Reduccion al absurdo

Ejemplos:

Teorema 0.3. $\sqrt{2}$ es un numero irracional.

Proof.

Lo demostraremos por reduccion al absurdo.
Supongamos que $\sqrt{2}$ es un numero racional. Entonces $\sqrt{2}$ se puede escribir como una

fraccion irreducible: $\sqrt{2} = \dfrac{a}{b}$ donde $a, b \in \mathbb{Z}$ y $b \neq 0$. Entonces

$$b\sqrt{2} = a \Rightarrow b^2 2 = a^2 \Rightarrow a^2 \text{ es par} \Rightarrow a \text{ es par} \Rightarrow a = 2c$$

Sustituyendo

$$b^2 2 = (2c)^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow b^2 \text{ es par } \Rightarrow \boxed{\text{b es par}}$$

Hay una contradiccion porque a y b no tenian factores en comun.
Luego lo supuesto tiene que ser falso y por tanto $\sqrt{2}$ <u>no es racional</u>. ■

1 Conjuntos, relaciones y funciones

§1.1 Conjuntos

Definición 1.1. Un conjunto es una coleccion de objetos, que se denominan elementos de ese conjunto.
Si A es un conjunto y b es un elemento de A decimos que b pertenece a A. Notacion: $b \in A$.
En caso contrario, decimos que b no pertenece a A. Notacion: $b \notin A$.

Una forma de expresar conjuntos es enumerar sus elementos:

Ejemplo 1.1. $A = \{1, 3, 5, 7\}$

Definición 1.2 — Subconjunto. Sean A y B dos conjuntos. Se dice que A es un subconjunto de B si todo elemento de A es tambien elemento de B.
Tambien se dice que A esta contenido en B. Notacion: $A \subseteq B$.
En caso contrario diremos que A no esta contenido en B.
Notacion: $A \nsubseteq B$.

Definición 1.3. Sean A y B dos conjuntos. Decimos que A y B son iguales si tienen los mismos elementos. Esto es lo mismo que decir que $A \subseteq B$ y $B \subseteq A$.
Notacion: $A = B$.
En caso contrario, diremos que A y B son distintos.
Notacion: $A \neq B$.

Observación 1.1. En un conjunto no se tienen en cuenta elementos repetidos.
Tampoco se tiene en cuenta el orden.

Definición 1.4 — Contenido estricto. Decimos que A esta estrictamente contenido en B si $A \subseteq B$ y $A \neq B$. Notacion: $A \subset B$.

La segunda forma de expresar conjuntos consiste en indicar una propiedad.

Ejemplo 1.2.

$$A = \{x \mid x \text{ es un numero primo menor que } 15\}$$

$$A = \{2, 3, 5, 7, 11, 13\}$$

$$B = \{x \mid x \text{ es un numero primo mayor que } 15\}$$

$$B = \{17, 19, 23, 29, 31, 37, 41, 43, \ldots\}$$

Definición 1.5 — Conjuntos numericos, informal.

- Numeros naturales:
  $\mathbb{N} := \{1, 2, 3, 4, 5, \ldots\}$. No tiene solucion $2 - x = 5$.
- Numeros enteros:
  $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. No tiene solucion $2x = 5$.
- Numeros racionales:
  $\mathbb{Q} := \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$. Tienen expresion decimal periodica. No tiene solucion $x^2 = 2$.
- Numeros reales:
  $\mathbb{R}$. Tienen expresion decimal arbitraria, periodica o no periodica. No tiene solucion $x^2 = -1$.
- Numeros complejos:
  $i := \sqrt{-1}$ la unidad imaginaria.
  $\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$

Definición 1.6. Se define el conjunto vacio como un conjunto sin elementos.
Notacion: $\varnothing$

Proposición 1.1. Sea A un conjunto cualquiera. Se cumple que $\varnothing \subseteq A$.

Proof.

Lo demostraremos por reduccion al absurdo.
Supongamos que $\varnothing \not\subseteq A$. Entonces, existe un elemento x tal que $x \in \varnothing$ y $x \notin A$.
Esto es una contradiccion, ya que el conjunto $\varnothing$ no tiene elementos.
Luego es falso que $\varnothing \not\subseteq A$ y por tanto $\varnothing \subseteq A$. ■

Definición 1.7 — Operaciones con conjuntos. Sean A y B dos conjuntos. Se definen:

- Interseccion de A y B:
  $A \cap B \coloneqq \{x \mid x \in A \text{ y } x \in B\}$
- Union de A y B:
  $A \cup B \coloneqq \{x \mid x \in A \text{ o } x \in B\}$
- Diferencia entre A y B (o A menos B):
  $A \setminus B \coloneqq \{x \mid x \in A \text{ y } x \notin B\}$

Definición 1.8. Decimos que un conjunto A es finito si tiene tantos elementos como un numero natural o bien si no tiene elementos ($\varnothing$).
En caso contrario decimos que A es infinito.

Definición 1.9. Si A es un conjunto finito, se define el cardinal de A como su numero de elementos. El cardinal de $\varnothing$ es 0. Si A es un conjunto infinito tiene cardinal infinito.
Notacion: $|A|$

Definición 1.10 — Partes de un conjunto. Sea A un conjunto. Se define el conjunto de las partes de A como el conjunto formado por todos los subconjuntos de A. Simbolicamente:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Ejemplo 1.3. Sean $A = \{1,2\}$, $B = \{1,2,3\}$, $C = \{1,2,3,4\}$. Escribir los conjuntos $\mathcal{P}(A), \mathcal{P}(B), \mathcal{P}(C), \mathcal{P}(\mathcal{P}(A))$.

- Subconjuntos de A: $\{1\}, \{2\}, \{1,2\}, \varnothing$.
  Luego $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$
- Subconjuntos de B: $\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}, \varnothing$.
  Luego $\mathcal{P}(B) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Teorema 1.1. Sea A un conjunto finito. Entonces se cumple que

$$|\mathcal{P}(A)| = 2^{|A|}$$

Proof.

Considero el conjunto A formado por n elementos donde $n \in \mathbb{N}$.
Sin perdida de generalidad, supongo que $A = \{1, 2, 3, \ldots, n\}$. Para contar subconjuntos de A, planteo el cuestionario

1. ¿Está 1 en el subconjunto?
2. ¿Está 2 en el subconjunto?

n. ¿Está n en el subconjunto?

Hay el mismo numero de subconjuntos de A que de respuestas al cuestionario. Como el cuestionario tiene n preguntas y cada una 2 respuestas posibles, hay 2^n respuestas diferentes al cuestionario y, por tanto, 2^n subconjuntos de A.
Falta probarlo para $A = \varnothing$. Se cumple que $\varnothing \subseteq \varnothing$ y es el unico posible.
Luego $\mathcal{P}(\varnothing) = \{\varnothing\}$
Tenemos que $|A| = 0$ y $|\mathcal{P}(A)| = 1$. Ademas, $2^{|A|} = 2^0 = 1 = |\mathcal{P}(A)|$ ■

Proof.

Tambien lo demostraremos por induccion sobre n, el numero de elementos de A.
El caso $n = 0$ esta hecho en la demostracion anterior.
En el caso base, $n = 1$, $A = \{1\}$ y $\mathcal{P}(A) = \{\varnothing, \{1\}\}$. Luego $|A| = 1$ y $|\mathcal{P}(A)| = 2 = 2^1 = 2^{|A|}$. Se cumple para $n = 1$.
Hipotesis de induccion: Supongamos que el resultado es cierto para n ($A = \{1, 2, 3, \ldots, n\}$ y $|\mathcal{P}(A)| = 2^n$)
Tengo que demostrar, a partir de esto, la tesis de induccion:
Si $B = \{1, 2, 3, \ldots, n, n+1\}$ entonces $|\mathcal{P}(A)| = 2^{n+1}$.
Hay 2 tipos de subconjuntos de B.

Tipo 1 Los que no tienen a $n+1$ como elemento. Por hipotesis de induccion hay 2^n subconjuntos de B de este tipo (son los mismos que los de A).

Tipo 2 Los que si tienen a $n+1$ como elemento. Cada uno de estos se obtiene añadiendo el elemento $n+1$ a un subconjunto de Tipo 1. Por tanto, hay tantos como habia de Tipo 1: 2^n.

En total, B tiene:

$$\underbrace{2^n}_{\text{Tipo 1}} + \underbrace{2^n}_{\text{Tipo 2}} = 2 \cdot 2^n = 2^{n+1} = |\mathcal{P}(B)|$$

Asi, queda demostrada la tesis de induccion. ■

Definición 1.11 — Par ordenado. Dados dos conjuntos A y B y dos elementos $a \in A$ y

$b \in B$, se define el par ordenado formado por a y b como la expresion simbolica

$$(a, b)$$

donde a es el primer elemento del par y b es el segundo elemento del par.

Definición 1.12 — Producto cartesiano. Sean A y B dos conjuntos no vacios. Se define el producto cartesiano de A por B como el conjunto formado por todos los pares ordenados de la forma (a, b) donde $a \in A$ y $b \in B$. Simbolicamente:

$$A \times B \coloneqq \{(a, b) \mid a \in A, b \in B\}$$

Ejemplo 1.4. $A = \{1, 2, 3\}$, $B = \{2, 4\}$

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

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

El producto cartesiano no es conmutativo.

Proposición 1.2. Sean A y B dos conjuntos finitos y no vacios. Se cumple que

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

Proof.

Para formar todos los pares ordenados posibles, tenemos $|A|$ opciones en la primera coordenada y $|B|$ en la segunda.
Por tanto, hay en total $|A| \cdot |B|$ pares ordenados.
Así, $|A \times B| = |A| \cdot |B|$ ■

Observación 1.2. Si A o B es infinito $\Rightarrow |A \times B| = \infty$

Definición 1.13 — n-tupla ordenada. Sea $n \in \mathbb{N}$, $n \geq 2$. Sean $A_1, A_2, \ldots, A_n$ conjuntos y $a_1 \in A_1$, $a_2 \in A_2$, $\ldots$, $a_n \in A_n$ elementos de sus conjuntos. Se define la n-tupla ordenada formada por esos elementos como la expresion simbolica

$$(a_1, a_2, \ldots, a_n)$$

Definición 1.14. Sea $n \in \mathbb{N}$, $n \geq 2$. Sean $A_1, A_2, \ldots, A_n$ conjuntos no vacios. Se define el producto cartesiano de esos conjuntos como

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

Si hacemos el producto cartesiano de un conjunto no vacio A por si mismo varias veces, usaremos

$$A^n := A \times A \times \ldots A \text{ (n veces)}$$

§1.2 Relaciones

Definición 1.15 — Relacion binaria de dos conjuntos. Sean A y B dos conjuntos no vacios. Una relacion binaria entre A y B es un subconjunto $R \subseteq A \times B$.

Definición 1.16 — Relacion binaria en un conjunto. Sea A un conjunto no vacio. Una relacion binaria en A es ub subconjunto $R \subseteq A \times A$.

Sea R una relacion entre dos conjuntos A y B. Si $(a, b) \in R$ decimos que a esta relacionado con b por R y escribimos: aRb

Ejemplo 1.5. $A \times B = 1, 2, 3 \times 2, 4$.
Una relacion es $R_1 = \{(1, 2), (1, 4)\}$ o $R_2 = \{(1, 2), (2, 2), (3, 4)\}$. El producto cartesiano $A \times B$ o $\varnothing$ tambien son relaciones.

Observación 1.3. Como $A \times B$ tiene 6 elementos, puedo encontrar $2^6 = 64$ relaciones distintas (porque $A \times B$ tiene 64 subconjuntos distintos).

Definición 1.17 — Dominio, imagen. Sea R una relacion binaria entre dos conjuntos A y B. Se definen

- Dominio de R como

$$dom(R) := \{a \in A \mid \exists b \in B \mid aRb\}$$

- Imagen o rango de R como

$$im(R) := \{b \in B \mid \exists a \in A \mid aRb\}$$

Definición 1.18. Sea R una relacion binaria entre dos conjuntos A y B. Sean $C \subseteq A$ y $D \subseteq B$. Se definen:

- Imagen inversa de D por R como
$$R^{-1}(D) := \{a \in A \mid \exists b \in D \mid aRb\}$$
- Imagen o imagen directa de C por R como
$$R(C) := \{b \in B \mid \exists a \in C \mid aRb\}$$

Observación 1.4.
$$dom(R) = R^{-1}(B)$$
$$im(R) = R(A)$$

Ejemplo 1.6. Sean $A = \{1, 3, 5\}$, $B = \{2, 3\}$, $C = \{1, 3\} \subseteq A$, $D = \{2\} \subseteq B$.

- $R_1 = \{(1, 2), (3, 2), (3, 3)\}$
$$dom(R_1) = \{1, 3\},\ im(R_1) = \{2, 3\},\ R_1^{-1}(D) = \{1, 3\},\ R_1(C) = \{2, 3\}$$
- $R_2 = \{(1, 2), (3, 3), (5, 2)\}$ - Funcion.
$$dom(R_2) = A, im(R_2) = B, R_2^{-1}(D) = \{1, 5\}, R_2(C) = \{2, 3\} = B$$

En total habia 2^6 relaciones entre A y B.

Ejemplo 1.7. Sean $A = \{1, 2, 4, 5\}$, $C = \{2, 5\} \subseteq A$.

- $R_1 = \{(x, y) \mid x = y\}$
$$dom(R_1) = A, im(R_1) = A, R_1^{-1}(C) = \{2, 5\} = C, R_1(C) = \{2, 5\} = C$$
- $R_2 = \{(x, y) \mid x \neq y\} = A^2 \setminus R_1$
$$dom(R_2) = A, im(R_2) = A, R_2^{-1}(C) = A, R_2(C) = A$$
- $R_3 = \{(x, y) \mid x < y\}$
$$dom(R_3) = \{1, 2, 4\}, im(R_4) = \{2, 4, 5\}, R_3^{-1}(C) = \{1, 2, 4\}, R_3(C) = \{4, 5\}$$
- $R_4 = \{(x, y) \mid x \leq y\} = R_1 \cup R_3$
$$dom(R_4) = A, im(R_4) = A, R_4^{-1}(C) = A, R_4(C) = \{2, 4, 5\}$$

- $R_5 = \{(x, y) \mid x \text{ es divisor de } y\} = \{(1,1),(1,2),(1,4),(1,5),(2,2),(2,4),(4,4),(5,5)\}$

$$dom(R_5) = A, im(R_5) = A, R_5^{-1}(C) = \{2,4,5\}, R_5(C) = \{2,4,5\}$$

- $R_6 = \{(1,1),(1,4),(2,4)\}$

$$dom(R_6) = \{1,2\}, im(R_6) = \{1,4\}, R_6^{-1}(C) = \varnothing, R_6(C) = \{4\}$$

Definición 1.19. Sean P y Q dos enunciados. La notacion

$$P \Rightarrow Q$$

se lee "P implica Q".
El unico caso en el que es falsa es cuando sucede P y no sucede Q. Esta situacion supone un contraejemplo a la implicacion.
La notacion

$$P \Leftrightarrow Q$$

se lee "P si y solo si Q" o "P es equivalente a Q" y quiere decir que $P \Rightarrow Q$ y $Q \Rightarrow P$ simultaneamente. Es falsa si sucede una de las dos afirmaciones y no la otra.

Definición 1.20. Sean A un conjunto no vacio y R una relacion binaria en A. Decimos que R cumple la propiedad

- Reflexiva si $\forall x \in A\ (xRx)$
- Simetrica si $\forall x, y \in A\ (xRy \Rightarrow yRx)$
- Antisimetrica si $\forall x, y \in A\ (xRy, x \neq y \Rightarrow y \not{R} x)$
  También se puede formular: $\forall x, y \in A\ (xRy, yRx \Rightarrow x = y)$
- Transitiva si $\forall x, y, z \in A\ (xRy, yRz \Rightarrow xRz)$

Definición 1.21. Sean A un conjunto no vacio y R una relacion binaria en A. Decimos que R es una relacion de

- Equivalencia si cumple las propiedades reflexiva, simetrica y transitiva.
- Orden si cumple las propiedades reflexiva, antisimetrica y transitiva.
- Orden total si es de orden y ademas $\forall x, y \in A\ (xRy \text{ o } yRx)$

Ejemplo 1.8. Sea $A = \{a, b, c, d\}$. Para cada una de las siguientes relaciones R_i en A, estudia si cumplen las propiedades reflexiva, simetrica, antisimetrica y transitiva. Tambien si son de equivalencia, orden y orden total.

- $R_1 = \{(a, b), (b, c)\}$
- $R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c)\}$
- $R_3 = \{(a, b), (c, d), (d, c)\}$
- $R_4 = A \times A$
- $R_5 = \varnothing$
- $R_6 = \{(x, y) \mid x = y\}$
- $R_7 = R_6 \cup \{(a, b), (b, a), (c, d), (d, c)\}$
- $R_8 = \{(x, y) \mid x \text{ va antes que } y \text{ en el alfabeto}\}$
- $R_9 = R_6 \cup R_8$
- $R_{10} = R_6 \cup \{(a, b), (c, d)\}$

Solucion:

- $R_1 = \{(a, b), (b, c)\}$

  No es reflexiva porque $a \not{R} a$ (contraejemplo). Por tanto no es de equivalencia ni de orden y, por tanto, no es de orden total.

  Tampoco es simetrica porque aRb pero $b \not{R} a$. R_1 es antisimetrica porque se cumple la definicion. Por ultimo, no es transitiva porque aRb y bRc pero $a \not{R} c$.

- $R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c)\}$

  R_2 no es reflexiva (contraejemplo: $d \not{R} d$). Luego no es de equivalencia, orden ni orden total.

  No es simetrica porque bRc pero $c \not{R} b$. Tampoco es antisimetrica porque $aRb, a \neq b \Rightarrow bRa$. Por ultimo, no es simetrica porque aRb y bRc pero $a \not{R} c$.

- $R_3 = \{(a, b), (c, d), (d, c)\}$.

  No es reflexiva. Contraejemplo: $a \not{R} a$. No es simetrica porque aRb pero $b \not{R} a$. No es antisimetrica porque cRd y dRc y $d \neq c$. No es transitiva porque cRd y dRc pero $c \not{R} c$.

- $R_4 = A \times A$.

  Es reflexiva porque se cumple la definicion (todos los elementos de A estan relacionados consigo mismos). Es simetrica (se cumple la definicion). No es antisimetrica: aRb y bRa. Es transitiva.

  Es una relacion de equivalencia.

- $R_5 = \varnothing$.

  No es reflexiva, $a \not R a$. Es simetrica porque se cumple la definicion (no hay ningun contraejemplo). Tambien es antisimetrica y transitiva por la misma razon.

- $R_6 = \{(x, y) \mid x = y\} = \{(a, a), (b, b), (c, c), (d, d)\}$.

  Es reflexiva ya que todos los elementos estan relacionados consigo mismos. Es simetrica y antisimetrica ($xRy, yRx \Rightarrow x = y$). Tambien es transitiva, ya que no hay ningun contraejemplo (xRy, yRz solo puede pasar si $x = y = z$).

  R_6 es una relacion de equivalencia y de orden. No es de orden total porque $a \not R b$ y $b \not R a$.

- $R_7 = R_6 \cup \{(a, b), (b, a), (c, d), (d, c)\}$.

  Es reflexiva porque estan los pares de R_6 (es decir, $R_6 \subseteq R_7$). Es simetrica porque en los pares que he añadido no he metido contraejemplos. No es antisimetrica; un contraejemplo es aRb, bRa. Es transitiva pues no se pueden encontrar contraejemplos.

  R_7 es de equivalencia. No es de orden y, por tanto, tampoco de orden total.

- $R_8 = \{(x, y) \mid x \text{ va antes que } y \text{ en el alfabeto}\}$

  No es reflexiva. No es simetrica (aRb y $b \not R a$). Es antisimetrica porque no hay contraejemplos. Es transitiva.

  Vamos a ver que es antisimetrica y transitiva solo con la definicion. Supongamos que A es el alfabeto español. $|A| = 27$ y R_8 es la misma relacion.

  Si α va antes que β, β va antes que λ, entonces α va antes que λ. Luego si es transitiva.

  Si α va antes que β ($\alpha R_8 \beta$) entonces β no va antes que α, luego ($\beta \not R_8 \alpha$). Entonces es antisimetrica.

- $R_9 = R_6 \cup R_8 = \{(\alpha, \beta) \mid \alpha \text{ va antes que } \beta \text{ o } \alpha = \beta\}$.

  Es reflexiva porque estan todos los pares de R_6. No es simetrica porque aRb pero $b \not R a$.

  Es antisimetrica: vamos a usar la definicion $\alpha R_9 \beta, \beta R_9 \alpha \Rightarrow \alpha = \beta$. α va antes o es igual que β y β va antes o es igual que α. La unica opcion es $\alpha = \beta$. Por tanto es antisimetrica.

  Si α va antes o es igual a β y β va antes o es igual a γ entonces α va antes o es igual a γ. Luego si es transitiva.

  R_9 es de orden. Tambien es de orden total porque todos los elementos estan relacionados.

- $R_{10} = R_6 \cup \{(a, b), (c, d)\}$

  Es reflexiva porque estan todos los pares de R_6. No es simetrica porque aRb pero $b \not R a$. Es antisimetrica. Es transitiva porque no se han añadido contraejemplos.

R_{10} es una relacion de orden. No es total ($a \not{R}_{10} c$).

Ejemplo 1.9.
$A = \{$conjunto formado por 9 boligrafos, dos rojos, tres azules y 4 negros$\}$
Dados $x, y \in A$, $xRy \Leftrightarrow$ x es del mismo color que y.
Tambien se puede definir $R = \{(x, y) \mid \text{x es del mismo color que y}\}$.
Esta relacion es reflexiva: $\forall x, x$ es del mismo color que x. Tambien es simetrica: si xRy (x es del mismo color que y), entonces yRx (y es del mismo color que x). Por ultimo, es transitiva: $\forall x, y, z$ si x es del mismo color que y, y es del mismo color que z, entonces x es del mismo color que z.
Luego R es de equivalencia. Una relacion de equivalencia genera una particion. A los elementos de la particion se les llama “clases de equivalencia”. En este caso, hay 3 clases de equivalencia: la de los bolis rojos, la de los bolis negros y la de los bolis azules:

$$\{B_1, B_2\} = [B_2]$$
$$\{B_3, B_4, B_5\} = [B_3]$$
$$\{B_6, B_7, B_8, B_9\} = [B_8]$$

B_2, B_3 y B_8 son representantes de clase (elegidos de forma arbitraria).
El conjunto cociente va a ser el conjunto formado por las clases de equivalencia $A/R = \{[B_2], [B_3], [B_8]\}$.

Definición 1.22 — Clase de equivalencia. Sea R una relacion de equivalencia en un conjunto A y sea $a \in A$. Llamamos clase de equivalencia de a por la relacion R al conjunto de todos los elementos de A que estan relacionados con a. Simbolicamente:

$$[a]_R \coloneqq \{b \in A \mid aRb\}$$

Si, por contexto, esta claro que solo podemos estar hablando de clases respecto de la relacion R, omitiremos el subindice y escribiremos $[a]$. Tambien se puede escribir $\overline{a}$.

Definición 1.23 — Conjunto cociente. Sea R una relacion de equivalencia en un conjunto A. Llamamos conjunto cociente de A bajo la relacion R al conjunto formado por todas las clases de equivalencia de la relacion. Simbolicamente:

$$A/R \coloneqq \{[a]_R \mid a \in A\}$$

Ejemplo 1.10. $R_4 = A \times A$.
$A = \{a, b, c, d\}$.
$[a]_{R_4} = \{a, b, c, d\}$.
$[b]_{R_4} = \{a, b, c, d\}$.

Hay una unica clase de equivalencia. El cociente es $A/R = \{[a]_{R_4}\}$.
Otra relacion de equivalencia es $R_6 = \{(x, y) \mid x = y\}$.
En este caso, $[a]_{R_6} = \{a\}$, $[b]_{R_6} = \{b\}$, $[c]_{R_6} = \{c\}$, $[d]_{R_6} = \{d\}$. El conjunto cociente esta formado por 4 elementos:

$$A/R_6 = \{[a]_{R_6}, [b]_{R_6}, [c]_{R_6}, [d]_{R_6}\}.$$

$R_7 = R_6 \cup \{(a, b), (b, a), (c, d), (d, c)\}$. En este caso, hay 2 clases:
$[a]_{R_7} = \{a, b\} = [b]_{R_7}$ y $[c]_{R_7} = \{b, c\} = [c]_{R_7}$.
El conjunto cociente es $A/R_7 = \{[a]_{R_7}, [d]_{R_7}\}$.
Otro ejemplo es $R = S \cup \{(a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$, siendo S la relacion de igualdad. Se puede demostrar que es una relacion de equivalencia.
Las clases de equivalencia son $[a]_R = \{a, b, c\} = [b]_R = [c]_R$ y $[d]_R = \{d\}$. El conjunto cociente es $A/R = \{[a]_R, [d]_R\}$.

Proposición 1.3. Sean R una relacion de equivalencia en un conjunto A y $a, b \in A$. Se cumple:

- $aRb \Rightarrow [a] = [b]$.
- $a\not{R}b \Rightarrow [a] \cap [b] = \varnothing$.

Proof.

Sean $a, b \in A$.

- Si aRb:

  Tenemos que demostrar que $[a] = [b]$. Para ello, vamos a ver un doble contenido de conjuntos.

  $\subseteq$) Vamos a ver que $[a] \subseteq [b]$.

  $[a] = \{x \in A \mid aRx\}$ y $[b] = \{x \in B \mid bRx\}$.

  Sea $x \in [a] \Rightarrow aRx$. Como aRx y R es simetrica (por ser una relacion de equivalencia), tenemos que xRa. Como xRa y aRb, por ser R transitiva, tengo que $xRb \overset{R \text{ simetrica}}{\Rightarrow} bRx \Rightarrow x \in [b]$.

  $\supseteq$) Sea $x \in [b] \Rightarrow bRx$.

  Como aRb y R es transitiva, $aRx \Rightarrow x \in [a]$.

- Si $a\not{R}b$:

  Tenemos que demostrar que $[a] \cap [b] = \varnothing$. Por reduccion al absurdo, supongamos que $[a] \cap [b] \neq \varnothing \Rightarrow \exists x \in [a]$ y $x \in [b]$.

  Sin embargo, $x \in [a] \Rightarrow aRx$ y $x \in [b] \Rightarrow bRx \Rightarrow xRb$ (R simetrica). Como aRx, xRb y R es transitiva entonces aRb. Hemos llegado a una contradiccion porque partimos de que $a\not{R}b$.

Por tanto, $[a] \cap [b] = \varnothing$.

■

Definición 1.24 — Conjuntos disjuntos. Sean A y B dos conjuntos. Decimos que son disjuntos si $A \cap B = \varnothing$.

Definición 1.25 — Partición. Sea A un conjunto. Decimos que una coleccion de subconjuntos de A constituye una particion de A si se cumplen las dos condiciones siguientes:

- Son disjuntos dos a dos: dos conjuntos diferentes cualesquiera de la coleccion son disjuntos.
- Recubren A: la union de todos ellos es A.

Teorema 1.2. Sea R una relacion de equivalencia en un conjunto A. Entonces las clases de equivalencia de R constituyen una particion de A.

Proof.

En la proposicion 3 hemos demostrado que las clases de equivalencia son disjuntas dos a dos.
Veamos que las clases recubren A.
Dado $a \in A$ se cumple que por ser R reflexiva que $aRa \Rightarrow a \in [a]$.
Luego todo elemento pertenece a una clase de equivalencia. ■

Ejemplo 1.11. $A = \{a, b, c, d\}$.
Una particion es: $A_1 = \{a\}$ $A_2 = \{b, d\}$ $A_3 = \{c\}$.
Defino R como: $R = \{(a, a), (b, b), (c, c), (d, d), (b, d), (d, b)\}$.
Entonces $[a] = \{a\}, [b] = \{b, d\}, [c] = \{c\}$. Dentro de cada conjunto de la particion he relacionado sus elementos de todas las formas posibles.

Teorema 1.3. Supongamos que tenemos una particion de un conjunto A. Definimos una relacion R en A de la siguiente forma:

$$aRb \Leftrightarrow \text{existe un subconjunto de la particion al que } a \text{ y } b \text{ pertenecen}$$

Entonces la relacion R es de equivalencia.

Ademas, las clases de equivalencia de R coinciden con los subconjuntos de la particion.

Proof.

Vamos a demostrar que R es de equivalencia.

- R es reflexiva?

  Dado $a \in A$, como la particion recubre A existe un conjunto de la particion al que a pertenece. Luego a y a estan en el mismo conjunto de la particion $\Rightarrow aRa$.

- R es simetrica?

  $aRb \Rightarrow a$ y b estan en el mismo conjunto de la particion $\Rightarrow bRa$.

  Por tanto, R es simetrica.

- R es transitiva?

  $aRb, bRc \Rightarrow a$ y b estan en el mismo conjunto de la particion y b y c estan en el mismo conjunto de la particion. Por lo tanto, a y c estan en el mismo conjunto y aRc.

Las clases de R son los conjuntos de la particion por construccion.

$$[a]_R = \{b \mid aRb\} = \{b \mid \text{a y b estan en el mismo conjunto de particion}\}$$

Luego es el conjunto de la particion al que a pertenece. ∎

Ejemplo 1.12. Cuantas relaciones de equivalencia se pueden definir sobre un conjunto de 4 elementos?

Proof.

Es lo mismo que contar cuantas particiones diferentes se pueden hacer de un conjunto de 4 elementos. Cuento por numero de "trozos".

- Con un subconjunto. Solo hay una particion que es tomar todo el conjunto.
- Con 2 trozos. En total, hay 7 trozos (3 con 2 trozos iguales, 4 con un trozo de 1 elemento y otro de 3).
- Con 3 trozos. Los trozos deben ser 2 de 1 elemento y otro de 2. Hay 6 distintas.
- Con 4 trozos hay una unica forma.

Hay $1+7+6+1 = 15$ relaciones de equivalencia distintas en A. Ver: Numeros de Bell. ∎

Ejemplo 1.13. Dos relaciones de equivalencia importantes:

- Construccion de los racionales.
- Enteros modulo 2.

Proof.

- Los numeros racionales como cociente.

  Si defino los racionales como $F = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$:

  En el conjunto F de fracciones vamos a definir una relacion R tal que

  $$\frac{a}{b} R \frac{c}{d} \Leftrightarrow a \cdot d = c \cdot b$$

  Vamos a demostrar que R es de equivalencia.

  - R reflexiva: $\forall a, b$ se cumple
    $\frac{a}{b} R \frac{a}{b}$
  - Simetrica: $\forall \frac{a}{b} \cdot \frac{c}{d}$
    $\frac{c}{d} R \frac{a}{b} \Rightarrow cb = ad \Rightarrow \frac{a}{b} R \frac{c}{d}$
  - Transitiva: $\forall \frac{a}{b} \cdot \frac{c}{d} \cdot \frac{e}{f}$
    $\frac{a}{b} R \frac{c}{d}, \frac{c}{d} R \frac{e}{f} \Rightarrow \frac{a}{b} R \frac{e}{f}?$
    $\frac{a}{b} R \frac{c}{d} \Rightarrow ad = cb$, $\frac{c}{d} R \frac{e}{f} \Rightarrow cf = de$
    Debemos llegar a que $af = eb$

    $$adf = cbf \Rightarrow adf = deb$$

    Como d es un denominador, implica que $d \neq 0$ y puedo dividir ambos enteros entre $d \Rightarrow af = eb$.

  Luego la relacion R es de equivalencia. Como son las clases?

  Por ejemplo:

  $$\left[\frac{2}{3}\right] = \left\{\frac{2}{3}, \frac{6}{9}, \dots, \frac{-2}{-3}, \frac{-4}{-6}, \dots\right\}$$

  $|[\frac{2}{3}]| = \infty$

  $F/R = \{[\frac{a}{b}] \mid \frac{a}{b} \in F\} = \mathbb{Q}$.

  Quien es $[\frac{4}{6}]$?

Luego en este cociente $[\frac{2}{3}] = [\frac{4}{6}]$.

Obs: $|Q| = \infty$.

- Enteros modulo 2.

  $A = \mathbb{Z}$. Dados $x, y \in \mathbb{Z}$, $xRy \Leftrightarrow x - y$ es par. Es decir, $\exists k \in \mathbb{Z}$ tal que $x - y = 2k$ ($x \equiv y \bmod 2$) (x congruente con y modulo 2).

  Veamos si esta relacion es de equivalencia:

  - Reflexiva: $\forall x \in \mathbb{Z},\ x \equiv x \bmod 2$?

    Si porque $x - x = 2 \cdot 0 = 0$
  - Simetrica: $\forall x, y \in \mathbb{Z},\ x \equiv y \bmod 2 \Rightarrow y \equiv x \bmod 2$?

    Si $x \equiv y \bmod 2 \Rightarrow \exists k \in \mathbb{Z}$ tal que $x - y = 2k \Rightarrow y - x = 2(-k) \Rightarrow y \equiv x \bmod 2$.
  - Transitiva: $\forall x, y, z \in \mathbb{Z},\ x \equiv y \bmod 2, y \equiv z \bmod 2 \Rightarrow x \equiv z \bmod 2$?

    $x \equiv y \bmod 2 \Rightarrow \exists k \in \mathbb{Z}/x - y = 2k$

    $y \equiv z \bmod 2 \Rightarrow \exists m \in \mathbb{Z}/y - z = 2m$.

    Sumando $x - y + y - z = 2k + 2m \Rightarrow x - z = 2(k + m)$. Por tanto $x \equiv z \bmod 2$.

  Hemos visto que la congruencia modulo 2 es una relacion de equivalencia.

  Ejemplos de enteros relacionados: $8 \equiv 6 \bmod 2$, $3 \equiv 7 \bmod 2$, $4 \equiv 4 \bmod 2$.

  Clases de equivalencia:

  $[1] = \{\ldots, -3, -1, 1, 3, 5, 7, \ldots\} = [3] = [5] = \ldots$

  $[2] = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = [4] = [0] = \ldots$

  Luego hay 2 clases y $\mathbb{Z}/\equiv \bmod 2 = \{[0], [1]\} = \mathbb{Z}_2$.

■

Definición 1.26 — Orden parcial. Decimos que una relacion es de orden parcial si es de orden pero no es de orden total.

Ejemplo 1.14.

- Relacion “menor o igual” en $\mathbb{Z}$ (orden total).
- Relacion “contenido o igual” en $\mathcal{P}(A)$, siendo A un conjunto (orden parcial si $|A| \geq 2$, orden total si $|A| = 1$ o $A = \varnothing$).

Definición 1.27. Sean $n \in \mathbb{N}, n \geq 2$ y $A_1, A_2, \ldots, A_n$ conjuntos no vacios. Una relacion n-aria entre $A_1, A_2, \ldots, A_n$ es un subconjunto $R \subseteq A_1 \times A_2 \times \cdots \times A_n$.

§1.3 Funciones

Definición 1.28 — Función. Sean A y B conjuntos no vacios. Decimos que f es una funcion de A en B si es una relacion binaria entre A y B tal que cada elemento de A esta relacionado con un unico elemento de B. Simbolicamente:

- $f \subseteq A \times B$
- $\forall a \in A\ \exists! b \in B \,/\, afb$

Dado cualquier $a \in A$, al unico $b \in B$ que esta relacionado con a lo llamamos imagen de a por f $(b = f(a))$.

Observación 1.5. Si f es una funcion, entonces $dom(f) = A$.

Definición 1.29 — Codominio. Si f es una funcion de A en B, decimos que B es el codominio de f.

Si f es una funcion de A en B es tipico escribir

$$\begin{aligned} f\colon A &\longrightarrow B \\ x &\mapsto f(x) = y \end{aligned}$$

Ejemplo 1.15.

$$\begin{aligned} f\colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\mapsto f(x) = x^2 - 5 \end{aligned}$$

$(1, -4) \in f$, $1f-4$, $f(1) = -4$

Definición 1.30 — Funcion inyectiva. Sea $f\colon A \to B$ una funcion. Decimos que f es inyectiva si no hay dos elementos que tengan la misma imagen. Simbolicamente:

$$\forall a, a' \in A\ (a \neq a' \Rightarrow f(a) \neq f(a'))$$

Tambien se puede escribir:

$$\forall a, a' \in A\ (f(a) = f(a') \Rightarrow a = a')$$

Definición 1.31 — Funcion suprayectiva. Sea $f\colon A \to B$ una funcion. Decimos que f es suprayectiva o sobreyectiva si todo elemento de B es imagen de algun elemento de A.

Simbolicamente:

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

Es decir, $Im(f) = B$.

Definición 1.32 — Funcion biyectiva. Sea $f\colon A \to B$ una funcion. Decimos que f es biyectiva si es inyectiva y suprayectiva a la vez. Por tanto,

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

Observación 1.6. Para que exista una funcion inyectiva entre dos conjuntos finitos es necesario que tengan el mismo cardinal.

Observación 1.7. "Calcular el dominio de una funcion".
Estamos resolviendo "busca el conjunto mas grande de numeros reales que pueda ser dominio de una funcion con esta expresion".
Puedo definir una funcion

$$\begin{aligned} f\colon \mathbb{R} \setminus \{1, -1\} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = \frac{x^2}{x^2 - 1} \end{aligned}$$

o tambien

$$\begin{aligned} g\colon (2, +\infty) &\longrightarrow \mathbb{R} \\ x &\longmapsto g(x) = \frac{x^2}{x^2 - 1} \end{aligned}$$

Definición 1.33. Sean $f\colon A \to B$ y $g\colon B \to C$ dos funciones. Se define una nueva funcion, llamada la composicion de f con g como una nueva funcion:

$$\begin{aligned} g \circ f\colon A &\longrightarrow C \\ x &\longmapsto y = (g \circ f)(x) := g(f(x)) \end{aligned}$$

Ejemplo 1.16. $A = \{1, 2, 3\}$
$B = \{a, b, c, d\}$
$C = \{2, 4, 6, 8\}$

$$
\begin{aligned}
f\colon A &\longrightarrow B \\
1 &\longmapsto f(1) = a \\
2 &\longmapsto f(2) = a \\
3 &\longmapsto f(3) = d
\end{aligned}
\qquad
\begin{aligned}
g\colon B &\longrightarrow C \\
a &\longmapsto f(a) = 2 \\
b &\longmapsto f(b) = 2 \\
c &\longmapsto f(c) = 6 \\
d &\longmapsto f(d) = 8
\end{aligned}
$$

Entonces

$$
\begin{aligned}
g \circ f\colon A &\longrightarrow C \\
1 &\longmapsto 2 \\
2 &\longmapsto 2 \\
3 &\longmapsto 8
\end{aligned}
$$

La composicion $f \circ g$ no tiene sentido (contraejemplo: f no esta definido en 8).

Ejemplo 1.17.

$$
\begin{aligned}
f\colon \mathbb{R} &\longrightarrow \mathbb{R} \\
x &\longmapsto f(x) = 2x + 1
\end{aligned}
$$

$$
\begin{aligned}
g\colon \mathbb{R} &\longrightarrow \mathbb{R} \\
x &\longmapsto g(x) = x^2
\end{aligned}
$$

Por ejemplo: $(g \circ f)(4) = g(f(4)) = g(9) = 81$
La expresion general de $g \circ f$ es: $(g \circ f)(x) = g(f(x)) = g(2x+1) = (2x+1)^2 = 4x^2+4x+1$.
En este caso si tiene sentido $f \circ g$:

$$(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2 + 1$$

Vamos a justificar que $f \circ g \neq g \circ f$. Hemos visto que $(g \circ f)(4) = 81$.
$(f \circ g)(4) = 2 \cdot 4^2 + 1 = 33$.
Luego son funciones distintas.

Observación 1.8. Para definir la composicion $g \circ f$ para dos funciones cualesquiera es suficiente que $im(f) \subseteq dom(g)$.

Definición 1.34 — Funcion identidad. Sea A un conjunto. Se define la funcion identidad en A como

$$
\begin{aligned}
id_A\colon A &\longrightarrow A \\
x &\longmapsto id_A(x) = x
\end{aligned}
$$

Definición 1.35. Sea $f\colon A \to B$ una funcion. Se dice que f tiene inversa si exista otra funcion $g\colon B \to A$ que cumple:

- $\forall a \in A\ ((g \circ f)(a) = a)$
- $\forall b \in B\ ((f \circ g)(b) = b)$

En ese caso se dice que g es la funcion inversa de f $(g = f^{-1})$.

Observación 1.9. Las dos condiciones anteriores se pueden reformular como

- $g \circ f = id_A$
- $f \circ g = id_B$

Observación 1.10. No todas las funciones tienen inversa.
Ejemplo: Sea $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$.
No existe ningun $a \in \mathbb{R}$ tal que $a^2 = -3$. Eso me impide que haya inversa.
Ahora, definimos $g\colon \mathbb{R} \to [0, +\infty],\ x \mapsto x^2$.
En este caso, tampoco tiene inversa porque no puedo definir una funcion que vaya bien para 4 $(f(2) = 4$ y $f(-2) = 4)$ o cualquier otro numero.

Teorema 1.4. Sea $f\colon A \to B$ una funcion. Se cumple

$$f \text{ tiene inversa} \Leftrightarrow f \text{ es biyectiva}$$

Proof.

$\Rightarrow$) Vamos a demostrar que si f tiene inversa, entonces f es biyectiva.
Al ser inversa, $\exists$ una funcion $g\colon B \to A$ tal que $f \circ g = id_A$ y $g \circ f = id_B$.

1. Vamos a ver que f es inyectiva. Sean $x, y \in A$ tales que $f(x) = f(y)$.

   Aplico la funcion g a ambos lados.

   $$\underbrace{g(f(x))}_{=x(id_A)} = \underbrace{g(f(y))}_{=y(id_B)}$$

   Por tanto, $x = y$.

2. Vamos a ver que f es suprayectiva. Sea $b \in B$ cualquiera. Tenemos que encontrar una preimagen de b, es decir, un $x \in A$ tal que $f(x) = b$.

   Tomo $x = g(b)$ ya que $f(x) = f(g(b)) = b$.

   Por tanto, f es biyectiva.

$\Leftarrow$) Vamos a demostrar que si f es biyectiva, entonces tiene inversa.
Vamos a formalizar la idea de “darle la vuelta a las flechas”.
Como se escribe f si la veo como una relacion? $f = \{(a, b) \mid a \in A, b = f(a)\}$.

Voy a construir la relacion $g \coloneqq \{(b, a) \mid a \in A, b = f(a)\}$.
Basta con comprobar que g es una funcion.
Como f es suprayectiva, tenemos que $dom(g) = B$, es decir, todos los elementos de B tienen imagen.
Como f es inyectiva, no hay ningun elemento de B que tenga dos imagenes distintas por g.
Por construccion, g que hemos visto que es una funcion, cumple la definicion de ser inversa de f. Por tanto, f tiene inversa. ■

Observación 1.11.

$$\begin{aligned} f\colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = e^x \end{aligned}$$

Como funcion de $\mathbb{R}$ en $\mathbb{R}$, e^x no tiene inversa, ya que no es suprayectiva.
En cambio, si consideramos

$$\begin{aligned} f\colon \mathbb{R} &\longrightarrow (0, +\infty) \\ x &\longmapsto f(x) = e^x \end{aligned}$$

Esta funcion si es biyectiva porque el codominio coincide con la imagen. En este caso su inversa es

$$\begin{aligned} g\colon (0, +\infty) &\longrightarrow \mathbb{R} \\ x &\longmapsto g(x) = \ln(x) \end{aligned}$$

Asi definidas se cumple $f^{-1} = g$.

Observación 1.12. Si $f^{-1} = g$, tambien es cierto que $g^{-1} = f$.

Observación 1.13. La notacion f^{-1} es ambigua. Puede referirse a la inversa de f, en el caso de que esta exista, o la imagen inversa de un conjunto por la relacion f.
Ejemplo: Dada $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^3$ (biyectiva y tiene inversa).
$f^{-1}(64) = 4,\ f^{-1}(2) = \sqrt[3]{2},\ f^{-1}([8, 64]) = [2, 4]$.

Otro ejemplo es $f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$.
$f^{-1}(9)$ no tiene sentido porque f no es biyectiva y por tanto no tiene inversa. En cambio, $f^{-1}(\{9\}) = \{3, -3\}$ o $f^{-1}([25, 49]) = [5, 7] \cup (-7, 5]$

2 Sintaxis de la lógica proposicional

§2.1 Definicion de formula

Definición 2.1 — Lenguaje, informal.

- Llamamos alfabeto a un conjunto A, cuyos elementos se denominan simbolos.
- Una palabra sobre A es una sucesion finita de simbolos de A, escritos uno a continuacion de otro.
- El conjunto de todas las palabras sobre A se denota como A^*.
- Un lenguaje sobre A es un subconjunto $L \subseteq A^*$.

Ejemplo 2.1. $A :=$ {letras, mayusculas o minusculas, del alfabeto}
$L :=$ {palabras que aparecen en el diccionario de la RAE .}
$A := \{0, 1\}$
$L_1 := A^*$ (todas las cadenas finitas de bits).
$L_2 := \{x \in A^* \mid x \text{ consta exactamente de 8 simbolos }\}$

Ejemplo 2.2. $A := \{0, 1\}$. Reglas que definen L:

1. $00 \in L$.
2. $w \in L, v \in L \Rightarrow wv \in L$ (cerrado por concatenacion).
3. $w \in L \Rightarrow w1 \in L$
4. Cualquier palabra que no se pueda obtener con la aplicacion de las reglas anteriores, no esta en L.

Se puede demostrar que L consiste en todas las cadenas de bits que comienzan por 00 y que no tienen una cantidad impar de ceros consecutivos.
Ejemplos de palabras que estan en el lenguaje L: $00 \in L(1), 0000 \in L(2), 001 \in L(3), 00100 \in L(2)$.

Definición 2.2 — Alfabeto de la logica proposicional. $A := \{p_1, p_2, p_3, \ldots\} \cup \{\top, \bot, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$

Nombre	Simbolo	Tipo	Aridad
Proposición atómica	p_i	Proposición atómica	-
Verdadero	$\top$	Conectiva	0
Falso	$\bot$		
Negación	$\neg$		1
Conjunción	$\vee$		2
Disyunción	$\wedge$		
Implicación	$\rightarrow$		
Doble implicación	$\leftrightarrow$		
Paréntesis izquierdo	(	Auxiliar	-
Paréntesis derecho	)		

Definición 2.3. Vamos a definir el lenguaje $\mathcal{F}_0 \subseteq A^*$ de las formulas de la logica proposicional mediante las siguientes reglas de formacion:

1. Formulas atomicas:
   - Si p es un simbolo de proposicion atomica $\Rightarrow p \in \mathcal{F}_0$
   - $\top \in \mathcal{F}_0$
   - $\bot \in \mathcal{F}_0$
2. Si $\varphi \in \mathcal{F}_0 \Rightarrow \neg\varphi \in \mathcal{F}_0$.
3. Si $\varphi, \psi \in \mathcal{F}_0$ entonces:
   - $(\varphi \wedge \psi) \in \mathcal{F}_0$
   - $(\varphi \vee \psi) \in \mathcal{F}_0$
   - $(\varphi \rightarrow \psi) \in \mathcal{F}_0$
   - $(\varphi \leftrightarrow \psi) \in \mathcal{F}_0$
4. Cualquier palabra que no se pueda obtener con la aplicacion de las reglas anteriores, no esta en $\mathcal{F}_0$.

Observación 2.1. Con estas reglas de formacion estrictas que hemos dado en la definicion, $p \wedge q$ no es una formula.

Observación 2.2. Por economia de escritura, muchas veces escribiremos la tercera regla de la definicion anterior como:

- Si $\varphi, \psi \in \mathcal{F}_0$ entonces $(\varphi \circ \psi) \in \mathcal{F}_0$, donde $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

§2.2 Fórmulas en forma abreviada

Definición 2.4 — Reglas de eliminacion de parentesis. Vamos a dar 3 reglas que permiten eliminar parentesis de una formula, dando como resultado una formula en forma abreviada:

1. Se puede eliminar el parentesis externo.
2. Las conectivas binarias $\wedge$ y $\vee$ tienen precedencia sobre las conectivas binarias $\rightarrow$ y $\leftrightarrow$. Si se "enfrentan" dos de estas conectivas, se puede eliminar el parentesis correspondiente a la que tiene precedencia.
3. Dos conectivas binarias iguales asocian por la derecha. Si se "enfrentan" dos conectivas binarias iguales y el parentesis esta a la derecha, puede eliminarse.

El resultado de aplicar cualquier cantidad de veces estas reglas a una formula se considera una forma abreviada de esa formula que tambien la representa.

Observación 2.3. La formula $p \wedge q \vee r$ no es abreviada, ya que no se puede aplicar ninguna regla de las anteriores.

Observación 2.4. Hay infinitas formulas, incluso si considerasemos solo un conjunto finito de proposiciones atomicas.
Por ejemplo: $p, \neg p, \neg\neg p, \neg\neg\neg p, \ldots$

§2.3 Definicion por recursion de funciones sobre formulas

Ejemplo 2.3. La funcion factorial

$$\begin{aligned} \mathrm{fact}\colon \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n! \end{aligned}$$

se puede definir recursivamente mediante las siguientes dos reglas:

1. $\mathrm{fact}(1) \coloneqq 1$
2. $\forall n \geq 2 \quad \mathrm{fact}(n) \coloneqq n \cdot \mathrm{fact}(n-1)$

Observación 2.5. Para definir una funcion sobre $\mathbb{N}$ por recursion basta con definir $f(1)$ y, a partir de $f(n)$, calcular $f(n+1)$.

Ejemplo 2.4. Vamos a definir por recursion una funcion que devuelva el numero de simbolos de una formula.

$$\begin{aligned} f\colon \mathcal{F}_0 &\longrightarrow \mathbb{N} \\ \text{formula} &\longmapsto \text{numero} \end{aligned}$$

Definimos f:

1. Si φ es una formula atomica, $f(\varphi) \coloneqq 1$.
2. Si φ es una formula, $f(\neg\varphi) = 1 + f(\varphi)$
3. Si φ, ψ son formulas, $f(\varphi \wedge \psi) = 3 + f(\varphi) + f(\psi)$, $f(\varphi \vee \psi) = 3 + f(\varphi) + f(\psi)$...
   $f(\varphi \circ \psi) = f(\varphi) + f(\psi) + 3$ donde $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

$f(\neg((\neg p \rightarrow q)) \wedge r) = f((()\neg p \rightarrow q) \wedge r)) + 1 = f((\neg p \rightarrow q)) + f(r) + 3 + 1 = f(\neg p) + f(q) + 3 + 1 + 3 + 1 = f(p) + 1 + 1 + 3 + 1 + 3 + 1 = 1 + 1 + 1 + 3 + 1 + 3 + 1 = 11$

Ejemplo 2.5. Definir por recursion una funcion f sobre el conjunto $\mathcal{F}_0$ que, dada una formula φ, devuelva el numero total de apariciones de conectivas en φ.
Solucion:

$$\begin{aligned} f\colon \mathcal{F}_0 &\longrightarrow \mathbb{N} \cup \{0\} \\ \text{formula} &\longmapsto \text{num conectivas} \end{aligned}$$

Definimos f:

1. Si φ es una formula atomica, $f(\varphi) = 0$. $f(\top) = 1$, $f(\bot) = 1$.
2. Si φ es una formula, $f(\neg\varphi) = 1 + f(\varphi)$
3. Si φ, ψ son formulas, $f(\varphi \circ \psi) = 1 + f(\varphi) + f(\psi)$, siendo $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

Ejemplo 2.6. Definir por recursion una funcion f sobre el conjunto $\mathcal{F}_0$ que, dada una formula φ, devuelva el conjunto formado por todos los simbolos que aparecen en φ.
Solucion:
$A = \{p, q, \top, \bot, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$

$$\begin{aligned} f\colon \mathcal{F}_0 &\longrightarrow \mathcal{P}(A) \\ \varphi &\longmapsto f(\varphi) \end{aligned}$$

1. $f(\top) = \{\top\}, f(\bot) = \{\bot\}, f(p) = \{p\}$.
2. Dado $\varphi \in \mathcal{F}_0$, $f(\neg\varphi) = f(\varphi) \cup \{\neg\}$
3. $\varphi, \psi \in \mathcal{F}_0$, $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.
   $f((\varphi \circ \psi)) = f(\varphi) \cup f(\psi) \cup \{(,), \circ\}$

§2.4 Arbol estructural de una formula

Ejemplo 2.7. Vamos a construir (antes de definirlo) el arbol estructural de la formula (abreviada):

$$\neg(p \leftrightarrow \neg q \vee \top) \to q \wedge \neg r \to \neg(p \vee \bot \vee r)$$

Definición 2.5 — Grafos, muy informal. Un grafo no dirigido es un conjunto de puntos (vertices) unidos por segmentos (aristas).
El grado de un vertice es el numero de aristas que inciden en ese vertice.
Un camino entre dos vertices es una sucesion de aristas que conectan esos dos vertices.
La longitud del camino es el numero de aristas que lo componen.

Definición 2.6 — Arboles, muy informal. Un arbol es un tipo especial de grafo que cumple dos condiciones:

- Es conexo: entre dos vertices siempre hay algun camino.
- No tiene ciclos: no hay caminos que empiecen y acaben en el mismo vertice (sin repetir arista).

Un arbol con raiz es un arbol con vertice marcado (llamado raiz).
Las hojas de un arbol son los vertices “terminales”, es decir, los vertices de grado 1 (a excepcion de la raiz).
La profundidad de un arbol es la longitud del camino mas largo que va desde la raiz hasta una hoja.

Definición 2.7. La construccion del arbol estructural de una formula se puede definir mediante el siguiente procedimiento recursivo:

1. Si φ es una formula atomica, su arbol es un unico vertice etiquetado con φ. Este vertice es raiz y no hoja. Por definicion, tiene profundidad 0.
2. Dada una formula cualquiera φ, el arbol de $\neg\varphi$ consiste en un vertice raiz etiquetado con $\neg$ del que sale una arista (hacia abajo). En el otro extremo se “pega” el arbol de φ.
3. Dadas dos formulas cualesquiera φ, ψ y una conectiva binaria $\circ$, el arbol de $(\varphi \circ \psi)$ consiste en un vertice raiz etiquetado con $\circ$ del que salen dos aristas (hacia abajo, una hacia la izquierda y otra hacia la derecha). En el extremo de la arista izquierda se “pega” el arbol de φ y en el extremo de la arista derecha se “pega” el arbol de ψ.

Ejemplo 2.8. Definir por recursion una funcion f sobre el conjunto $\mathcal{F}_0$ que, dada una formula φ, devuelva el numero total de vertices del arbol estructural de φ.

$$\begin{aligned} f\colon \mathcal{F}_0 &\longrightarrow \mathbb{N} \\ \varphi &\longmapsto f(\varphi) = \text{ num vertices} \end{aligned}$$

1. Si φ es formula atomica, $f(\varphi) = 1$.
2. Dada $\varphi \in \mathcal{F}_0$.

   $f(\neg\varphi) = f(\varphi) + 1$
3. $\varphi, \psi \in \mathcal{F}_0$, $\circ \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

   $f(\varphi \circ \psi) = f(\varphi) + f(\psi) + 1$

Observacion: coincide con el numero de simbolos no auxiliares de la formula (porque cada vertice tiene un simbolo que no es un parentesis).

§2.5 Induccion para formulas

Definición 2.8. Sea P cierta propiedad que esta enunciada para formulas. Denotaremos como $P(\varphi)$ el hecho de que la formula φ cumpel la propiedad P.
Supongmaos que queremos demostrar que, para toda formula φ se tiene $P(\varphi)$. Esto se puede hacer por induccion sobre el conjunto de todas las formulas mediante los siguientes pasos:

1. Caso base: demostrar que, para toda formula atomica φ, se tiene $P(\varphi)$.
2. Para toda formula φ, suponiendo que es cierta la hipotesis de induccion $P(\varphi)$ demostrar que se cumple $P(\neg\varphi)$.
3. Para todo par de formulas φ, ψ y toda conectiva binaria $\circ$, suponiendo que es cierta la hipotesis de induccion: $P(\varphi)$ y $P(\psi)$ demostar que se cumple $P((\varphi \circ \psi))$.

Ejemplo 2.9. Demostrar por induccion que toda formula tiene el mismo numero de parentesis izquierdos que de derechos.
$P(\varphi) =$ "φ tiene mismos parentesis izquierdos y derechos".

1. Caso base: φ atomica. $P(\varphi)$?

   Si pongo una formula atomica tiene 0 parentesis en la izquierda y 0 en la derecha.
2. Negacion. H.I. $P(\varphi)$, T.I. $P(\neg\varphi) =?$. Num parentesis izq de $\neg\varphi =$ num parent izq de $\varphi =$ num parent dchos de $\varphi =$ num parent dchos de $\neg\varphi$.
3. Conectiva binaria.

   H.I. $P(\varphi)$, $P(\psi)$.

   T.I. $P((\varphi \circ \psi))$?

num parent izq de $(\varphi \circ \psi)$ = num parent izq de φ + num parent izq de $\psi + 1$ = num parent dchos de φ + num parent dchos de $\psi + 1$ = num parent dchos de $(\varphi \circ \psi)$.

§2.6 Formalizacion

Definición 2.9. Una proposicion es una oracion escrita en lenguaje natural de la que se podria afirmar que es verdadera o que es falsa.
Una proposicion atomica es una proposicion dentro de la que no puede encontrarse otra proposicion mas simple.

Observación 2.6. El “o” no es excluyente: cierto si pasa cualquiera de las dos cosas o las dos a la vez.

Tiene un papel muy importante la implicacion:

Ejemplo 2.10.

- p: “Llueve”
- q: “Hace viento”
- $p \to q$: “Si llueve, entonces hace viento”

p recibe los nombres: premisa, hipotesis, condicion suficiente.
q recibe los nombres: conclusion, tesis, condicion necesaria.

Observación 2.7. Una implicacion solamente es falsa en el caso en que se cumpla la premisa p y no la conclusion q. En el ejemplo, solamente si llueve y no hace viento.

Veamos la doble implicacion como la conjuncion de dos implicaciones:

Ejemplo 2.11. “Si llueve hace viento y si hace viento llueve”
Formalizacion: $(p \to q) \wedge (q \to p)$ o $p \leftrightarrow q$
es lo mismo que: “Solo si hace viento llueve y si hace viento llueve”
es lo mismo que: “Llueve solo si hace viento y llueve si hace viento”
es lo mismo que: “Llueve si hace viento y llueve solo si hace viento”
es lo mismo que: “Llueve si y solo si hace viento”

Definición 2.10 — Razonamiento. Llamamos razonamiento a un conjunto de premisas representadas por formulas $\varphi_1, \varphi_2, \ldots, \varphi_n$ seguidas de una conclusion que se deduce de ellas, representada por una formula ψ.
El razonamiento se presenta mediante la formula:

$$\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n \to \psi$$

3 Semantica de la logica proposicional

§3.1 Evaluacion semantica de formulas (valores de verdad)

Definición 3.1. Llamamos signatura al conjunto Σ formado por todos los simbolos de proposicion atomica.

Observación 3.1. Como en una formula o conjunto finito de formulas solo aparecera una cantidad finita de simbolos de proposicion atomica, por extension, llamaremos tambien signatura a cualquier conjunto finito de simbolos de proposicion atomica (y lo denotaremos tambien con Σ).

Definición 3.2. Sea Σ una signatura. Llamamos valoracion ...

Ejemplo 3.1. Sea $\Sigma = \{p, q, r\}$ Un ejemplo de valoracion sobre Σ es

$$\begin{aligned} v_1 \colon \Sigma &\longrightarrow (0,1) \\ p &\longmapsto 0 \\ q &\longmapsto 1 \\ r &\longmapsto 1 \end{aligned}$$

Observación 3.2. En total habria $2^3 = 8$ valoraciones diferentes.

Definición 3.3. Sea Σ la signatura formada por todos los simbolos de proposicion atomica y u una valoracion concreta definida sobre Σ. Vamos a definir por recursion una funcion que asocia a cada formula φ un valor de verdad que denotaremos $(\varphi)^u$, extendiendo la valoracion y de proposiciones atomicas a todas las formulas:

- Si p es un simbolo de proposicion atomica $\Rightarrow (p)^u := u(p)$, $(\bot)^u := 0$, $(\top)^u := 1$.
- Si $\varphi \in \mathcal{F}_0 \Rightarrow (\neg\varphi)^u := \begin{cases} 1 \text{ si } (\varphi)^u = 0 \\ 0 \text{ si } (\varphi)^u = 1 \end{cases}$

Definición 3.4. Sean $\varphi, \psi \in \mathcal{F}_0 \Rightarrow$

$$((\varphi \wedge \psi))^u := \begin{cases} 1 \text{ si } (\varphi)^u = (\psi)^u = 1 \\ 0 \text{ en otro caso} \end{cases}$$

$$((\varphi \vee \psi))^u := \begin{cases} 0 \text{ si } (\varphi)^u = (\psi)^u = 0 \\ 1 \text{ en otro caso} \end{cases}$$

$$((\varphi \to \psi))^u := \begin{cases} 0 \text{ si } (\varphi)^u = 1 \text{ y } (\psi)^u = 0 \\ 1 \text{ en otro caso} \end{cases}$$

$$((\varphi \leftrightarrow \psi))^u := \begin{cases} 1 \text{ si } (\varphi)^u = (\psi)^u \\ 0 \text{ si } (\varphi)^u \neq (\psi)^u \end{cases}$$

Observación 3.3. Si no se genera ambiguedad escribiremos φ^u en lugar de $(\varphi)^u$

Observación 3.4. Los valores de verdad de las conectivas binarias se pueden resumir con tablas de verdad.

Ejemplo 3.2. Sea u la valoracion dada por $u(p) = u(q) = 1, u(r) = 0$. Hallar φ^u siendo

$$\varphi = (p \to \neg(q \wedge r)) \leftrightarrow (p \vee \neg q \to \neg r)$$

$(q \wedge r)^u = 0$, $\neg(q \wedge r)^u = 1$, $(p \to \neg(q \wedge r))^u = 1$.
Por otro lado $(\neg q)^u = 0$, $(p \vee \neg q)^u = 1$, $(\neg r)^u = 1$, $(p \vee \neg q \to \neg r)^u = 1$
Por tanto, $\varphi^u = 1$.

§3.2 Modelos y contraejemplos. Clasificacion de formulas

Observación 3.5. Cuando hablemos de una formula φ y su valor de verdad bajo una valoracion u, supondremos siempre que los simbolos de proposicion atomica que aparecen en φ pertenecen al dominio de u.

Definición 3.5. Sean φ una formula y u una valoracion.

- Si $\varphi^u = 1$

Definición 3.6. Sea φ una formula. Decimos que φ es:

- satisfacible si $\exists u$ valoracion tal que $\varphi^u = 1$.

- insatisfacible si no es satisfacible.
- tautologia si $\forall u$ valoracion se tiene que $\varphi^u = 1$
- contradiccion si $\forall u$ valoracion se tiene que $\varphi^u = 0$
- contingencia si no es tautologia ni contradiccion

Observación 3.6. Esta clasificacion puede resumirse en la tabla

Satisfacible	Tautologia o contingencia
Insatisfacible	Contradiccion

Cuando hablemos de "clasificar una formula" nos referiremos a decidir si es tautologia, contingencia o contradiccion.

Ejemplo 3.3. Clasifica la formula

$$\varphi = (p \to \neg(q \wedge r)) \leftrightarrow (p \vee \neg q \to \neg r)$$

Ya hemos encontrado 2 modelos. Sabemos que es satisfacible.
Voy a buscar un contraejemplo. w para conseguir esto
Si $w(p) = 0 \Rightarrow (p \to \neg(q \wedge r))^w = 1$.
Voy a intentar que la segunda parte sea falsa.
$w(q) = 0 \Rightarrow (\neg q)^w = 1 \Rightarrow (\neg q)^w = 1$. $(p \vee \neg q)^w = 1$.
Si $w(r) = 1 \Rightarrow (\neg r)^w = 0 \Rightarrow (p \vee \neg q \to \neg r)^w = 0$.
$\varphi^w = 0$. Luego w es un contraejemplo de φ, por tanto φ es una contingencia.

Ejemplo 3.4. Demuestra que la siguiente formula es una tautologia

$$\varphi = (p \to q) \wedge (q \to r) \to (p \to r)$$

Lo demostraremos utilizando una tabla de verdad.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	φ
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

He visto que las 8 valoraciones posibles son modelos de φ. Por tanto, φ es una tautologia.

Ejemplo 3.5. Demuestra que la siguiente formula es una contradiccion

$$\varphi = (p \to q) \wedge (r \to s) \wedge p \wedge r \wedge (\neg q \vee \neg s)$$

$(p \wedge q) \wedge r$ y $p(q \wedge r)$ son verdaderas si y solo si $p = q = r = 1$. Son formulas distintas sintacticamente pero son equivalentes semanticamente.
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \equiv p \wedge q \wedge r$.

- Caso 1: Si $p = 0 \Rightarrow \varphi = 0$ (son 8 valoraciones).
- Caso 2: $p = 1$.
  - Caso 2.1: $r = 0 \Rightarrow \varphi = 0$ (son 4 valoraciones)
  - Caso 2.2 : $r = 1$

    Hacer tabla de verdad con q y s (4 filas). Salen todas falsas.

Luego φ es una contradiccion.
Alternativa: por reduccion al absurdo. Supongo que φ no es contradiccion $\Rightarrow$ existe u modelo de φ. Como es una conjuncion de varias formulas, tenemos que

$$u \begin{cases} p \to q = 1(a) \\ r \to s = 1(b) \\ p = 1(c) \\ r = 1(d) \\ \neg q \vee \neg s = 1(e) \end{cases}$$

$$\left.\begin{matrix} (a) + (c) \Rightarrow q = 1 \Rightarrow \neg q = 0 \\ (b) + (d) \Rightarrow s = 1 \Rightarrow \neg s = 0 \end{matrix}\right\} \Rightarrow \neg q \vee \neg s = 0 \text{ Contradicion con (e)} \Rightarrow$$

Por tanto, φ es contradiccion.

§3.3 Consecuencia logica

Definición 3.7. Sea $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ un conjintp de formulas y u una valoracion. Decimos que u es modelo de Φ si $\forall i (u \models \varphi_i)$.

Definición 3.8. Sean $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ un conjunto de formulas y ψ otra formula. Decimos que ψ es consecuencia logica de Φ si todo modelo de Φ tambien es modelo de ψ.

Observación 3.7. Si $\Phi = \{\varphi\}$ consta de una unica formula y φ es otra formula, en lugar de

Definición 3.9. Recordemos que un razonamiento es una formula de tipo

$$\varphi_1 \land \varphi_2 \land \cdots \land \varphi_n$$

Ejemplo 3.6. Estudia si la siguiente implicacion logica es cierta

$$\{p \to q, q \to r, \neg r\} \models \neg p$$

p	q	r	$p \to q$	$q \to r$	$\neg r$	$\neg p$	$\varphi_1 \land \varphi_2 \land \varphi_3$	$(\varphi_1 \land \varphi_2 \land \varphi_3) \to \psi$
0	0	0	1	1	0	1	1	0
0	0	1	1	1	0	1	0	0
0	1	0	1	0	1	1	0	0
0	1	1	1	1	0	1	0	0
1	0	0	0	1	1	0	0	1
1	0	1	0	1	0	0	0	1
1	1	0	1	0	1	0	0	1
1	1	1	1	1	0	0	0	1

ψ es consecuencia logica del compuesto de formulas $\{\varphi_1, \varphi_2, \varphi_3\}$. Contradiccion...

Proposición 3.1. Sean $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ un conjunto de formulas y ψ otra formula. Entonces las siguientes afirmaciones son equivalentes:

- $\Phi \models \psi$
- El razonamiento $\varphi_1 \land \varphi_2 \land \cdots \land \varphi_n \to \psi$ es correcto.
- La formula $\varphi_1 \land \varphi_2 \land \cdots \land \varphi_n \land \neg\psi$ es una contradiccion.

Proof.

Los tres puntos son equivalentes a decir que, para toda valoracion v que cumpla que

$$\varphi_1^v = 1, \varphi_2^v = 1, \ldots, \varphi_n^v = 1$$

Si cumple inversamente que $\psi^v = 1$ ■

Ejemplo 3.7. Estudia si el razonamiento: "Si llueve hace viento. No hace viento a menos que haga frio. No hace frio. Por tanto, no llueve."
formalizado mediante la formula

$$(l \to v) \wedge (\neg f \to \neg v) \wedge \neg f \to \neg l$$

es correcto.
Supongamos que el razonamiento es incorrecto, es decir, que existe una valoracion u que hace ciertas las premisas y falsa la conclusion, es decir,
$(l \to v)^u = 1$ (1), $(\neg f \to \neg v) = 1$ (2), $(\neg f)^u = 1$ (3), $(\neg l)^u = 0$ (4).
(4) $\Rightarrow u(l) = 1 \Rightarrow u(v) = 1 \Rightarrow (\neg v)^u = 0 \Rightarrow (\neg f \Rightarrow \neg v)^u = 0$.
Contradiccion porque $\neg f \to \neg v$ es a la vez verdadera y falsa.
Luego el razonamiento es correcto.

Ejemplo 3.8. Estudia si el razonamiento del ejercicio 14 de la hoja 2:
"Si llueve las calles estaran vacias. Si las calles estan vacias, el comercio obtiene perdidas. Los musicos no podrian sobrevivir si los comerciantes no les contratasen para componer canciones para publicidad. Los comerciantes invierten en canciones publicitarias cuando tienen perdidas. Por tanto, si llueve, los musicos pueden sobrevivir"
formalizado mediante la formula

$$(l \to v) \wedge (v \to p) \wedge (\neg c \to \neg m) \wedge (p \to c) \to (l \to m)$$

es correcto.
$l \to v$ (1), $v \to p$ (2), $\neg c \to \neg m$ (3), $p \to c$ (4)
Conclusion: $l \to m$ (5).
Supongamos que el razonamiento es incorrecto, es decir, existe una valoracion u tal que
$(l \to v) = 1$, $(v \to p) = 1$, $(\neg c \to \neg m) = 1$, $p \to c = 1$, $l \to m = 0 \Rightarrow l = 1, m = 0$
$l = 1 \Rightarrow v = 1(1) \Rightarrow p = 1(2) \Rightarrow c = 1(4)$
Con esta valoracion, $l = 1, m = 0, v = 1, p = 1$ y $c = 1$ se tiene que (3) es verdadera.
Luego esta valoracion es un contraejemplo al razonamiento y, por tanto, el razonamiento es incorrecto.

§3.4 Equivalencia de formulas

Definición 3.10. Sean φ y ψ dos formulas. Decimos que son equivalentes si se cumple simultaneamente:

- $\varphi \models \psi$
- $\psi \models \varphi$

Notacion: $\varphi \equiv \psi$

Proposición 3.2. Sean φ y ψ dos formulas. Las siguientes dos afirmaciones son equivalentes.

- $\varphi \equiv \psi$
- $\varphi \leftrightarrow \psi$ es una tautologia

Proof.

Ambas afirmaciones son equivalentes a que todo modelo de φ tambien lo es de ψ y viceversa. ∎

Proposición 3.3. La relacion $\equiv$ de equivalencia de formulas es una relacion de equivalencia en $\mathcal{F}_0$.

Proof.

1. Reflexiva: $\forall\varphi$, $\varphi = \varphi$?

   Si φ tiene los mismos modelos y los mismos contraejemplos que φ.

2. $\forall\varphi,\psi$ Si $\varphi \equiv \psi \Rightarrow \psi \equiv \varphi$?.

   Si φ y ψ tienen los mismos modelos y contraejemplos $\Rightarrow$ ψ y φ tienen los mismos modelos y contraejemplos.

3. $\forall\varphi,\psi,\alpha$

   $$\left.\begin{aligned}\varphi \equiv \psi\\ \psi \equiv \alpha\end{aligned}\right\} \overset{?}{\Rightarrow} \varphi \equiv \alpha$$

   Si φ,ψ tienen los mismos modelos y contraejemplos y φ,α tienen los mismos modelos y contraejemplos, entonces φ y α tienen los mismos modelos y contraejemplos.

∎

Ejemplo 3.9. Asociatividad de conectivas binarias.

- $(\varphi \leftrightarrow \psi) \leftrightarrow \omega \equiv \varphi \leftrightarrow (\psi \leftrightarrow \omega)$

φ	ψ	ω	$(\varphi \leftrightarrow \psi)$	$(\varphi \leftrightarrow \psi) \leftrightarrow \omega$	$\psi \leftrightarrow \omega$	$\varphi \leftrightarrow (\psi \leftrightarrow \omega)$
0	0	0	1	0	1	0
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	1	0	0	1	0
1	0	0	0	1	1	1
1	0	1	0	0	0	0
1	1	0	1	0	0	0
1	1	1	1	1	1	1

Obs: la implicacion no es conmutativa ni asociativa en general.
Contraejemplos: $p \to q \not\Rrightarrow q \to p$.
Para justificarlo encuentro una valoracion que haga una verdadera y otra falsa.

$$u \begin{cases} p = 1 \\ q = 0 \end{cases} \Rightarrow p \to q = 0, q \to p = 1$$

$p \to (q \to r) \not\equiv (p \to q) \to r$ con la valoracion $u : p = 1, q = 1, r = 0$.

Definición 3.11 — Subformula. Sea φ una formula. Decimos que σ es subformula de φ si σ es una cadena de simbolos consecutivos que aparecen dentro de la formula φ y que es, a su vez, una formula.

Teorema 3.1 — de sustitucion. Sean

- φ una formula
- σ una subformula de φ
- ρ una formula tal que $\varphi \equiv \rho$
- ψ el resultado de sustituir en φ la subformula σ por ρ

Entonces $\varphi \equiv \psi$.

Proof.

Obvio. ■

4 Teoria de la demostracion para logica proposicional

§4.1 Sistemas formales de demostracion

Definición 4.1 — Sistema formal de demostracion. Un sistema formal de demostracion consiste en los siguientes tres elementos:

- Una sintaxis: un alfabeto y un lenguaje definido sobre ese alfabeto que establece cuales son las formulas bien construidas del sistema.
- Un conjunto de axiomas: formulas que se admiten como validas en el sistema sin necesidad de demostracion.
- Un conjunto de reglas de inferencia o reglas de deduccion: permiten demostrar la validez de una formula en el sistema tomando como punto de partida axiomas u otras formulas ya demostradas válidas.

Definición 4.2 — Teorema. Un teorema en un sistema de demostracion formal es una formula valida, en el sentido de que se obtiene de una de estas dos formas:

- Es un axioma del sistema.
- Se obtiene a partir de otros teoremas usando una regla de inferencia.

Notacion: $\vdash \varphi$ ("φ es un teorema").

Definición 4.3 — Razonamiento valido. Un razonamiento valido en un sistema de demostracion formal es una coleccion de formulas formada por un conjunto de premisas y una conclusion φ de manera que la conclusion se puede demostrar a partir de las premisas (como describiremos a continuacion).
Notacion: $\{\varphi_1, \varphi_2, \ldots, \varphi_n\} \vdash \varphi$

Definición 4.4 — Demostracion de un teorema. Una demostracion de un teorema φ

es una sucesion finita de formulas

$$\psi_1, \psi_2, \dots \psi_m, \varphi$$

donde cada formula de la sucesion cumple una de las siguientes afirmaciones:

1. Es un axioma del sistema.
2. Es un teorema ya demostrado en el sistema.
3. Se obtiene a partir de las formulas anteriores de la sucesion usando una regla de inferencia.

Definición 4.5 — Demostracion de un razonamiento. Una demostracion de un razonamiento $\{\varphi_1, \dots, \varphi_n\} \vdash \varphi$ es una sucesion finita de formulas

$$\varphi_1, \dots, \varphi_n, \psi_1, \dots, \psi_m, \varphi$$

donde cada formula de la sucesion cumple:

1. Es una premisa (las n primeras).
2. Es un axioma del sistema.
3. Es un teorema ya demostrado.
4. Se obtiene a partir de las formulas anteriores de la sucesion usando una regla de inferencia.

§4.2 El sistema de Gentzen para la logica proposicional

Definición 4.6 — Sistema de Gentzen. El sistema de Gentzen o sistema de deduccion natural para la logica proposicional viene dado por:

- Sintaxis: la misma que la de la logica proposicional vista en el tema 2, con dos excepciones:
  - No incluimos $\top$ ni $\bot$ en el alfabeto.
  - No consideramos que $\leftrightarrow$ sea una conectiva binaria. La usaremos como una abreviatura:

    $\varphi \leftrightarrow \psi$ se considera una abreviatura de $(\varphi \to \psi) \wedge (\psi \to \varphi)$
- El conjunto de axiomas es vacio.
- Hay 8 reglas de inferencia que describiremos a continuacion. Sus nombres son:

$E\neg$	$I\neg$
$E\wedge$	$I\wedge$
$E\vee$	$I\vee$
$E\rightarrow$	$I\rightarrow$

En lo que sigue denotaremos con A, B, C a formulas cualesquiera de la logica proposicional.

Definición 4.7 — Regla de eliminacion de la negacion, $E\neg$.

$$\frac{\neg\neg A}{A}$$

Definición 4.8 — Regla de introduccion de la conjuncion, $I\wedge$.

$$\frac{\begin{array}{c}A\\B\end{array}}{A\wedge B}$$

Definición 4.9 — Regla de eliminacion de la conjuncion, $E\wedge$. Son, en realidad, dos reglas que llamaremos con el mismo nombre:

$$\frac{A\wedge B}{A} \qquad \frac{A\wedge B}{B}$$

Definición 4.10 — Regla de introduccion de la disyuncion, $I\vee$. Tambien son dos reglas que llamaremos con el mismo nombre:

$$\frac{A}{A\vee B} \qquad \frac{B}{A\vee B}$$

Definición 4.11 — Regla de eliminacion de la implicacion, $E\rightarrow$. Tambien recibe el nombre de modus ponens.

$$\frac{\begin{array}{c}A\\A\rightarrow B\end{array}}{B}$$

Ejemplo 4.1. Demostrar la validez de $\{p, p \to q\} \vdash p \wedge q$.

1. p Premisa
2. $p \to q$ Premisa
3. $q \quad E \to, 1, 2$
4. $p \wedge q \quad I\wedge, 1, 3$

Ejemplo 4.2. Demostrar la validez de $\{p \wedge q \to r, q \to p, q\} \vdash r$.

1. $p \wedge q \to r$ Premisa
2. $q \to p$ Premisa
3. q Premisa
4. $p \quad E \to, 2, 3$
5. $p \wedge q \quad I\wedge, 3, 4$
6. $r \quad E \to, 1, 5$

Ejemplo 4.3. Demostrar la validez de $\{\neg\neg p, p \to q \wedge \neg\neg r, \neg p \vee q \to s\} \vdash s \wedge r$

1. $\neg\neg p$ Premisa
2. $p \to q \wedge \neg\neg r$ Premisa
3. $\neg p \vee q \to s$ Premisa
4. $p \quad E\neg, 1$
5. $q \wedge \neg\neg r \quad E \to, 4, 2$
6. $q \quad E\wedge, 5$
7. $\neg p \vee q \quad I\vee, 6$
8. $s \quad E \to, 7, 3$
9. $\neg\neg r \quad E\wedge, 5$
10. $r \quad E\neg, 9$
11. $s \wedge r \quad I\wedge, 8, 10$

Definición 4.12 — Regla de introduccion de la implicacion, $I \to$.

donde la “caja” es una demostracion auxiliar cuya primera linea es A, que se supone temporalmente valida como premisa auxiliar y cuya ultima linea es B.

Observación 4.1. Las lineas dentro de la “caja” solo son validas bajo la suposicion temporal de la validez de A, en el contexto de la demostracion auxiliar. No son validas en la demostracion principal.

Ejemplo 4.4. Demostrar la validez de $\{p \to q, p \to r\} \vdash p \to q \wedge r$.

1. $p \to q$ Premisa
2. $p \to r$ Premisa

3. p Pr aux
4. $q \quad E \to, 1, 3$
5. $r \quad E \to, 2, 3$
6. $q \wedge r \quad I\wedge, 4, 5$

7. $p \to q \wedge r \quad I \to (3-6)$

Definición 4.13 — Regla de introduccion de la negacion, $I\neg$.

$$\frac{A \to B \wedge \neg B}{\neg A}$$

Observación 4.2. El uso tipico de la regla $I\neg$ es para demostraciones que modelan la reduccion al absurdo. Si quiero demostrar A, supongo $\neg A$ como premisa auxiliar de una demostracion auxiliar en la que trato de llegar como conclusion a $B \wedge \neg B$ para una formula cualquiera B. A partir de ahi, deduzco A:

$\neg A$	Premisa auxiliar
$\vdots$	
$B \wedge \neg B$	
$\neg A \to B \wedge \neg B$	I $\to$
$\neg\neg A$	I$\neg$
A	E$\neg$

Ejemplo 4.5. Demostrar la validez de $\{p \to q, q \to r, \neg r\} \vdash \neg p$.

Definición 4.14 — Regla de eliminacion de la disyuncion, $E\vee$.

$$\begin{array}{c} A \vee B \\ A \to C \\ B \to C \\ \hline C \end{array}$$

Observación 4.3. El uso tipico de la regla $E\vee$ es para demostraciones que modelan el uso de la tecnica de la demostracion por casos. Si quiero demostrar C y tengo como hipotesis $A \vee B$, primero supongo A como premisa auxiliar de una demostracion auxiliar en la que trato de llegar como conclusion a C. A continuacion hago lo mismo suponiendo B como premisa auxiliar.

Ejemplo 4.6. Demostrar la validez de $\{p \to q, q \to s, p \vee q\} \vdash r \vee s$

Ejemplo 4.7. Demostrar la validez de $\{p \to (q \to r)\} \vdash q \to (p \to r)$.

§4.3 Teorema de la deduccion

Ejemplo 4.8. Demostrar la validez de $\{p \to r \wedge s, r \to q\} \vdash p \to q \wedge s$.

Ejemplo 4.9. Demostrar la validez de $\{p \to r \wedge s, r \to q, p\} \vdash q \wedge s$.

Teorema 4.1 — de la deduccion. Sean $n \geq 1$ y $\varphi_1, \varphi_2, \ldots, \varphi_n, \varphi$ una coleccion de formulas. Entonces

$$\{\varphi_1, \varphi_2, \ldots, \varphi_n\} \vdash \varphi$$

si y solo si

$$\{\varphi_1, \varphi_2, \ldots, \varphi_{n-1}\} \vdash \varphi_n \to \varphi$$

Proof.

$\Rightarrow$) Si tengo una demostracion

$$\begin{array}{c} \varphi_1 \\ \vdots \\ \varphi_n \\ \alpha_1 \\ \vdots \\ \alpha_m \\ \varphi \end{array} \Rightarrow \begin{array}{c} \varphi_1 \\ \vdots \\ \varphi_{n-1} \\ \varphi_n \text{ Pr aux} \\ \alpha_1 \\ \vdots \\ \alpha_m \\ \varphi \\ \varphi_n \to \varphi \\ \text{Demostracion del 2} \end{array}$$

$\Leftarrow$)

$$\begin{array}{c} \varphi_1 \\ \vdots \\ \varphi_{n-1} \\ \beta \\ \vdots \\ \beta_m \\ \varphi_n \to \varphi \end{array} \Rightarrow \begin{array}{c} \varphi_1 \\ \vdots \\ \varphi_{n-1} \\ \varphi_n \\ \beta_1 \\ \vdots \\ \beta_m \\ \varphi_n \to \varphi \\ \varphi E \to a, b \end{array}$$

■

Observación 4.4. No se puede demostrar que un razonamiento es incorrecto con Gentzen.

Observación 4.5. El teorema de la deduccion permite transformar cualquier razonamiento valido del sistema de Gentzen en un teorema de ese sistema. Por ejemplo, si

$$\{\varphi_1, \varphi_2\} \vdash \varphi$$

es un razonamiento valido, entonces

$$\vdash \varphi_1 \to (\varphi_2 \to \varphi)$$

es un teorema.

§4.4 Reglas derivadas en el sistema de Gentzen

Teorema 4.2 — Modus tollens, MT. $\{A \to B, \neg B\} \vdash \neg A$

Proof.

A, B formulas cualesquiera.
Cons: $\neg A$

1. $A \to B$ Pr
2. $\neg B$ Pr

3. A Pr aux
4. $B \quad E \to 3, 1$
5. $B \wedge \neg \quad I \wedge 4, 2$

6. $A \to B \wedge \neg B \quad I \to (3-5)$
7. $\neg A \quad I\neg, 6$

■

Teorema 4.3 — Teorema de la identidad, TI.

$$\{A\} \vdash A$$

Usando el Teorema de deduccion puede reformularse como

$$\vdash A \to A$$

Proof.

1. A Pr

2. $\neg A$ Pr aux
3. $A \wedge \neg A \quad I\wedge, 2, 1$

4. $\neg A \to A \wedge \neg A \quad I \to (2-3)$
5. $\neg\neg A \quad I\neg, 4$
6. $A \quad E\neg, 5$

■

Teorema 4.4 — Excontradictione quodlibet, EQ.

$$\{A \wedge \neg A\} \vdash B$$

Proof.

1. $A \wedge \neg A$ Pr

2. $\neg B$ Pr aux
3. $A \wedge \neg A$

4. $\neg B \to A \wedge \neg A \quad I \to (2, -3)$
5. $\neg\neg B \quad I\neg, 4$
6. B

■

Teorema 4.5 — Tollendo ponens, TP.

$$\{A \vee B, \neg A\} \vdash B$$

Proof.

1. $A \vee B$ Pr
2. $\neg A$ Pr

3. A Pr aux
4. $A \wedge \neg A \quad I\wedge, 1, 2$
5. $B \quad EQ, 4$

6. $A \to B \quad I \to (3-6)$

7. B Pr aux

8. $B \to B \quad I \to (7)$
9. $B \quad E\vee, 1, 6, 8$

■

Ejemplo 4.10. Uso de reglas derivadas en una demostracion:

$$\{p \to t \vee r, p \vee q, q \to t, \neg t \wedge s\} \vdash r \wedge s$$

Cons: $r \wedge s$

1. $p \to t \vee r$ Pr
2. $p \vee q$ Pr
3. $q \to t$ Pr
4. $\neg t \wedge s$ Pr
5. $\neg t \quad E\wedge, 4$
6. $\neg q \quad MT, 5, 3$
7. $p \quad TP, 6, 2$
8. $t \vee r \quad E \to, 7, 1$
9. $r \quad TP, 8, 5$
10. $s \quad E\wedge, 4$
11. $r \wedge s \quad I\wedge, 9, 10$

Teorema 4.6 — Doble negacion, DN.

$$\{A\} \vdash \neg\neg A$$

Teorema 4.7 — Contraposicion, CP. Son dos reglas que establecen la "equivalencia" entre dos formulas en este sistema formal.

$$\{A \to B\} \vdash \neg B \to \neg A$$

$$\{\neg B \to \neg A\} \vdash A \to B$$

Proof.

1. $A \to B$ Pr

2. $\neg B$ Pr aux 3. $\neg A \quad MT, 1, 2$

4. $\neg B \to \neg A \quad I \to (2-3)$

1. $\neg B \to \neg A$

2.

■

Teorema 4.8 — Leyes de De Morgan, DM. Cuatro reglas:

$$\{\neg(A \vee B)\} \vdash \neg A \wedge \neg B$$

$$\{\neg A \wedge \neg B\} \vdash \neg(A \vee B)$$

$$\{\neg(A \wedge B)\} \vdash \neg A \vee \neg B$$

$$\{\neg A \vee \neg B\} \vdash \neg(A \wedge B)$$

Proof.

DM1:

1. $\neg(A \vee B)$ Pr

2. A Pr aux
3. $A \vee B \quad I\vee, 2$
4. $(A \vee B) \wedge \neg(A \vee B) \quad I\wedge, 1, 3$

5. $A \rightarrow (A \vee B) \wedge \neg(A \vee B) \quad I \rightarrow (2-4)$
6. $\neg A \quad I\neg, 5$

6. B Pr aux
7. $A \vee B \quad I\vee, 6$
8. $(A \vee B) \wedge \neg(A \vee B) \quad I\wedge, 1, 7$

9. $\neg BI \rightarrow, I\neg(6-8)$
10. $\neg A \wedge \neg B \quad I\wedge, 5, 9$

DM2:

1. $\neg A \wedge \neg B$ Pr

2. $A \vee B$ Pr aux
3. $\neg A \quad E\wedge, 1$
4. $B \quad TP, 2, 3$
5. $\neg B \quad E\wedge, 1$
6. $B \wedge \neg B \quad I\wedge, 4, 5$

7. $\neg(A \vee B) \quad I \rightarrow, I\neg(2-6)$

DM3:

1. $\neg(A \wedge B)$ Pr

2. $\neg(\neg A \vee \neg B)$ Pr aux
3. $\neg\neg A \wedge \neg\neg B \quad DM, 1, 2$
4.
4. $\neg\neg A \quad E\wedge, 3$
5. $A \quad E\neg, 4$
6. $\neg\neg B \quad E\wedge, 3$
7. $B \quad E\neg, 6$
8. $A \wedge B \quad I\wedge, 5, 7$
9. $(A \wedge B) \wedge \neg(A \wedge B) \quad I\wedge, 1, 8$

10. $\neg A \vee \neg B \quad I \rightarrow, I\neg, E\neg(2-9)$

DM4:

1. $\neg A \vee \neg B$ Pr

2. $A \wedge B$ Pr aux
3. $A \quad E\wedge, 2$
4. $\neg B \quad TP, 3, 1$
5. $B \quad E\wedge, 2$
6. $B \wedge \neg B \quad I\wedge, 5, 4$

7. $\neg(A \wedge B) \quad I \rightarrow, I\neg(2-6)$

■

Teorema 4.9 — Interdefinicion. Cuatro reglas:

$$\{A \rightarrow B\} \vdash \neg A \vee B$$

§4.5 Correccion, completitud y decidibilidad

Definición 4.15. Todo sistema de demostracino formal se puede ver como un modelo formal de cierto ambito (usualmente formado por objetos matematicos).
Decimos que un sistema formal es

- Correcto si todo teorema del sistema formal es una afirmacion verdadera en el ambito que se esta modelando.
- Completo si toda afirmacion verdadera en el ambito que se esta modelando es un teorema del sistema formal.
- Decidible si existe un procedimiento algoritmico finito para determinar si una formula es un teorema del sistema formal.

Ejemplo 4.11. El sistema formal de Gentzen es un modelo formal de la logica proposicional, vista en el Tema 3 (sin incluir los simbolos $\top$ y $\bot$).

Teorema 4.10. El sistema de Gentzen es correcto: todo teorema del sistema de Gentzen es una tautologia de la logica proposicional.

Proof.

No la hacemos con detalle. Es facil: se debe, basicamente, a que todas las 8 reglas de inferencia son razonamientos validos en logica proposicional. ■

Teorema 4.11. El sistema de Gentzen es completo: toda tautologia de la logica proposicional es un teorema del sistema de Gentzen.

Proof.

No la hacemos. ■

Teorema 4.12. El sistema de Gentzen es decidible.

Ejemplo 4.12. El sistema formado por la sintaxis de la logica proposicional, sin axiomas y con las reglas de inferencia:

- $I\neg, E\neg, I\wedge, E\wedge, I\vee, I\rightarrow, E\rightarrow$

- $E\vee' : \{A \vee B\} \vdash A, \{A \vee B\} \vdash B$

no es correcto.

Ejemplo 4.13. El sistema formado por la sintaxis de la logica proposicional, sin axiomas y con las reglas de inferencia:

- $I\neg, E\neg, I\wedge, E\wedge, I\vee, I \rightarrow, E \rightarrow$

no es completo.

Ejemplo 4.14. Asumamos que ya sabemos que el sistema de Gentzen es correcto y completo. Demostrar que el siguiente sistema es completo:
El sistema formado por la sintaxis de la logica proposicional, sin axiomas y con las reglas de inferencia:

- $I\neg, E\neg, I\wedge, E\wedge, I\vee, I \rightarrow, E \rightarrow$
- $TP : \{A \vee B, \neg B\} \vdash A, \{A \vee B, \neg A\} \vdash B.$

Obs: el sistema de con las 7 reglas y TP es correcto. Si fuera incorrecto, podria demostrar un teorema que no fuera tautologia usando esas reglas, pero como TP es demostrar en Gentzen, eso implicaria que Gentzen es incorrecto.
Tenemos que ver que el sistema propuesto es completo. Para ello, basta con ver que $E\vee$ se puede demostrar en este sistema y luego usar que Gentzen es completo.
En el sistema nuevo:

1. $A \rightarrow C$ Pr
2. $B \rightarrow C$ Pr
3. $A \vee B$ Pr

> 4. $\neg C$ Pr aux
> 5. $\neg A \quad MT4,1$ (MT es valido en el sistema nuevo)
> 6. $B \quad TP, 3, 5$
> 7. $C \quad E \rightarrow, 6, 2$
> 8. $C \wedge \neg C \quad I\wedge, 4, 7$

9. $\neg C \rightarrow C \wedge \neg C \quad I \rightarrow (4-8)$
10. $\neg\neg C \quad I\neg, 9$
11. $C \quad E\neg, 10$

5 Sintaxis de la logica de predicados

§5.1 Introduccion intuitiva a la formalizacion

IDEA: Ampliar la logica proposicional para poder formalizar (y demostrar la correccion) de razonamientos del tipo:
"Socrates es humano. Todo humano es mortal. Por tanto, Socrates es mortal."
Formalizacion con proposicional: $p \wedge q \to r$ que no es un razonamiento correcto.
Con logica de predicados:
Dominio:

- $D = \{\text{humanos y dioses de la antiguedad griega}\}$

Simbolos:

- s : Socrates (s es una constante).
- $H(x)$: x es humano (H es un simbolo de predicado de aridad 1).
- $M(x)$: x es mortal (M es un simbolo de predicado de aridad 1)

Formalizacion:

$$\begin{array}{l} H(s) \\ \forall x(H(x) \to M(x)) \\ \hline M(s) \end{array}$$

Ejemplo 5.1. Vamos a formalizar las sigueintes frases con logica de predicados en el dominio formado por las personas.
Dominio: $D = \{\text{personas}\}$
Simbolos:

- a: Antonio (a es una constante).
- b: Barbara (b es una constante).
- $M(x)$: x es moreno (M es un simbolo de predicado de aridad 1).
- $R(x)$: x es rubio (R es un simbolo de predicado de aridad 1).

Formalizaciones:

- $M(a)$: Antonio es moreno.
- $R(b)$: Barbara es rubia.
- $\forall x M(x)$

- $\exists x R(x)$

Simbolos:

- $S(x)$: x es sevillano (S es un simbolo de predicado de aridad 1).
- $T(x)$: x es toledano (T es un simbolo de predicado de aridad 1).
- $m(x)$: la madre de x (m es un simbolo de predicado de aridad 1).

Formalizaciones:

- Todos los sevillanos son morenos: $\forall x(S(x) \to M(x))$
- Hay toledanos rubios: $\exists x(T(x) \land R(x))$
- La madre de Antonio es rubia: $R(m(a))$
- Barbara es la madre de Antonio: $b = m(a)$.

Simbolos:

- $A(x, y)$: x es mas alto que y (A es un simbolo de pred. de aridad 2)

Formalizaciones:

- Antonio es mas alto que Barbara: $A(a, b)$
- Todo el mundo es mas alto que Barbara: $\forall x A(x, b)$
- Hay gente rubia mas alta que la madre de Antonio: $\exists x(R(x) \land A(x, m(a)))$

§5.2 Alfabeto y reglas de formacion de formulas

Definición 5.1 — Alfabeto de la logica de predicados. $A := \{p_1, p_2, p_3, \ldots\} \cup \{\top, \bot, \neg, \lor, \land, \to, \leftrightarrow, (,)\} \cup \{c_1, c_2, \ldots\} \cup \{P_1, P_2, \ldots\} \cup \{x_1, x_2, \ldots\} \cup \{=\} \cup \{, \}$.

Nombre	Símbolo	Tipo	Aridad
Constante	c_i	Función	0
Función de aridad $n \geq 1$	f_i		$n \geq 1$
Proposición atómica	p_i	Predicado	0
Predicado de aridad $n \geq 1$	P_i		$n \geq 1$
Variable	x_i	Variable	-

Nombre	Símbolo	Tipo	Aridad
Verdadero	$\top$	Conectiva	0
Falso	$\bot$		
Negación	$\neg$		1
Conjunción	$\wedge$		2
Disyunción	$\vee$		
Implicación	$\rightarrow$		
Doble implicación	$\leftrightarrow$		
Igualdad	$=$	Igualdad	2
Para todo	$\forall$	Cuantificador	-
Existe	$\exists$		
Paréntesis izquierdo	(	Auxiliar	-
Paréntesis derecho	)		
Coma	,		

Vamos a definir de manera recursiva dos lenguajes sobre A:

- El conjunto $\mathcal{T}$ de los terminos de la logica de predicados (que representaran elementos del dominio).
- El conjunto $\mathcal{F}_1$ de las formulas de la logica de predicados (que representaran enunciados).

Definición 5.2 — Recursiva de termino.

1. Terminos atomicos:
   - Si c es un simbolo constante $\Rightarrow$ c es un termino.
   - Si x es un simbolo de variable $\Rightarrow$ x es un termino.
2. Si f es un simbolo de funcion de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos entonces $f(t_1, t_2, \ldots, t_n)$ es un termino.
3. Cualquier palabra que no se pueda obtener con la aplicacion de las reglas anteriores no es un termino.

Definición 5.3 — Recursiva de formula de la logica de primer orden.

1. Formulas atomicas:
   - Si p es un simbolo de proposicion atomica $\Rightarrow$ p es una formula.
   - $\top$ es una formula.
   - $\bot$ es una formula.
   - Si P es un simbolo de predicado de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos, entonces $P(t_1, t_2, \ldots, t_n$ es una formula.
   - Si t_1, t_2 son terminos, entonces $(t_1 = t_2)$ es una formula.

2. Si φ es una formula $\Rightarrow \neg\varphi$ es una formula.

3. Si φ, ψ son formulas y $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ entonces $(\varphi \circ \psi)$ es una formula.

4. Si x es un simbolo de variable y φ es una formula, entonces:
   - $\forall x\varphi$ es una formula.
   - $\exists x\varphi$ es una formula.

5. Cualquier palabra que no se pueda obtener con la aplicacion de las reglas anteriores no esu na formula.

Observación 5.1. Se aplican los mismos criterios para abreviar formulas mediante eliminacion de parentesis que vimos en logica proposicional.

§5.3 Arbol estructural, recursion, induccion

Observación 5.2.

Ejemplo 5.2. Dibujar el arbol estructural de la formula:

$$\forall x(P(a, f(x)) \wedge Q(f(a))) \rightarrow (p \vee P(g(b, y), a) \leftrightarrow \exists y(Q(y) \wedge (g(a, a) = x)))$$

Ejemplo 5.3. Recursion. Definir por recursion una fubcion que, dada una formula cualquiera de la logica de predicados, devuelva el numero de conectivas que aparecen en la formula.

$$\begin{aligned} f\colon \mathcal{F}_1 &\longrightarrow \mathbb{N} \cup \{0\} \\ \varphi &\longmapsto f(\varphi) = \text{ num conectivas} \end{aligned}$$

1. Para formulas atomicas, $f(\top) = 1$, $f(\bot) = 1$. Si p es un simbolo de proposicion atomica, $f(p) = 0$. $f(P(t_1, \dots, t_n)) = 0$, $f(t_1 = b_1) = 0$

   Alternativamente si φ es atomica,

   $$f(\varphi) = \begin{cases} 1 \text{ si } \varphi = \top, \bot \\ 0 \text{ en el resto de casos} \end{cases}$$

2. Si $\varphi \in \mathcal{F}_1$, entonces $f(\neg\varphi) = f(\varphi) + 1$.

3. Si $\varphi, \psi \in \mathcal{F}_1 \Rightarrow f((\varphi \circ \psi)) = f(\varphi) + f(\psi) + 1$

4. $f(\forall x\varphi) = f(\varphi)$

5. $f(\exists x\varphi) = f(\varphi)$

Ejemplo 5.4. Definir por recursion una funcion que, dada una formula cualquiera de la logica de predicados, devuelva el numero de simbolos no auxiliares que aparecen en esa formula.

$$\begin{aligned} f\colon \mathcal{F}_1 &\longrightarrow \mathbb{N} \\ \varphi &\longmapsto f(\varphi) = \text{num simbolos no aux} \end{aligned}$$

1. Si φ es atomica,

   $f(\top) = 1$

   $f(\bot) = 1$

   p simb de prop atomica $\Rightarrow f(p) = 1$

   Sea P es un pred. de aridad n con $t_1, \ldots, t_n$ terminos.

   Necesito una funcion nueva que cuente el numero de simbolos no auxiliares de un termino, que vamos a definir tambien por recursion.

   $$\begin{aligned} g\colon \mathcal{T} &\longrightarrow \mathbb{N} \\ t &\longmapsto g(t) = \text{ num simbolos no aux} \end{aligned}$$

   a) Si t es termino atomico, $g(t) = 1$.

   b) Terminos compuestos:

      Sea h un simbolo de funcion de aridad n y $t_1, \ldots, t_n$ terminos: $g(h(t_1, \ldots, t_n)) = g(t_1) + g(t_2) + \cdots + g(t_n) + 1$

   Luego $f(P(t_1, t_2, \ldots, t_n)) = g(t_1) + g(t_2) + \cdots + g(t_n) + 1$

   Si t_1, t_2 son terminos, $f((t_1 = t_2)) = g(t_1) + g(t_2) + 1$

2. Sea $\varphi \in \mathcal{F}_1 \Rightarrow f(\neg\varphi) = f(\varphi) + 1$

3. Sea $\varphi, \psi \in \mathcal{F}_1 \Rightarrow f((\varphi \circ \psi)) = f(\varphi) + f(\psi) + 1$

4. Sea $\varphi \in \mathcal{F}_1$

   $f(\forall x\varphi) = f(\varphi) + 2$ $f(\exists x\varphi) = f(\varphi) + 2$

§5.4 Variables libres y variables ligadas

Definición 5.4. Sea x un simbolo de variable que aparece en una formula φ.

- Decimos que una aparicion de x en φ es ligada si esta afectada por un cuantificador. En particular la aparicion de una variable justo despues de un cuantificador se considera ligada.
- Decimos que una aparicion de x en φ es libre si no es ligada.
- Decimos que una variable x es libre en la formula φ si tiene alguna aparicion libre.

- Decimos que una variable x es ligada en la formula φ si no es libre, es decir, si todas sus apariciones son ligadas.

Definición 5.5. Sea φ una formula. Decimos que es:

- Abierta si hay alguna variable que aparece libre en φ.
- Cerrada si no es abierta, es decir, si todas las variables que aparezcan en φ son ligadas.

Ejemplo 5.5.

- $\forall x(P(x) \to Q(x)) \land R(x)$

  Las 3 primeras apariciones de x son ligadas. La cuarta es libre. La formula es abierta.
- $\forall x(P(x) \to Q(x) \land R(x))$

  Las 4 apariciones de x son ligadas. La formula es cerrada.
- $\exists x(P(x) \land Q(y)) \lor \forall y(P(y) \to Q(x))$

  Las 2 primeras apariciones de x son ligadas. La tercera es libre. La primera aparicion de y es libre. Las 2 ultimas son ligadas. La formula es abierta.
- $\exists x \forall y((P(x) \land Q(y)) \lor (P(y) \to Q(x)))$

  Todas las apariciones de x e y son ligadas. La formula es cerrada.

Observación 5.3. Estamos interesados, sobre todo, en formulas cerradas. Siempre usaremos formulas cerradas para formalizar enunciados. Las formulas abiertas aparecen porque son necesarias como pasos intermedios para poder dar la definicion recursiva de formula.

Ejemplo 5.6. Definir por recursion una funcion que, dada una formula cualquiera de la logica de predicados, devuelva el conjunto formado por todas las variables libres de la formula.
Empezamos definiendo una funcion que devuelva las variables de un termino.

$$\begin{aligned} var\colon \mathcal{T} &\longrightarrow \mathcal{P}(V) \\ t &\longmapsto \text{conjunto de variables de t} \end{aligned}$$

donde $V = \{x \mid x \text{ es un simbolo de variable}\}$.

1. Terminos atomicos:

   Si c es simbolo de constante: $var(c) = \varnothing$.

Si x es simbolo de variable: $var(x) = \{x\}$.

2. Terminos compuestos:

   Si f es un simbolo de funcion de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos, $var(f(t_1, t_2, \ldots, t_n)) = \bigcup_{i=1}^{n} var(t_i)$.

Ahora definimos

$$\begin{aligned} lib\colon \mathcal{F}_1 &\longrightarrow \mathcal{P}(V) \\ \varphi &\longmapsto \text{cjto de variables libres de } \varphi \end{aligned}$$

3. Formulas atomicas:

   $lib(\top) = lib(\bot) = lib(p) = \varnothing$ donde p es simbolo de proposicion atomica.

   Si P es un simbolo de predicado de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos: $lib(P(t_1, t_2, \ldots, t_n)) = \bigcup_{i=1}^{n} var(t_i)$

   $lib((t_1 = t_2)) = lib(t_1) \cup lib(t_2)$

4. Negacion:

   Si $\varphi \in \mathcal{F}_1 \Rightarrow lib(\neg\varphi) = lib(\varphi)$

5. Conectiva binaria:

   Dados $\varphi, \psi \in \mathcal{F}_1 \Rightarrow lib((\varphi \circ \psi)) = lib(\varphi) \cup lib(\psi)$

6. Cuantificadores:

   Sea φ una formula y x un simbolo de variable:

   $lib(\forall x\varphi) = lib(\varphi) \setminus \{x\}$

   $lib(\exists x\varphi) = lib(\varphi) \setminus \{x\}$

Ejemplo 5.7. Definir por recursion una funcion que, dada una formula cualquiera de la logica de predicados, devuelva el conjunto formado por todas las variables ligadas de la formula.

$$\begin{aligned} lig\colon \mathcal{F}_1 &\longrightarrow \mathcal{P}(V) \\ \varphi &\longmapsto \text{conjunto de las variables ligadas de } \varphi \end{aligned}$$

1. Formulas atomicas:

   Si φ es atomica $\Rightarrow lib(\varphi) = \varnothing$

2. Negacion:

   $\varphi \in \mathcal{F}_1 \Rightarrow lig(\neg\varphi) = lig(\varphi)$

3. Conectiva binaria:

   $\varphi, \psi \in \mathcal{F}_1 \Rightarrow lig((\varphi \circ \psi)) = (lig(\varphi) \cup lig(\psi)) \setminus (lib(\varphi) \cup lib(\psi))$

4. Cuantificadores:

   $\varphi \in \mathcal{F}_1, x$ variable.

   $lig(\forall x\varphi) = lig(\exists x\varphi) = lig(\varphi) \cup \{x\}$

6 Semantica de la logica de predicados

§6.1 Evaluacion semantica de formulas (valores de verdad)

Objetivo de la seccion: Definir por recursion el valor de verdad de una formula, que podra ser

- $0 =$ "falso" o bien
- $1 =$ "verdadero".

Definición 6.1 — Signatura. Llamamos signatura al conjunto Σ formado por todos los simbolos de funcion y predicado (incluyendo los de constante y proposicion atomica).

Definición 6.2 — Interpretacion. Sea Σ una signatura. Llamamos interpretacion definida sobre Σ a un par (D, I) donde:

- D es un conjunto no vacio, llamado el dominio de la interpretacion.
- I es la funcion interpretacion que asocia a cada elemento de Σ un objeto matematico como se describe a continuacion:
  - A cada simbolo de constante $c \mapsto$ un elemento del dominio $c' \in D$.
  - A cada simbolo de funcion f de aridad $n \geq 1 \mapsto$ una funcion $f' : D^n \to D$.
  - A cada simbolo de predicado P de aridad $n \geq 1 \mapsto$ una relacion n-aria $P' \subseteq D^n$.

Observación 6.1. En la definicion anterior la relacion P' describe el conjunto de n-tuplas de D'' que "cumplen" el predicado P en la interpretacion dada.

Definición 6.3. Dado el conjunto de simbolos de variable, llamamos asignacion a una funcion A que asocia:

- A cada simbolo de variable $x \mapsto$ un elemento del dominio $x^A \in D$.

Observación 6.2. Normalmente, para evaluar una formula, solo asignaremos el conjunto finito de variables que aparezcan en la formula.
...

A continuacion, fijadas una interpretacion y una asignacion, vamos a asociar, de forma recursiva, a cada termino un elemento del dominio de la interpretacion.

Definición 6.4 — Definicion recursiva de la evaluacion de un termino. Sean Σ una signatura, (D, I) una interpretacion definida sobre Σ y A una asignacion.
Vamos a asociar, de forma recursiva, a cada termino t un elemento del dominio $t^{I,A} \in D$.

- Si c es un simbolo de constante $\Rightarrow (c)^{I,A} := c^I$
- Si x es un simbolo de variable $\Rightarrow (x)^{I,A} := x^A$
- Si f es un simbolo de funcion de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos $\Rightarrow$ $(f(t_1, t_2, \ldots, t_n))^{I,A} := f^I(t_1^{I,A}, t_2^{I,A}, \ldots, t_n^{I,A})$.

Sean D un conjunto no vacio, $d \in D$, A una asignacion y x un simbolo de variable. Se define una nueva asignacion, que se denota $A[x/d]$, como la asignacion que asocia a todas las variables el mismo elemento de D que les asignaba A, salvo al simbolo x al que se asigna el valor d.
A continuacion, fijadas una interpretacion y una asignacion, vamos a asociar, de forma recursiva, a cada formula un valor de verdad.

Definición 6.5 — Definicion recursiva de la evaluacion de una formula. Sean Σ una signatura, (D, I) una interpretacion definida sobre Σ y A una asignacion.
Vamos a asociar, de forma recursiva, a cada formula φ un valor de verdad $\varphi^{I,A} \in \{0, 1\}$

- $(\top)^{I,A} := 1$
- $(\bot)^{I,A} := 0$
- Si p es un simbolo de proposicion atomica $\Rightarrow (p)^{I,A} := p^I$
- Si P es un simbolo de predicado de aridad $n \geq 1$ y $t_1, t_2, \ldots, t_n$ son terminos $\Rightarrow$

$$(P(t_1, t_2, \ldots, t_n))^{I,A} := \begin{cases} 1 \text{ si } (t_1^{I,A}, t_2^{I,A}, \ldots, t_n^{I,A}) \in P^I \\ 0 \text{ en caso contrario} \end{cases}$$

- Si t_1, t_2 son terminos $\Rightarrow$

$$((t_1 = t_2))^{I,A} = \begin{cases} 1 \text{ si } t_1^{I,A} = t_2^{I,A} \\ 0 \text{ en caso contrario} \end{cases}$$

- Si φ es una formula $(\varphi)^{I,A}$ se define como en proposicional: ...
- Si φ, ψ son formulas ...

- Si φ es una formula y x es simbolo de variable $\Rightarrow$

$$(\forall x\varphi)^{I,A} := \begin{cases} 1 \text{ si } \varphi^{I,A[x/d]} = 1 \text{ para todos los elementos } d \in D \\ 0 \text{ en caso contrario} \end{cases}$$

$$(\exists x\varphi)^{I,A} := \begin{cases} 1 \text{ si } \varphi^{I,A[x/d]} = 1 \text{ para algun elemento } d \in D \\ 0 \text{ en caso contrario} \end{cases}$$

Observación 6.3. La nocion intuitiva que hay tras la definicion de la evaluacion de los cuantificadores es:

- $\forall x\varphi$ es verdadera si y solo si φ es verdadera cuando x toma todos los valores posibles de D.

  (Para justificarlo hace falta un argumento general).

- $\forall x\varphi$ es falsa si y solo si se encuentra un valor del dominio para x que hace que φ sea falsa.

  (Para justificarlo es suficiente un contraejemplo).

- $\exists x\varphi$ es verdadera si y solo si se encuentra un valor del dominio para x que hace que φ sea verdadera.

  (Para justificarlo es suficiente un ejemplo).

- $\exists x\varphi$ es falsa si y solo si φ es falsa cuando x toma todos los valores posibles de D.

  (Para justificarlo hace falta un argumento general).

§6.2 Modelos. Clasificacion de formulas.

Definición 6.6. Sea φ una formula. Decimos que φ es

- satisfacible bajo una interpretacion (D, I) si $\varphi^{I,A} = 1$ para alguna asignacion A.
- satisfacible si es satisfacible bajo una interpretacion.
- insatisfacible o contradiccion si no es satisfacible.
- verdadera bajo una interpretacion (D, I) si $\varphi^{I,A} = 1$ para toda asignacion A.

  En ese caso decimos que (D, I) es modelo de φ y escribimos $(D, I) \vDash \varphi$.
- valida o tautologia si es verdadera bajo toda interpretacion. Escribimos $\vDash \varphi$.
- falsificable si no es tautologia.

Observación 6.4. Si φ es cerrada, el valor de verdad $\varphi^{I,A}$ no depende de la asignacion A. Lo denotaremmos simplemente φ^{I}.
Ademas las definiciones anteriores son mas sencillas y parecidas a las de logica proposicional para formulas cerradas. Decimos que φ es:

1. verdadera bajo una interpretacion (D, I) si $\varphi^{I} = 1$.

   En ese caso decimos que (D, I) es modelo de φ y escribimos

§6.3 Consecuencia logica

Definición 6.7. Sean $\phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ un conjunto de formulas y ψ otra formula. Decimos que ψ es consecuencia logica de ϕ si para toda interpretacion (D, I) y para toda asignacion A se cumple:

$$(\forall i \exists \{1, \ldots, n\} \varphi_i^{I,A} = 1) \Rightarrow \psi^{I,A} = 1$$

Tambien decimos que ϕ implica logicamente a ψ.
Notacion: $\phi \vDash \psi$

Definición 6.8. Recordemos que un razonamiento es una formula de tipo

$$\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n \to \psi.$$

Decimos que el razonamiento anterior es correcto si es una tautologia o formula valida.

Proposición 6.1. Sean $\phi = \{\varphi_1, \ldots, \varphi_n\}$

Ejemplo 6.1. Estudia si el razonamiento:
"Socrates es humano. Todo humano es mortal. Por tanto, Socrates es mortal."
formalizado mediante

$$\begin{array}{l} \varphi_1 = H(s) \\ \varphi_2 = \forall x (H(x) \to M(x)) \\ \hline \psi = M(s) \end{array}$$

es correcto.
Como son formulas cerradas, basta con considerar interpretaciones, no hace falta considerar asignaciones.
Queremos ver que $\{\varphi_1, \varphi_2\} \vDash \psi$ o lo que es lo mismo, $\varphi_1 \wedge \varphi_2 \to \psi$ es una tautologia.
Sea (D, I) una interpretacion tal que $\varphi_1 = 1$ y $\varphi_2 = 1$.
La condicion de que $\varphi_1^I = 1$ es que $(H(s))^I = 1$.
$s^I \in H^I \subseteq D$ si la formula es verdadera. Entonces tengo que $s^I \in H^I$.

La condicion de $\varphi_2^I = 1$ es $\forall x(H(x) \to M(x))^I = 1$. Esto es lo mismo que decir que $H^I \subseteq M^I$.
Uniendo $s^I \in H^I$ y que $H^I \subseteq M^I$ tengo $s^I \in M^I \Rightarrow (M(s))^I = 1$.

Ejemplo 6.2. Estudia si el razonamiento:

$$\begin{array}{l} \varphi_1 = M(s) \\ \varphi_2 = \forall x(H(x) \to M(x)) \\ \hline \psi = H(s) \end{array}$$

es correcto.
Es incorrecto. Tengo que demostrarlo con un contraejemplo.
Por ejemplo, $D = \mathbb{N}$.
$H(x) = x$ es multiplo de 4
$M(x) = x$ es par
Mas formal: $H^I = \{x \mid x \text{ es multiplo de } 4\}$ y $M^I = \{x \mid x \text{ es multiplo de } 2\}$.
$\varphi_2^I = 1$ porque si se cumple que un elemento es multiplo de 4 entonces tambien es multiplo de 2.
$S^I = 6$. Con esta interpretacion $M(s)^I = 1$ porque $2|6$ pero $H(s)^I = 0$ porque $4 \nmid 6$.
Otra alternativa es elegir conjuntos finitos sencillos.

$$\left.\begin{array}{l} D = \{a, b\} \\ H^I = \{a\} \\ M^I = \{a, b\} \\ s^I = b \end{array}\right\}$$

Esta interpretacion tambien es un contraejemplo al razonamiento.
$\varphi_1^I = 1$ porque $s^I \in M^I$
$\varphi_2^I = 1$ porque $H^I \subseteq M^I$ $\psi^I = 0$ porque $S^I \notin H^I$

Definición 6.9. Sean φ y ψ dos formulas. Decimos que son equivalentes si se cumple simultaneamente

Proposición 6.2. Sean φ y ψ dos formulas. Las siguientes dos afirmaciones son equivalentes:

- $\varphi \equiv \psi$

Ejemplo 6.3. Sean φ y ψ formulas cualesquiera y α una formula donde no aparece libre la variable x.

1. $\neg\forall x\varphi \equiv \exists x\neg\varphi$

Vamos a ver que $\varphi_1 \vDash \varphi_2$.

Sean (D, I) interpretacion y A asignacion tales que $(\neg\forall x\varphi)^{I,A} = 1 \Rightarrow (\forall x\varphi)^{I,A} = 0 \Rightarrow \varphi^{I,A[x/d]} = 0$ para algun $d \in D \Rightarrow (\neg\varphi)^{I,A[x/d]} = 1$ para algun $d \in D \Rightarrow (\exists x\neg\varphi)^{I,A} = 1$.

¿Como demuestro que $\varphi_2 \vDash \varphi_1$?

Son los reciprocos del argumento anterior. En realidad, se puede escribir la demostracion como una cadena de dobles implicaciones.

2. $\neg\exists x\varphi \equiv \forall x\neg\varphi$

   Vamos a utilizar (1).

   $\neg\exists x\varphi \equiv \neg\exists x\neg\neg\varphi \overset{(1)}{\equiv} \neg\neg\forall x\neg\varphi \equiv \forall x\neg\varphi$.

3. $\forall x(\varphi \wedge \psi) \equiv \forall x\varphi \wedge \forall x\psi$

   Sean (D, I) una interpretacion y A una asignacion.

   $\forall x(\varphi \wedge \psi)^{I,A} = 1 \Rightarrow$ para todos los valores $d \in D(\varphi \wedge \psi)^{I,A[x/d]} = 1 \Leftrightarrow \varphi^{I,A[x/d]} = 1$ y $\psi^{I,A[x/d]} \Leftrightarrow (\forall x\varphi)^{I,A[x/d]}$ y $(\forall x\psi)^{I,A[x/d]} = 1 \Leftrightarrow ((\forall x\varphi) \wedge (\forall x\psi))^{I,A} = 1$

4. $\exists x(\varphi \vee \psi) \equiv \exists x\varphi \vee \exists x\psi$

   $\exists x(\varphi \vee \psi) \equiv \neg\neg\exists x(\varphi \vee \psi) \equiv \neg\forall x\neg(\varphi \vee \psi) \equiv \neg\forall x(\neg\varphi \wedge \neg\psi) \equiv \neg(\forall x\neg\varphi \wedge \forall x\neg\psi) \equiv \neg\forall x\neg\varphi \vee \neg\forall x\neg\psi \equiv \exists x\neg\neg\varphi \vee \exists x\neg\neg\psi \equiv \exists x\varphi \vee \exists x\psi$

5. $\forall x\varphi \wedge \alpha \equiv \forall x(\varphi \wedge \alpha)$

   Sean (D, I) una interpretacion y A una asignacion.

   $\forall x(\varphi \wedge \alpha) = 1 \Leftrightarrow (\varphi \wedge \alpha)^{I,A[x/d]} = 1$ para todo $d \in D \Leftrightarrow \varphi^{I,A[x/d]} = 1$ y $\psi^{I,A[x/d]} = 1$ para todo $d \in D \Leftrightarrow \varphi^{I,A[x/d]} = 1$ para todo $d \in D$ y $\alpha^{I,A} = 1$ (porque x no aparece libre en α) $\Leftrightarrow \forall x\varphi^{I,A} = 1$, $\alpha^{I,A} = 1 \Leftrightarrow (\forall x\varphi \wedge \alpha)^{I,A} = 1$

Ejemplo 6.4. Sean φ y ψ cualesquiera y α una formula donde no aparece libre la variable x. En general las siguientes formulas no son equivalentes:

b) $\forall(\varphi \vee \psi) \not\equiv \forall x\varphi \vee \forall x\psi$

   Elijo P, Q dos predicados de aridad 1.

   $D = \{a, b\}$, $P^I = \{a\}$, $Q^I = \{b\}$.

$$\begin{cases} \forall x(P(x) \vee Q(x)) = \varphi_1 \\ \forall x P(x) \vee \forall x Q(x) = \varphi_2 \end{cases}$$

   $\varphi_1^I = 1$ porque si $x = a$ $\underbrace{\underbrace{P(a)}_{1} \vee Q(a)}_{1}$ y si $x = b$, $\underbrace{P(b) \vee \underbrace{Q(b)}_{1}}_{1}$.

$\varphi_2^I = 0$ porque

$$\begin{cases} \forall x P(x)^I = 0 \text{ porque } x = b \text{ es un contraejemplo} \\ \forall x P(x)^I = 0 \text{ porque } x = a \text{ es un contraejemplo} \end{cases}$$

Hemos visto que $\varphi_1 \not\equiv \varphi_2$. ¿Alguna implica logicamente a la otra?

$\psi \vDash \varphi$

Si $\varphi_2^{I,A} = 1 \Rightarrow$ o bien $(\forall x P(x))^{I,A} = 1 \Rightarrow \varphi^{I,A} = 1$ o bien $(\forall x(Q(x)))^{I,A} = 1 \Rightarrow \varphi^{I,A} = 1$.

c) $\exists x(P(x) \wedge Q(x)) = \varphi_1$

$\exists x P(x) \wedge (\exists x Q(x)) = \varphi_2$

$D = \{a, b\}$, $P^I = \{a\}$, $Q^I = \{b\}$

$\varphi_2^I = 1$ porque $\exists x P(x)^I = 1$ como $x = a$ y $\exists x Q(x)^I = 1$ con $x = b$.

$\varphi_1^I = 0$ porque si $x = a$ $\underbrace{\underbrace{P(a)}_{1} \wedge Q(a)}_{0}$ y si $x = b$ $\underbrace{(P(b) \wedge \underbrace{Q(b)}_{1})}_{0}$.

Se que φ_1 porque $\varphi_2 \not\vDash \varphi_1$.

Es cierto que $\varphi_1 \vDash \varphi_2$?

Si I es una interpretacion tal que $\varphi_1 = 1 \Rightarrow$ Existe $d \in D$ tal que $d \in P^I$ y $d \in Q^I \Rightarrow \exists x P(x)^I = 1$ y $\exists x Q(x)^I = 1 \Rightarrow \varphi_2^I = 1$.

d) $\forall x\varphi \to \alpha \not\equiv \forall x(\varphi \to \alpha)$

$\forall x(\varphi \to \alpha) \equiv \forall x(\neg\varphi \vee \alpha) \equiv \forall x \neg\varphi \vee \alpha \equiv \neg\exists\varphi \vee \alpha \equiv \exists x\varphi \to \alpha \not\equiv \forall x\varphi \to \alpha$.

Justificacion de que no son equivalentes:

Con $\alpha = p$ simbolo de proposicion atomica y $\varphi = P(x)$ predicado de aridad 1.

$\exists P(x) \to p \not\equiv \forall x P(x) \to p$

$D = \{a, b\}$, $P^I = \{a\}$ y $p^I = 0$

$\underbrace{\underbrace{\exists x P(x)}_{1} \to \underbrace{p}_{0}}_{0} \quad \underbrace{\underbrace{\forall x P(x)}_{0} \to \underbrace{p}_{0}}_{1}$

7 Teoria de la demostracion en logica de predicados

Observación 7.1. Los simbolos de funcion no son necesarios para la logica de predicados. Se pueden "simular" con predicados.

Ejemplo 7.1. $D = \{\text{personas}\}$
$m(x)$: la madre de $x \to M(x, y)$: x es la madre de y.
"La madre de Antonio es rubia".
$R(x)$: x es rubio. $R(m(a))$.
$\forall x(M(x, a) \to R(x))$
"Todos los hermanos de Antonio son rubios" $\Rightarrow \forall x(H(x, a) \to R(x))$ (que no la puedo hacer con funciones).

Vamos a ampliar el sistema de Gentzen para la logica proposicional, añadiendo a las 8 relgas que teniamos 4 nuevas reglas para los cuantificadores. El sistema de demostracion resultante es valido para la logica de predicados sin igualdad (definir un sistema que sea valido para la logica de predicados con igualdad que hemos introducido en los temas 5 y 6 requeriria reglas adicionales y tiene cierto grado de complejidad).
Los nombres de las 4 nuevas reglas de inferencia son:

$E\forall$	$I\forall$
$E\exists$	$I\exists$

Proposición 7.1.

- $\varphi, \psi, \ldots$ representaran formulas cualesquiera de la logica de predicados.
- $\varphi(x)$ denotara una formula donde la variable x tiene apariciones libres. Si despues escribimos $\varphi(t)$, donde t puede ser un termino cualquiera, esto representara la formula φ donde todas las apariciones libres de x se han sustituido por t.
- Llamaremos variable fresca a una variable que no ha aparecido previamente en el razonamiento.

Definición 7.1 — Regla de eliminacion del universal, $E\forall$. Sea t un termino cualquiera

$$\frac{\forall x \varphi(x)}{\varphi(t)}$$

Definición 7.2 — Regla de introduccion del existencial, $I\exists$. Sea t un termino cualquiera

$$\frac{\varphi(t)}{\exists x \varphi(x)}$$

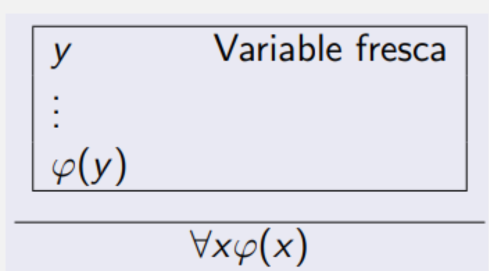
Ejemplo 7.2. Demostrar la validez de $\{\forall x(P(x) \to Q(x)), P(a)\} \vdash Q(a)$.

1. $\forall x(P(x) \to Q(x))$ Pr
2. $P(a)$ Pr
3. $P(a) \to Q(a) \quad E\forall, 1, x = a$
4. $Q(a) \quad E \to, 2, 3$

Ejemplo 7.3. Demostrar la validez de $\{P(b), \exists x P(x) \to Q(a)\} \vdash Q(a)$.

1. $P(b)$ Pr
2. $\exists x P(x) to Q(a)$ Pr
3. $\exists x P(x) \quad I\exists, 1$
4. $Q(a) \quad E \to, 2, 3$

Definición 7.3 — Regla de introduccion del universal, $I\forall$. .



Observación 7.2. Este es el unico caso en el que usamos una demostracion auxiliar que

no empieza con una premisa auxiliar, sino con una variable libre y que no sirve para introducir un implica sino un para todo.

Ejemplo 7.4. Demostrar la validez de $\forall x P(x) \wedge \forall x Q(x) \vdash \forall x(P(x) \wedge Q(x))$

1. $\forall x P(x) \wedge \forall x Q(x)$

2. y Variable fresca
3. $\forall x P(x) \quad E\wedge, 1$
4. $P(y) \quad E\forall, 3, x = y$
5. $\forall x Q(x) \quad E\wedge, 1$
6. $Q(y) \quad E\forall, 5, x = y$
7. $P(y) \wedge Q(y)$

8. $\forall x(P(x) \wedge Q(x)) \quad I\forall(2-7)$

Ejemplo 7.5. Demostrar la validez de $\forall x(P(x) \wedge Q(x)) \vdash \forall x P(x) \wedge \forall x Q(x)$.

1. $\forall x(P(x) \wedge Q(x))$ Pr

2. y Variable fresca
3. $P(y) \wedge Q(y) \quad E\forall, 1, x = y$
4. $P(y) \quad E\wedge, 3$

5. $\forall x P(x) \quad I\forall(2-3)$

6. z Variable fresca
7. $P(z) \wedge Q(z) \quad E\forall, 1, x = z$
8. $Q(z) \quad E\wedge, 7$

9. $\forall x Q(x) \quad I\forall(6-8)$
10. $\forall x P(x) \wedge \forall x Q(x) \quad I\wedge, 5, 9$

Definición 7.4 — Regla de eliminacion del existencial, $E\exists$. Sea y una variable fresca y que no aparece libre en ψ.

$$\frac{\begin{array}{c}\exists x\varphi(x)\\ \varphi(v)\rightarrow\psi\end{array}}{\psi}$$

Observación 7.3. Tipicamente la regla $E\exists$ se usa cuando se tiene una formula $\exists x\varphi(x)$, iniciando una demostracion auxiliar que tiene como premisa auxiliar $\varphi(y)$ y llegando a una conclusion que no dependa de y.

$$\begin{array}{ll}
\exists x\varphi(x) & \\
\boxed{\begin{array}{ll}\varphi(y) & \text{Premisa auxiliar}\\ \vdots & \\ \psi & \end{array}} & \\
\varphi(y)\rightarrow\psi & \mathrm{I}\rightarrow\\
\psi & \mathrm{E}\exists
\end{array}$$

Ejemplo 7.6. Demostrar la validez de $\{\forall x(P(x)\rightarrow Q(x)), \exists xP(x)\}\vdash\exists xQ(x)$.

1. $\exists xP(x)$ Pr
2. $\forall x(P(x)\rightarrow Q(x))$ Pr

> 3. $P(y)$ Pr aux (var fresca)
> 4. $P(y)\rightarrow Q(y)$ $\quad E\forall, 2, x=y$
> 5. $Q(y)$ $\quad E\rightarrow, 3, 4$
> 6. $\exists xQ(x)$ $\quad I\exists, 5, x=y$

7. $P(y)\rightarrow\exists xQ(x)$ $\quad I\rightarrow(3-6)$
8. $\exists xQ(x)$ $\quad E\exists, 1, 7$

Ejemplo 7.7. Demostrar la validez de $\{\exists xP(x), \exists xQ(x)\}\vdash\exists x\exists y(P(x)\wedge Q(y))$.

1. $\exists xP(x)$ Pr
2. $\exists xQ(x)$ Pr

3. $P(z)$ Pr aux (z var fresca)

4. $Q(t)$ Pr aux (t var fresca)
5. $P(z) \wedge Q(t) \quad I\wedge, 3, 4$
6. $\exists y(P(z) \wedge Q(y)) \quad I\exists, 5, y = t$

7. $Q(t) \to \exists y(P(z) \wedge Q(y)) \quad I \to (4-6)$
8. $\exists y(P(z) \wedge Q(y)) \quad E\exists, 2, 7$
9. $\exists x \exists y(P(x) \wedge Q(y)) \quad I\exists, 8, x = z$

10. $P(z) \to \exists x \exists y(P(x) \wedge Q(y)) \quad I \to (3-9)$
11. $\exists x \exists y(P(x) \wedge Q(y)) \quad E\exists, 1, 10$

Ejemplo 7.8. Demostrar la validez de $\exists y \forall x P(x,y) \vdash \forall x \exists y P(x,y)$.

1. $\exists y \forall x P(x,y)$ Pr

2. $\forall x P(x,z)$ Pr aux (var fresca)

3. t Var fresca
4. $P(t,z) \quad E\forall, 2, x = t$
5. $\exists y P(x,y) \quad I\exists, 4, y = z$

6. $\forall x \exists y P(x,y) \quad I\forall(3-5)$

7. $\forall x P(x,z) \to \forall x \exists y P(x,y) \quad I \to (2-6)$
8. $\forall x \exists y P(x,y) \quad E\exists, 1, 7$

Observación 7.4. Se puede demostrar que el sistema de Gentzen que hemos introducido es correcto y completo para la logica de predicados. Sin embargo, esta logica no es decidible.