Proposición lógica

Afirmación matemática que es verdadera o falsa

Función proposicional

Afirmación matemática que involucra variables y que es verdadera o falsa según los valores que tomen las variables.

Tanto funciones proposicionales como proposiciones pueden combinarse mediante conectores lógicos: $\neg$, $\wedge$, $\vee$. También pueden contener cuantificadores.

Los cuantificadores deben ir a la izquierda, separados por ",", y el orden en que aparecen importa.

Cada cuantificador DEBE cuantificar una variable DISTINTA, y las variables no cuantificadas se llaman **variables libres**

Cuantificador ***universal***

Una expresión de la forma:

$\forall\langle$variable$\rangle$ en $\langle$conunto$\rangle$, $\langle$función proposicional$\rangle$

Afirma que la función proposicional se hace verdadera en *todos* los valores de la variable dentro del conjunto especificado. Aquí la "," se pude leer como "cumple que".

Cuantificador ***existencial***

Una expresión de la forma:

$\exists\langle$variable$\rangle$ en $\langle$conunto$\rangle$, $\langle$función proposicional$\rangle$

Afirma que la función proposicional se hace verdadera en *alguno* de los valores de la variable dentro del conjunto especificado. Aquí la "," se pude leer como "tal que".

Definición intuitiva de conjunto

Un *conjunto* es una colección bien definida de objetos bien definidos.

Conjunto vacío El conjunto que no tiene ningún elemento se llama *conjunto vacío*, y se denota por ϕ.

Notación En un conjunto, llamamos *elementos* a los objetos que lo constituyen, en ese caso decimos que los elementos *pertenecen* al conjunto.

Si C es un conjunto, y x es elemento de C escribimos $x \in C$.

Descripción por extensión (o extensiva)

Consiste en *listar* todos los elementos del conjunto, encerrados entre llaves "{" "}" y separados por comas ",". El uso de las llaves es esencial a los conjuntos.

Ejemplo: $\{14, -5, 0\}$

Descripción por comprensión (o intensiva) de un conjunto

Consiste en ofrecer una propiedad que *caracteriza* a sus elementos.

Sintaxis

$$A = \{x : \ p(x)\}$$

$$x \in A \Leftrightarrow p(x) \text{ es una proposición verdadera}$$

o bien, si $f(x)$ es una expresión algebraica.

$$B = \{f(y) : \ p(y)\}$$

$$x \in B \Leftrightarrow \exists y, \ x = f(y) \wedge p(y) \text{ es una proposición verdadera}$$

Relación binaria interna

Dado un conjunto A, una *relación binaria interna* en A es un conjunto $R \subseteq A \times A$.

Cuando $(a, b) \in R$, escribimos $a\ R\ b$, y leemos "*a está relacionado con b*".

- R es **refleja** si $\forall a \in A,\ a\ R\ a$.
- R es **simétrica** si $\forall a, b \in A,\ a\ R\ b \Rightarrow b\ R\ a$.
- R es **antisimétrica** si $\forall a, b \in A,\ (a\ R\ b\ \wedge\ a \neq b) \Rightarrow b\ \not R\ a$.
- R es **transitiva** si $\forall a, b, c \in A,\ (a\ R\ b\ \wedge\ b\ R\ c) \Rightarrow a\ R\ c$.

R es **relación de orden** si es refleja, antisimétrica y transitiva.

R es **relación de equivalencia** si es refleja, simétrica y transitiva.

Dada una relación de orden R en A se define lo siguiente.

- a es **comparable** con b si $a\ R\ b\ \vee\ b\ R\ a$.
- R es **relación de orden total** si $\forall a, b \in A,\ a$ es comparable con b.
- R es **relación de orden parcial** si no es de orden total.
- a es **sucesor** de b si $a\ R\ b$, $a \neq b$ y $\forall z \in A,\ (a\ R\ z\ \wedge\ z\ R\ b) \Rightarrow (a = z \vee b = z)$ (*no hay nadie entremedio*).
- m es **mínimo** de A, si $\forall b \in A,\ m\ R\ b$ (*está relacionado con todos*).
- m es **minimal** de A, si $\forall b \in A,\ b\ R\ m\ \Rightarrow b = m$ (*no hay otro relacionado con él*).
- M es **máximo** de A, si $\forall b \in A,\ b\ R\ M$ (*todos están relacionados con él*).
- M es **maximal** de A, si $\forall b \in A,\ M\ R\ b\ \Rightarrow b = M$ (*no está relacionado con nadie más*).

Propiedades

- El mínimo y el máximo, cuando existen, son únicos.
- Si m es mínimo, también es minimal.
- Si M es máximo, también es maximal.
- Si $m \neq m'$ son minimales, entonces no existe mínimo.
- Si $M \neq M'$ son maximales, entonces no existe máximo.
- Si R es de orden total y m es minimal, entonces m también es mínimo.
- Si R es de orden total y M es maximal, entonces M también es máximo.

Dada una relación de equivalencia R en A se define lo siguiente.

Clases de equivalencia

La *clase de equivalencia* de un elemento $a \in A$ es el conjunto:

$$[a] = \{b \in A \mid b\ R\ a\}$$

Propiedades

- $\forall a \in A,\ a \in [a]$
- $\forall a, b \in A,\ [a] \cap [b] \neq \phi \Rightarrow a\ R\ b$
- $\forall a, b \in A,\ a\ R\ b \Rightarrow [a] = [b]$
- El conjunto de las clases de equivalencias confirma una partición de A.

Conjunto cuociente

El conjunto de las clases de equivalencias de A relativo a una relación R se llama *conjunto cuociente de* A, y se denota A/R:

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

La función f que a cada elemento de A le asocia su clase de equivalencia se llama *sobreyección canónica* de A en A/R:

$$\begin{aligned} f : A &\rightarrow A/R \\ f(a) &= [a] \end{aligned}$$

La relación R puede ser caracterizada por esta función, es decir:

$$\forall a, b \in A,\ a\ r\ b \Leftrightarrow f(a) = f(b)$$

Congruencias módulo p

Dado un natural $p \geq 2$, la relación $\sim_p$ en $\mathbb{Z}$ se llama *congruencia módulo p* y se define como sigue.

$$\forall a, b \in \mathbb{Z},\ a \sim_p b \Leftrightarrow \exists m \in \mathbb{Z},\ a + mp = b$$

Se tiene que $\sim_p$ es una relación de equivalencia, y las clases de equivalencia que genera se llaman *clases de congruencia módulo p.*

$$[a] = \{mp + a \mid m \in \mathbb{Z}\}$$

El conjunto cuociente $\mathbb{Z}/\sim_p$ tiene exactamente p clases $\{[0], [1], \ldots, [p-1]\}$.

En $\mathbb{Z}/\sim_p$ se puede definir la suma y la multiplicación, y se resulta tener inverso aditivo, pero no inverso multiplicativo.

$$[a] + [b] = [a + b] \quad \wedge \quad -[a] = [-a] \quad \wedge \quad [a][b] = [ab]$$

Divisibilidad

Dados a, $b \in \mathbb{N}$, se dice que a *divide* a b si $\exists m \in \mathbb{N}, am = b$, en tal caso escribimos $a|b$ y decimos que a es divisor de b.

Primos

Un número p se dice *primo* si sus divisores son solo 1 y p.

Teorema de división entera

Dados $a \in \mathbb{N}$, $b \in \mathbb{N} \setminus \{0\}$, existen únicos $q \in \mathbb{N}$ y $r \in \{0, \ldots, b-1\}$ tales que $a = qb + r$.

El número q se llama *cuociente* y el número r se llama *resto*.

Propiedades

- Se tiene que $b|a$ si y solo si la división entera de a por b arroja resto igual a 0.
- Si $a = qb + r$, entonces $[a] = [r]$ bajo la relación $\sim_b$.

Máximo divisor común

$D(a) = \{n \in \mathbb{N} \;:\; n|a\}$ es el conjunto de los divisores de a. Consideremos $A = D(a) \cap D(b)$, el conjunto de los divisores comunes de a y b, con la relación de orden *divide a*. Resulta que A tiene máximo para esa relación y a ese máximo le llamamos $\mathrm{mcd}(a, b)$.

Algoritmo de Euclides

Dados $a, b \in \mathbb{N}$ hacer la siguiente secuencia de divisiones enteras, hasta obtener resto nulo.

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&\cdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1} \\
r_k &= q_{k+2} r_{k+1} + 0
\end{aligned}$$

Teorema

El último resto no nulo, r_{k+1}, que se obtiene al aplicar el Algoritmo de Euclides a dos naturales a, b es igual a $\mathrm{mcd}(a, b)$.

Teorema de Bezout

Para todo $a, b \in \mathbb{N}$, existen $e, f \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = ea + fb$.

Lema de Euclides

Dados $a, b, c \in \mathbb{N}$ tales que $a|bc$ y $\mathrm{mcd}(a, c) = 1$, se cumple que $a|b$.

Teorema de descomposición única en números primos

Para todo natural $n \geq 2$, existe una única forma de escribirlo como producto de números primos, esto es, existen únicos $p_1, \ldots, p_k$ primos, y $r_1, \ldots, r_k \in \mathbb{N} \setminus \{0\}$ tales que

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}.$$