

# La Lógica de los Teoremas

## 1. Las fórmulas que son tautologías

Una fórmula lógica de  $F(p_1, \dots, p_k)$  de  $k$  variables,  $p_1, \dots, p_k$  se dice que es una tautología si es siempre cierta para cualesquiera valores de certeza o falsedad de las variables  $p_1, \dots, p_k$ .

Ejemplo 1: Sea la fórmula de una sola variable  $p \vee p'$ , que se puede leer por "se verifica  $p$  o bien no se verifica  $p$ ". Veamos que siempre es cierta (C) para cualesquiera valores de la variable, cierto (C) o falso (F):

P	P'	$P \vee P'$
C	F	C
C	C	C

Ejemplo 2: La fórmula de dos variables  $p \rightarrow p \vee q$  ("Si se verifica  $p$  eso implica que se verifica  $p$  o bien  $q$ ") es una tautología también, pues siempre es cierta, cualesquiera que sean los valores de certeza (C) o de falsedad (F) de ambas variables:

P	Q	$P \vee Q$	$P \rightarrow P \vee Q$
C	C	C	C
C	F	C	C
F	C	C	C
F	F	F	C

## 2. Las reglas básicas para la inferencia

Para la obtención de resultados, obtención de fórmulas, es necesario partir de otras fórmulas o resultados, ya previamente obtenidos, o, simplemente, postulados como ciertos (en este último caso se partiría de axiomas o postulados).

Las fórmulas o resultados de los que se parte para obtener un nuevo resultado se llaman premisas, y la fórmula que se obtiene desde las premisas constituye la conclusión.

El paso desde las premisas a la conclusión es lo que llamamos *proceso de inferencia* o bien *proceso de demostración*.

Para que el proceso de inferencia sea válido los pasos que constituyen el proceso han de ser ciertos, es decir han de estar constituidos por fórmulas tautológicas, por tautologías

Las reglas básicas de la inferencia son muy sencillas:

1. Regla de Inserción: *Cualquier tautología es premisa en el proceso de demostración de cualquier fórmula*, esto es, toda fórmula cierta puede servir para la obtención de otra fórmula o resultado.

2. Regla de Unión: Si se verifica la fórmula  $F$  y se verifica también la fórmula  $G$ , entonces se verificará también la fórmula constituida por  $F$  y  $G$ :

$$F \wedge G \rightarrow (F \wedge G)$$

3. Regla de Sustitución: Si la variable o fórmula  $p$  es equivalente a la variable o fórmula  $q$  entonces, en cualquier fórmula que contenga a una de ellas, puede ésta ser sustituida por la otra:

$$(p \leftrightarrow q) \rightarrow (F(p) \leftrightarrow F(q))$$

4. Regla de Separación 1 o "Modus Ponens": Si una fórmula condicional,  $p \rightarrow q$ , y su antecedente,  $p$ , se toman como premisas, su consecuente,  $q$ , se infiere como conclusión:

$$[(p \rightarrow q) \wedge p] \Rightarrow q$$

5. Regla de Separación 2 o "Modus Tollens": Si una fórmula condicional,  $p \rightarrow q$ , y la negación de su consecuente,  $q'$ , se toman como premisas, la negación de su antecedente,  $p'$ , se infiere como conclusión:

$$[(p \rightarrow q) \wedge q'] \Rightarrow p'$$

### 3. Los términos y proposiciones del lenguaje de la demostración

Los términos que constituyen las fórmulas a demostrar o las fórmulas de las premisas, y, en general, la lógica del proceso de inferencia pueden ser términos primitivos o bien términos definidos.

- Los términos primitivos son los que se introducen en una determinada construcción simplemente con su enunciado, como *elemento*, *conjunto*, ...
- Los términos definidos son los que se definen a partir de términos primitivos o a partir de otros términos anteriormente definidos, como *anillo*, *curva plana*, *grupo*, ...

Las proposiciones o argumentaciones pueden ser axiomas o bien pueden ser teoremas.

- Los axiomas o postulados son afirmaciones o fórmulas postuladas como ciertas para poder desarrollar mediante las reglas de inferencia la construcción de un determinado cuerpo doctrinal.
- Los teoremas son también afirmaciones o fórmulas, pero obtenidas mediante el proceso de la demostración desde los axiomas o postulados, o bien desde otros teoremas previamente demostrados.

### 4. Los axiomas:

Las proposiciones que se tomen como axiomas para obtener a partir de ellas los resultados que constituyen todo el cuerpo doctrinal han de tener las condiciones básicas de

1. Indecibilidad:

Ningún axioma del sistema puede ser obtenido como un teorema partiendo de los restantes.

2. Consistente internamente:

Nunca podrá ser derivada una contradicción como teorema.

3. No contradictoriedad:

Lo afirmado por un axioma no contradice a lo afirmado por cualquiera de los restantes axiomas del sistema.

### 5. La estructura de los teoremas

Mediante las proposiciones o enunciados que constituyen los teoremas obtenemos resultados o fórmulas que también es costumbre identificar con el teorema que ha permitido su obtención.

Los teoremas, en definitiva, son enunciados por los que se afirma el cumplimiento de un determinado resultado o tesis (T), que es la conclusión del teorema, siempre que previamente se verifique una determinada condición o hipótesis (H), constituida por las premisas del proceso de la demostración.

La demostración del teorema es el proceso guiado por las leyes de la inferencia que permite obtener la tesis a partir de la hipótesis:

$$H \Rightarrow T$$

Si dice, en el teorema  $H \Rightarrow T$  que H es suficiente para que se verifique T, o bien, sencillamente, que H implica T.

Se llama *teorema recíproco del teorema  $H \Rightarrow T$*  al teorema  $T \Rightarrow H$ , es decir, la tesis de uno coincide con la hipótesis del otro.

Se llama *teorema contrario del teorema  $H \Rightarrow T$*  al teorema  $H' \Rightarrow T'$ , es decir, es el teorema cuya hipótesis es la negación de la hipótesis del teorema dado, y su tesis es la negación de la tesis.

Se llama *teorema contrarrecíproco del teorema  $H \Rightarrow T$*  al teorema  $T' \Rightarrow H'$ , esto es, al teorema cuya hipótesis es la negación de la tesis del primero y cuya tesis es la negación de la hipótesis del primer teorema.

Es fácil comprobar que los dos teoremas contrarrecíprocos son ciertos o falsos simultáneamente, es decir son lógicamente equivalentes, ya que la fórmula que representa esta equivalencia  $(p \rightarrow q) \leftrightarrow (q' \rightarrow p')$  es una tautología, como podemos comprobar:

P	Q	P'	Q'	P→Q	Q'→P'	(P→Q)↔(Q'→P')
C	C	F	F	C	C	C
C	F	F	C	F	F	C
F	C	C	F	C	C	C
F	F	C	C	C	C	C

Ejemplo:

Veamos un teorema que es sobradamente conocido en el análisis elemental (Teorema de Rolle):

Si una función real de una sola variable real es continua en un intervalo cerrado  $[a,b]$  y diferenciable en su interior  $(a,b)$ , tomando el mismo valor en los extremos del intervalo, entonces existe un punto  $c$  del interior del intervalo en donde la derivada primera de la función se anula. Simbólicamente:

$$\left. \begin{array}{l} f(x) \text{ cont en } [a,b] \\ f(x) \text{ deriv en } (a,b) \\ f(a) = f(b) \end{array} \right\} \rightarrow \exists c \in (a,b) / f'(c) = 0$$

Hipótesis:

La función es continua en un intervalo cerrado, derivable en su interior y tiene el mismo valor en los extremos.

Tesis:

La derivada de la función se anula en algún punto del interior del intervalo.

Teorema recíproco:

Si una función tiene derivada nula en algún punto  $c$  del interior de un intervalo, entonces la función es continua en tal intervalo cerrado y derivable en su interior, teniendo el mismo valor en los extremos del intervalo.

Hipótesis:

La derivada de la función se anula en algún punto del interior del intervalo.

Tesis:

La función es continua en el intervalo cerrado, derivable en su interior y tiene el mismo valor en los extremos.

Obviamente este teorema recíproco no se verifica, pues la función puede tener la derivada nula en algún punto del interior del intervalo sin que necesariamente sea continua en todo punto del mismo ni necesariamente derivable en todo punto interior. Tampoco es necesario que tenga el mismo valor en los extremos del intervalo.

Teorema contrario:

Si una función real de una sola variable real no es continua en un intervalo cerrado  $[a,b]$ , o bien no diferenciable en su interior  $(a,b)$ , o no toma el mismo valor en los extremos del intervalo, entonces no existe un punto  $c$  del interior del intervalo en donde la derivada primera de la función se anula.

Hipótesis:

La función no es continua en un intervalo cerrado, o bien no es derivable en su interior o bien no tiene el mismo valor en los extremos.

Tesis:

La derivada de la función no se anula en algún punto del interior del intervalo.

También es obvio que este teorema contrario tampoco es cierto. Puede ser nula la derivada en algún punto interior aunque no fuera continua en todo el intervalo, o no fuera derivable en todo su interior, o no tuviera el mismo valor en los extremos.

Teorema contrarrecíproco:

Si una función real de una sola variable real no tiene derivada nula en algún punto del interior de un intervalo cerrado, entonces o no es continua en todo el intervalo cerrado, o no es derivable en todo el interior del intervalo, o no tiene el mismo valor en los extremos del intervalo.

Hipótesis:

La función no tiene derivada nula en algún punto del interior del intervalo

Tesis:

La función no es continua en el intervalo, o no es derivable en su interior o no tiene el mismo valor en los extremos del intervalo.

Este teorema es el que se verifica, si es cierto el teorema directo de partida.

## 6. Los tipos de demostración

### 1) Demostraciones directas:

Consisten en considerar las definiciones, axiomas y resultados previamente obtenidos mediante otros teoremas los cuales, sirviendo como premisas, permiten obtener, mediante las reglas de derivación o inferencia, el resultado o los resultados que se indican en la tesis del teorema.

Ejemplo:

Veamos una forma directa de demostrar el teorema de Rolle, enunciado antes.

- Si una función es continua en un intervalo cerrado, por el teorema de Bolzano-Wierstrass existen en el interior del intervalo al menos dos puntos,  $c_1$  y  $c_2$  donde la función toma un valor máximo  $M$  y un valor mínimo  $m$ , respectivamente:

$$\exists c_1 \in (a, b) / f(c_1) = M \text{ (máximo)}$$

$$\exists c_2 \in (a, b) / f(c_2) = m \text{ (mínimo)}$$

Pueden darse solamente dos situaciones:

$$1) m = M \qquad 2) m \neq M$$

2) Si  $m = M$  la función es constante en todo el intervalo  $[a, b]$ , por lo que la derivada en cualquier punto del intervalo es nula, verificándose el teorema para este caso.

3) Si es  $m \neq M$  será  $M \neq f(a) = f(b)$  o bien  $m \neq f(a) = f(b)$ .

- Supongamos que sea  $M \neq f(a) = f(b)$  y sea  $c_1$  el punto donde se obtiene el valor máximo  $M$  que da el teorema de Bolzano-Weirstrass:  $c_1 \in (a, b) / f(c_1) = M$ .  $f(x)$  ha de ser derivable en  $c_1$  por ser derivable en todo el interior del intervalo, es decir, existen las derivadas laterales en el punto  $c_1$ , que son iguales:

$$h > 0 \rightarrow \frac{f(c_1 + h) - f(c_1)}{h} \leq 0 \rightarrow f'(c_1^+) = \lim_{h \rightarrow 0} \frac{f(c_1 + h) - f(c_1)}{h} \leq 0$$

$$h < 0 \rightarrow \frac{f(c_1 + h) - f(c_1)}{h} \leq 0 \rightarrow f'(c_1^-) = \lim_{h \rightarrow 0} \frac{f(c_1 + h) - f(c_1)}{h} \leq 0$$

$$f'(c_1^+) = f'(c_1^-) \rightarrow f'(c_1) = 0$$

- Supongamos que sea  $m \neq f(a) = f(b)$ . El razonamiento es el mismo y también obtenemos que  $f'(c_2) = 0$

#### 4) Demostraciones indirectas o por reducción al absurdo:

Estas demostraciones se basan en el hecho de que cualquier teorema es equivalente a su teorema contrarrecíproco.

El proceso consiste en probar el teorema contrarrecíproco  $T' \Rightarrow H'$  para establecer como probado el teorema directo  $H \Rightarrow T$ .

Ejemplo:

En el caso del teorema de Rolle, se entiende que el teorema contrarrecíproco queda demostrado con la demostración del teorema directo vista más arriba, o bien, recíprocamente, que el teorema directo queda demostrado si demostramos el teorema contrarrecíproco, antes enunciado.

Son innumerables las situaciones en las que es mucho más sencillo, a la hora de probar un teorema, efectuar la demostración de su teorema contrarrecíproco.

#### 5) Demostraciones por recurrencia o inducción completa:

Son estas las demostraciones que se apoyan en el proceso de la inducción completa:

- Comprobar que la fórmula a probar es cierta par un primer valor de un conjunto ordenado A.
- Demostrar mediante las reglas de la inferencia que si la fórmula es cierta para un determinado valor n del conjunto indicado A, también será fórmula cierta para el valor siguiente, n+1, en dicho conjunto ordenado.

Se concluye, entonces, que la fórmula es cierta para todo elemento del conjunto ordenado A, a partir del primer valor

Ejemplo:

Demostración de que la expresión  $a^{2n} - 1$  es divisible por  $a+1$ ,  $\forall n \in \mathbb{N} / n > 0$ :

Veamos que es cierta para  $n=1$ :

Si es  $n=1$ , entonces  $a^{2n} - 1 = a^2 - 1 = (a+1).(a-1)$ . Por tanto  $\frac{a^{2n} - 1}{a+1} = \frac{a^2 - 1}{a+1} = a - 1$ ,

lo que implica que se verifica la proposición para  $n=1$ .

Supongamos la condición cierta para  $n=k$ , es decir, que la expresión  $a^{2k} - 1$  es divisible por  $a+1$ . Vamos a probar, que, entonces, para  $n=k+1$  también es divisible por  $a+1$ , es decir, que  $a^{2(k+1)} - 1$  es divisible por  $a+1$ :

$$\begin{aligned} a^{2(k+1)} - 1 &= a^{2k} \cdot a^2 - 1 = a^{2k} \cdot a^2 - a^2 + a^2 - 1 = (a^{2k} - 1) \cdot a^2 + a^2 - 1 = \\ &= (a^{2k} - 1) \cdot a^2 + (a+1) \cdot (a-1) \end{aligned}$$

que es divisible por  $a+1$  por serlo ambos sumandos.

En definitiva, la expresión dada es divisible por  $a+1$  para todo  $n > 1$ .

## 7. Conjeturas

En la Matemática, el concepto de *conjetura* se refiere a una afirmación o enunciado que no siendo considerado un axioma o postulado se supone o se sospecha que es cierta dentro de una determinada construcción, pero que no ha podido ser probada ni tampoco refutada. La conjetura deja de serlo en cuanto se consigue una demostración de la misma usando las reglas de la inferencia, pasando entonces a ser un teorema, a partir del cual pueden ser probados otros resultados o proposiciones, esto es, nuevos teoremas.

Ejemplos:

1. La Conjetura de Fermat, también llamada (antes de que se consiguiera su demostración y, por tanto, impropriamente) Último Teorema de Fermat. Afirma este enunciado que para números enteros  $a$ ,  $b$ ,  $c$ , la siguiente expresión no se verifica nunca si  $n > 2$ :

$$a^n + b^n = c^n$$

- Esta conjetura, como sabemos, dejó de serlo en el año 1994 cuando Andrew Wiles y Richard Taylor consiguieron la demostración a partir de otros resultados previos, como el teorema de Taniyama-Shimura (en realidad, la parte principal de la demostración consistió en probar que el enunciado de Taniyama-Shimura era un teorema, pues hasta entonces era también conjetura).
2. La hipótesis del Continuo. Esta conjetura de George Cantor afirma que entre el cardinal transfinito de los números naturales  $\aleph_0$  (Aleph sub cero) y el cardinal transfinito de los números reales  $\aleph_1$  (aleph sub uno) no existe ningún otro cardinal transfinito. Esta conjetura, que constituye uno de los 23 problemas de Hilbert, fue objeto de diferentes intentos de demostración en la primera mitad del siglo XX hasta que Gödel logró probar que no es demostrable desde los axiomas de la construcción que se utilizaba, los axiomas llamados de Zermelo-Fraenkel con axioma de elección. Y qué, por consiguiente, podrían ocurrir solo dos alternativas: que la hipótesis fuera falsa, o bien que tampoco fuera refutable desde el sistema de axiomas indicado, con lo que la hipótesis del continuo sería no decidible dentro de la construcción de referencia. Este último hecho fue el que se comprobó cuando en 1963 Paul Cohen probó la no demostrabilidad de la negación de la hipótesis del continuo. Esto quiere decir que tanto la hipótesis como su negación podrían ser un nuevo axioma para una nueva matemática, pudiéndose establecer tanto una matemática que aceptara como nuevo axioma la hipótesis de Cantor, como una matemática que aceptara como nuevo axioma su negación.
  3. La conjetura de Golbach. Afirma que todo número par mayor que 2 es la suma de dos números primos. El problema de demostrar esta conjetura está abierto desde su enunciado en 1742. Se ha convertido hoy en uno de los problemas de mayor dificultad existentes en la matemática. La conjetura se ha comprobado cierta, mediante procesos de computación, para números pares menores de un millón de billones, pero la demostración mediante reglas de inferencia no ha sido lograda.